DOI 10.15302/J-SSCAE-2021.02.007

Development Trend and Path of Industrial Internet Security Industry in China

Wang Qiuhua [1], Wu Guohua [1], Wei Dongxiao [2], Miao Gongxun [2], Xu Yanfei [3], Ren Yizhi [1]

1. School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China
2. Zhongfu Information Inc., Jinan 250101, China
3. Chinese Academy of Cyberspace Studies, Beijing 100010, China

Abstract: Industrial Internet security is a prerequisite and guarantee for the high-quality development of China's industrial Internet industry. It is also important for enhancing China's cyber and manufacturing industries. This study aims to contribute to the future development of the industrial Internet security industry in China. First, we analyze the development status of the industry in terms of industrial policies, standards system, industrial structure, and industrial scale. Subsequently, we elaborate on the opportunities and trends of the industry and propose the development path for the next-generation industrial Internet security industry in China. To explore a sustainable development path suitable for China's industrial Internet security industry, top-level design and policy guidance should be enhanced, technological innovation and transformation should be reinforced, the advantages of enterprises and organizations should be complemented to construct a healthy development ecosystem, the security and stability of the supply chain should be emphasized, and personnel training and team building should be promoted to support the research collaboration among government, industry, universities, research institutes, and application.

Keywords: industrial Internet security; industry ecosystem; classified protection of cybersecurity; independent and controllable

1 Introduction

China is in a period of historical opportunity for a new round of industrial revolution. As an important part of new infrastructure construction, the industrial Internet is a key path to promoting the deep integration of digital and real economies. Accordingly, China attaches great importance to the industrial Internet and proposes requirements for the in-depth implementation of the industrial Internet innovation development strategy [1]. Since China's State Council issued the *Guiding Opinions on Deepening the Internet Plus Advanced Manufacturing Development of the Industrial Internet* in 2017, a series of supporting policies have been issued successively. The Internet innovation development strategy has been gradually implemented, and significant progress has been made. At present, China's industrial Internet is developing rapidly and has been widely used in energy, transportation, manufacturing, national defense, and other industries, and its driving effect on economic and social development has become increasingly significant. While constructing a new manufacturing and service system, the Industrial Internet provides support for high-quality development and supply-side reforms. It also breaks the relatively closed and credible state of the traditional industrial environment and increases the possibility of cyber-attacks [2]. Security incidents in the industrial fields of various countries are frequent, and the effects are becoming increasingly serious. Cyber-attacks have become a key factor restricting the development of the industrial Internet. As an important part

Received date: January 20, 2021**; Revised date:** February 22, 2021
Corresponding author: Ren Yizhi, professor of School of Cyberspace of Hangzhou Dianzi University. Major research field is cyberspace security. E-mail: renyz@hdu.edu.cn
Funding program: CAE Advisory Project "Research on Development Strategy for Next-Generation Industrial Internet Security Technology" (2020-XZ-02)
Chinese version: Strategic Study of CAE 2021, 23(1): 046–055
Cited item: Wang Qiuhua et al. Development Trend and Path of Industrial Internet Security Industry in China. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2021.02.007

of national security, industrial Internet security is related to economic development and social stability; hence, it is inevitable to eliminate industrial control security threats and hidden dangers and establish a scientific and systematic security protection system [3].

From the perspective of product competition, the global industrial Internet industry can be divided into three major sectors: hardware and network, software and platform, and information security. In 2018, hardware and network products accounted for 49.8% of the global industrial Internet industry, software and platform products accounted for 48.3%, and information security products accounted for 1.9%. The market size of the global industrial Internet information security industry in 2019 was 15.66 billion US dollars, and it is expected to reach 22.2 billion US dollars in 2025 [4]. In comparison with developed countries, the independent research and development capabilities of software and hardware products in China's industrial Internet security industry are insufficient, and there are still huge gaps in core technology, industrial scale, promotion, and application. High-end key infrastructure equipment, control systems, software, and platform markets have been occupied by foreign products for a long time, such as the micro-control unit, digital signal processor, field-programmable gate array, and other core component technologies in industrial control systems. There is, therefore, a big gap when compared with foreign countries. Data acquisition and monitoring control systems, programmable logic controllers, distributed control systems, and process control systems rely more on foreign supplies [5]. To accelerate the development of the industrial Internet security system and enhance industrial Internet security capabilities, China needs to promote the implementation of industrial Internet security responsibilities, develop an Internet security management system, improve the level of corporate Internet security protection, strengthen Internet data security protection capabilities, improve national industrial Internet security technology measures, strengthen industrial Internet security public service capabilities, and promote industrial Internet security technology innovation and industrial development through continuous effort in these seven areas.

2 Development status of China's industrial Internet security industry

2.1 Continuous in-depth improvement and refinement of industrial Internet security industry policies

With the continuous integration of new-generation information technologies such as cloud computing, fifth-generation mobile communications (5G), and the Internet of Things, network security risks in the industrial field are gradually increasing, and industrial Internet security has become a topic of great concern to the country and enterprises. From the perspective of national security, China has performed top-level design and strategic layout of the industrial Internet security system; adheres to the development path of ensuring development with safety, thereby promoting safety with development; and focuses equally on safety and development, thereby ensuring that safety protection and information construction are planned and that synchronized construction and simultaneous operation [6] have laid a good foundation for the healthy development of the industrial Internet security industry. In recent years, China has successively issued a series of policies and guidelines to continuously refine and improve its industrial Internet security policy system at the macro, meso, and micro levels. In July 2019, ten departments including the Ministry of Industry and Information Technology jointly issued the *Guiding Opinions on Strengthening Industrial Internet Security Work*, which systematically laid out the industrial Internet security work and indicated the direction for healthy development within the industry. More industrial policies are likely to be introduced in the future to continuously support industrial Internet security and to guide its comprehensive development.

2.2 Gradual adjustment and continuous optimization of Industrial Internet security industry structure

The industrial Internet security standard system is mainly composed of basic common, security protection, security service, and vertical industry standards [7] (Table 1). Standardization is essential for the construction of an industrial Internet security system. In recent years, in response to the cross-industry, cross-professional, and cross-field characteristics of industrial Internet standards, China has accelerated the development of related standards and successively released standards and specifications such as the *General Requirements for Industrial Internet Security Protection* and the *Industrial Internet Platform Security Protection Requirements*. The *Industrial Internet Comprehensive Standardization System Construction Guide* initially formed an industrial Internet security standards system covering equipment, control, network, data, application, and platform security, along with security management (Fig. 1). In future, industrial Internet security-related standards will be further improved and industry development will become more standardized.

DOI 10.15302/J-SSCAE-2021.02.007

Table 1. Industrial Internet security standards system.

Standards category	Standardization direction
Basic common standards	Definition of terms
	Security architecture and model
Security protection standards	Equipment and control security
	Edge computing security
	Platform security
	Data security
	Identity resolution security
	Network and communication security
	Application security
	Security management
Security service standards	Inspection and evaluation
	Situational awareness and early warning
	Emergency services
	Operation and maintenance services
	Testing and certification
Vertical industry standards	To develop a more targeted and guiding national set of standards of industrial information security for automobile, steel, petrochemical, and other key industries, combined with industry characteristics and needs

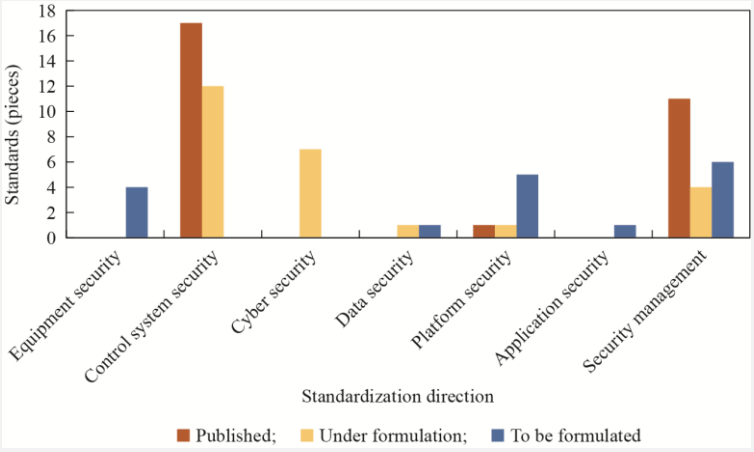

Fig. 1. Development of China's industrial Internet security standards.

2.3 Gradual adjustment and continuous optimization of Industrial Internet security industry structure

The structure of the industrial Internet security industry is divided into two categories: security products and security services, based on market applications [8] (Table 2). At present, both the industrial Internet security product market and the service market in China are continuously developing and expanding; the product and service system is being accelerated; and the industrial structure is continuously being optimized, exhibiting the following characteristics.

Table 2. Industrial structure of industrial Internet security.

Name	Primary classification	Secondary classification	Typical products or services
Industrial Internet security industry structure	Security products	Protection products	Firewall, network isolation equipment, anti-virus software, application whitelist, terminal intrusion detection, network intrusion detection, industrial security audit, etc.
		Management products	Asset management, patch management, identity authentication management, security operation and maintenance management, security compliance management, etc.
	Security service	Consulting services	Security assessment, security consulting, security audit, etc.
		Implementation services	Security integration, security reinforcement, etc.
		Operation services	Security emergency, security training, security custody, etc.

In terms of industrial Internet security products, the border and the terminal security protection of the protection products are the current main distribution patterns, which are relatively mature and have a large market share. With the formal implementation of cybersecurity level protection 2.0, protection products will become essential security measures in the overall industrial Internet security solution, and the market size will continue to grow steadily. In addition, although the market size of network inspection and industrial security audit products in protection products is small, they have developed rapidly. Among management products, products such as situational awareness, security compliance management, along with security operation and maintenance are important layout directions for security vendors. Under the dual promotion of national and industrial policies, the demand for compliance safety and endogenous safety of Chinese industrial enterprise users has increased, and the market size of such products will also grow steadily in the future.

In terms of industrial Internet security services, owing to the evolution of industrial cyber threats in the direction of diversification and complexity in recent years, it has been difficult for traditional single security product models to meet the security protection needs of users. Therefore, security services such as risk assessment, security management consulting, security emergency response, and security custody services have garnered increasing attention, and the demand for industrial Internet security assessment and security training is growing. Scientific research institutes, colleges, and universities have focused more on the training of industrial information security talents, thus promoting the rapid growth of the security training service market and further optimizing the industrial structure.

2.4 Continuous growth of the scale of the industrial Internet security industry

Effective security is inseparable from solid industry support. With the full implementation of China's industrial Internet strategy, the government and enterprises continue to increase security investment, and the industrial Internet security industry has ushered in a period of rapid growth (Fig. 2). In 2018, the market size of China's industrial Internet security industry was 9.46 billion yuan, and it is expected to reach 30.76 billion yuan in 2022, with an average annual compound growth rate of approximately 32.66% [9]. Under the joint effect of the policy environment and market demand, strengthening security will become the focus of future work. China's industrial Internet security industry has entered a new stage of rapid development.

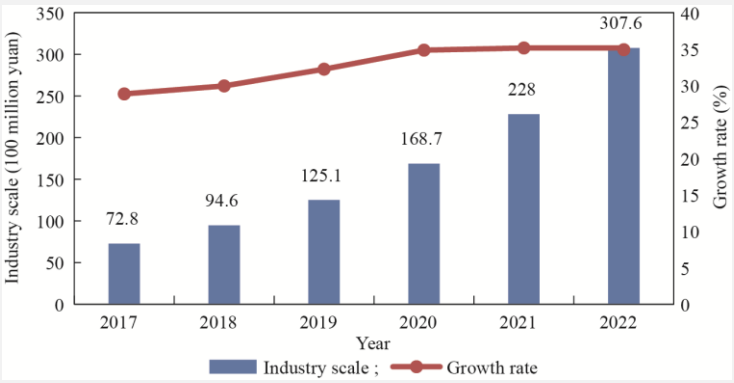

Fig. 2. China's 2017–2022 industrial Internet security industry market scale and forecast.

3 Development trend of China's industrial Internet security industry

3.1 Release of favorable industrial policies and the solid nature of industrial foundation

Industrial Internet security is not only an important guarantee for China to strength its manufacturing and network industries but also an important entry point for the implementation of the overall national security concept. Against the background of the accelerated development of new infrastructure such as 5G and the industrial Internet, coordinated development and security will become the main theme of the digital transformation of China's manufacturing industry in the new era. With the in-depth promotion of the industrial Internet strategy, China continues to strengthen policy and financial support, promote the growth of domestic demand in the industrial Internet security industry, guide enterprises to increase investment in security technology, and accelerate the development and industrialization of related security technology. With the continuous promotion of relevant national laws and policies, the industrial environment of the industrial Internet will continue to be optimized, the industrial foundation will become more solid, and the industrial agglomeration effect will gradually form.

DOI 10.15302/J-SSCAE-2021.02.007

3.2 Compliance demand as the main driving force to promote the development of industrial Internet security industry

Network security grade protection 2.0 expands the scope of network security protection, and it proposes higher security expansion requirements for industrial control systems to be suitable for proprietary technology and application of scenario characteristics of industrial control. Industrial enterprises must continue to strengthen their own security protection systems, further implement their main responsibilities, increase security investment, and strengthen systematic security planning and layout. It has been verified that the endogenous demand of the industrial Internet security industry will further expand [10].

3.3 Promotion of the in-depth integration of information technology (IT) security and operation technology (OT) security by the demand for industrial Internet security

Industrial Internet security is a field of integration of industrial production security and cyberspace security, covering the security of various elements and links in the process of digitization, networking, and intellectualization in the industrial field [11], which requires special security products, technologies, and services. At present, China's industrial Internet enterprises mostly use traditional network information security protection technology, focusing on the "outside-built" security protection products and solutions for industrial control systems. There is no special security protection equipment for the OT of the industrial Internet, and the overall security solution is not mature yet.

China's industrial Internet security technology system can be divided into two categories: external security (IT security) and embedded security (OT security). With the acceleration of the industrial Internet, the security problems from industrial control systems, industrial smart devices, industrial platforms, and data cannot be ignored, and the market demand for products and services with information security functions has increased rapidly. Traditional products and services based on IT security can no longer fully meet the actual market demand and should be fully integrated with OT security for in-depth development. Therefore, the future development of the industrial Internet security industry should consider the market demand for IT and OT security and improve the level of the comprehensive protection of industrial enterprises. In terms of special performance requirements, ensuring the continuity and reliability of production is the primary task of the industrial Internet. Network delay or higher-cost IT security solutions will not apply to OT networks, and technical solutions to balance security risks and business impacts need to be studied while considering the characteristics of OT networks [9,12].

3.4 Emergence of industrial Internet security solutions combining multiple disciplines and new technologies

With the rapid application of new-generation information technologies such as big data, cloud computing, artificial intelligence (AI), 5G, and edge computing in the industrial Internet field, the integration of IT and OT has accelerated. Moreover, the industrial Internet security environment that incorporates new technologies will become more complex and diverse and security risks will exhibit diversified characteristics; hidden security hazards will be more difficult to detect and the security situation will further intensify. This series of technological and situational changes has resulted in new requirements for security concepts and technologies, and it will promote new technologies such as security situation awareness, security visualization, threat intelligence, and big data processing to make continuous breakthroughs in the field of industrial Internet security [10]. This includes promoting the accelerated emergence of customized security products to meet the needs of customers for different product forms and performance; security services will be based on on-site services and supplemented by remote services, and it will shift to remote, cloud-based, automated, and platform-based development. Overall, industrial Internet security solutions that focus on the five major security areas—equipment, control, network, application, and data—and that combine multiple fields and new technologies will continue to emerge, providing a reference model for industrial enterprises to deploy security protection measures.

3.5 Promotion of the rapid development of the industrial Internet security industry through the localized replacement demand of security products

China's important industrial control systems mostly use foreign technology and equipment. This is a matter of concern in that the core technology is restricted by others. The industrial control system of a significant number of industrial enterprises relies on the operation and maintenance services provided by foreign manufacturers. The controllability of the operation of the system is relatively low and the lack of necessary supervision mechanisms

and technical testing measures for foreign products and services has certain potential safety hazards [10]. Industrial Internet security is related to economic development and social stability. Once important industrial data are stolen, tampered with, or destroyed, it poses a serious threat to national security. Frequent incidents of theft and attacks have further intensified the confrontation of various countries in the field of cyberspace security. It is, therefore, necessary to focus more on the independent controllability of information security products, raise the localization of information security products to the level of national security, and rely on independent innovation to actively develop information security products with independent intellectual property rights [13]. In recent years, under the promotion of the policy of localization of information products, a trend of the localization of information security products has emerged.

4 Challenges facing the development of China's industrial Internet security industry

With the transformation and upgrading of China's manufacturing industry to digitalization, networking, and intelligence, the threat of network security is spreading to the industrial field. China's industrial Internet security field still has an imperfect institutional mechanism, its level of comprehensive protection is low, its key core technology products are immature, it has a shortage of high-end technical personnels, and there is a serious security risk facing the industrial field [10]. In addition, with the development of new infrastructure construction, the number of objects that industrial systems need to protect has increased significantly, the attack surface of industrial systems has expanded, the protection requirements and difficulties have continuously improved, the fusion application of new technologies and industrial Internet has been accompanied by emerging security problems, and the sharing flow of data elements has aggravated the potential security risks. These new challenges have promoted the accelerated transformation of industrial Internet security technology products, and protection work has gradually shifted to dynamic coordination, which promotes the innovation of the security ecosystem [14].

4.1 Imperfect institutional mechanism of industrial development and the unclear responsibility of joint development

China has issued several top-level policy documents to guide the development of industrial Internet security. However, industrial enterprises in the actual implementation of security protection projects related to the design, construction, implementation, operation, and maintenance process still lack specific policy documents for overall guidance. In addition, security subject responsibility is unclear, among other issues. The industrial Internet security standards system has not been fully established, and there is a lack of both strict logical correlation between the relevant standards and key technology management standards. Further, the inability to provide a standards basis for enterprises to perform security protection work makes it difficult to meet the security needs of industrial development. Industrial Internet security is uniquely important in terms of guaranteeing target objects and security demands, and the diversity of protection scenes associated with industrial attributes poses a challenge to its own development. Therefore, there is an urgent need to establish a targeted and distinctive industrial Internet security system.

4.2 Non-smooth operation mechanism of protection construction and difficulty in improving the comprehensive guarantee capacity

At present, China's industrial Internet security construction is mostly based on the basic security needs of industrial enterprises, and it is in the initial stage of equipment procurement. On one hand, after completing the construction of industrial Internet security projects, users of industrial enterprises cannot achieve the maximum effect of security products because of the lack of relevant channels for continuous learning of industrial Internet security configuration along with the acquisition of equipment operation and maintenance knowledge. On the other hand, enterprise users cannot generally conduct quantitative assessment and evaluation of the effectiveness of security measures, and there are other problems such as the security system being empty and idler safety equipment.

4.3 Imperfect product service certification mechanism and the unbalanced scale of application progress

Although there are various types of industrial Internet security products and services, the corresponding market access and certification mechanisms are not perfect and there is a lack of testing certification standards and technology. This is because industrial Internet security has only garnered attention in recent years, and the relevant

DOI 10.15302/J-SSCAE-2021.02.007

standards are still in the process of development in which there is a certain degree of difficulty. The industrial Internet security industry is still in the initial stages of development, and it should not only adapt to the needs of current users but also have a certain foresight to guide and lead the development of such products. The demand for industrial Internet security products varies widely among industries and the environment, and various industrial control protocols also make it more difficult to develop standards. At this stage, the industrial Internet security products and services are detected using, primarily, traditional IT security testing certification standards and evaluation methods, which is clearly inappropriate. The unified standards and certification mechanisms of industrial Internet security products and services are evidently lacking, which makes it difficult to promote the relevant certification to the market timeously and to perform large-scale production and industrialization applications [15,4].

4.4 Lack of clarity on the clustering effect of industrial innovation and the immature development of key products

In terms of industrial agglomeration, China's industrial Internet began late and on a small scale. For instance, the scale of external security products and services accounts for less than 5% of the overall network security industry. There are approximately 266 companies engaged in industrial Internet security in China, and approximately 47 companies focus on this field. The scale of the companies is generally small; traditional information security, automation, and IT integration companies generally got into industrial Internet security a short time ago. These companies have insufficient technological innovation and lack core products with market competitiveness [15]. At present, China's security service companies have relatively high maturity in external protection product technology and low maturity in built-in information security industrial control technology. The company's security service capabilities cannot meet actual needs, and they do not have a basic leader to steer the development of the industry. For enterprises, the agglomeration effect of industrial innovation is not clear, and the overall scale of the industry is still low [4,13]. In terms of pivotal products, China's industrial Internet security, industrial technology, and industrial applications are still immature, both industrial software and hardware products are highly dependent on external sources, and unpredictable security risks have intensified [16].

Fig. 3 shows the technical maturity and application of China's industrial Internet security technology system. (1) In terms of external security protection, the maturity of protection technologies is advanced, and the market application level is also high, such as policy-based access control, network isolation, and application whitelisting. However, external security protection products are compatible in industrial scenarios, including the richness of protocol support, intelligence level, and visualization level. There is still a gap when compared with advanced foreign technologies in terms of detection and response technologies, such as fingerprint matching-based asset identification, vulnerability database-based risk correlation, and threat tracing. There are shortcomings and there is still a huge gap in the international Internet industry security companies. (2) In terms of embedded security protection, China has made certain breakthroughs in communication access control, communication and data encryption, and identification, but there is still a huge gap when compared with the international level due to the poor overall compatibility of the industrial system, insufficient price competitiveness, and other factors. Thus, the overall market application level is low.

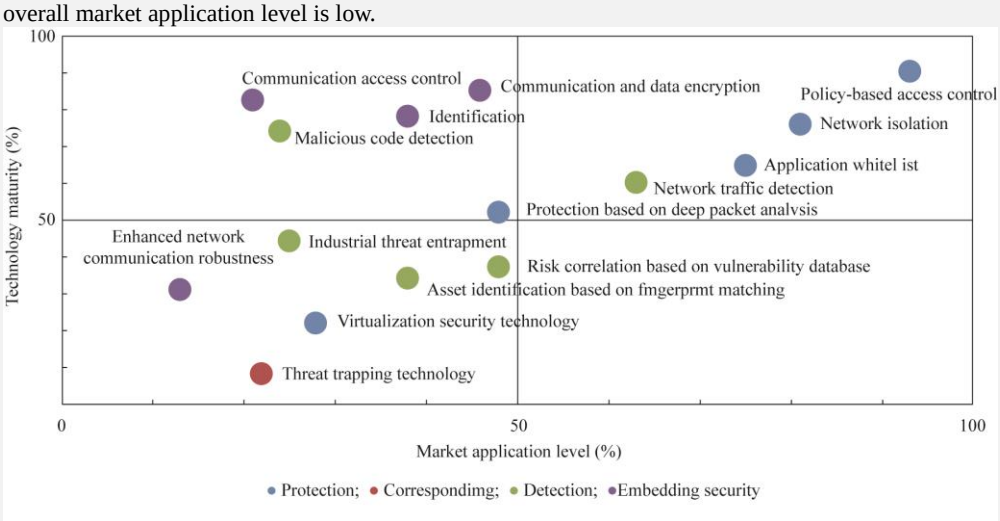

Fig. 3. Industrial Internet security technology maturity and application status.

4.5 Unreasonable layout of security personnel structure and insufficient core competitiveness of personnels

Network security is essentially a contest between offensive and defensive capabilities. The final analysis is a comparison of comprehensive capabilities among skilled personnels. As industrial Internet security risks become increasingly prominent, industrial enterprises urgently need to continuously improve their security capabilities. In addition to purchasing network security products to obtain security capabilities, they should also enhance their operation and maintenance capabilities by cultivating network security personnels and purchasing network security consulting services to compensate for the insufficient security capabilities. There is a large gap in China's network security personnel, and there is an urgent need for people with security protection compound talents, network security skills, and the ability to adapt to complex industrial scenarios. The imbalance of talent supply and demand has intensified talent competition among enterprises. Thus, the talent pool cannot meet the challenges of future development.

5 Proposals for the development of the new generation of industrial Internet security industry

5.1 Strengthening of policy guidance and support and the creation of a new development pattern of domestic and international dual-cycle mutual promotion

It is recommended to strengthen the construction and top-level design of the industrial Internet management system and to establish and improve laws and regulations. The implementation of policy guidance and support, continuous improvement of strategic measures for industrial development, and the formation of a long-term mechanism for sustainable development are also recommended. Further, strengthening the security protection concept of preventing problems before they happen, formulating security management policy systems and standards in emerging fields such as industrial big data and industrial cloud platforms promptly, and regulating and guiding the integration and application of new security technologies and the industrial Internet field should be considered [17]. The focus should be placed on the effect of policy implementation, strengthening the main responsibility of the safety of industrial enterprises, enhancing the awareness of protection, and creating a new industrial development pattern that takes the domestic cycle as the main body while the domestic and international double cycles promote each other.

5.2 Strengthening technological innovation and transformation and promoting technological innovation to become an endogenous driving force for industrial development

Technological innovation is the primary task during the 14th Five-Year Plan period. This is an important support for the construction of new infrastructure and the foundation of network security. It is recommended that the industrial Internet security industry adhere to the concept of innovative development, gradually establish a technical framework and standards based on independent intellectual property rights, complete the construction of an open ecosystem, and lay a solid foundation for the healthy development of the industry.

To strengthen systematic technological innovation capabilities, we should develop a national industrial Internet security guarantee system, target the commanding heights of industrial development, guide the release of technical innovation guidelines in crucial areas, address the bottlenecks and shortcomings in technical fields, such as asset identification, risk management, and emergency response, and guide market players' innovation breakthroughs. We should continuously explore solutions for industrial Internet security innovation and integration applications and encourage security companies to actively explore and apply big data, AI, 5G, blockchain, and other emerging technologies to solve industrial Internet security issues, form typical solutions, and deploy these solutions for industrial enterprises.

China should promote the research and development of industrial Internet security technology products and set up the enterprise-led industry–university–research–application joint innovation mechanism aimed at the basic technology of industrial Internet security, common key technology, and cutting-edge technology, along with information security system solutions and core links in key industrial fields. It should study the integrated application of emerging Internet security technology in the industrial field and facilitate the breakthrough of several key core technologies as soon as possible. It should also strengthen collaborative research, eliminate bottlenecks, fan out from point to area, make up for weaknesses, and push forward together. We should focus on developing several high-end products to form a product system with market competitiveness, actively promote the transformation and transaction of core technological achievements, strengthen the protection and management of

DOI 10.15302/J-SSCAE-2021.02.007

intellectual property rights, promote the transformation of innovative achievements, and constantly improve the integration ability of innovation, industrial, and value chains.

5.3 Guidance of relevant enterprises and institutions to complement each other's advantages and construction of a good ecology of industrial development

Cross-border cooperation is an effective way to handle cross-domain security issues. With an increasing amount of industrial equipment networking, it is difficult for enterprises to defend themselves against potential industrial Internet security risks using their own strengths only. It needs the complementary advantages and close cooperation of government departments, scientific research institutions, security service providers, industrial enterprises, and industrial control equipment providers, aiming at the characteristics of various relevant industries, to construct a multi-dimensional network. We need to construct a multi-level defense mechanism to jointly handle security threats and challenges from various fields and construct a good industrial ecosystem for coordinated development [12,13].

China should strengthen industrial policy preferences and encourage in-depth cooperation among industrial control system manufacturing, industrial, and network security enterprises. Relevant policies should be formulated to promote cooperation, encourage relevant enterprises of industrial Internet to focus on the industry's pain points according to the production and operation characteristics of various industries, combine technological breakthroughs, model innovation, and the actual needs of the industry, and gradually form a benign industrial ecology with government guidance, user guidance, manufacturer participation, and capital promotion.

China should focus on tackling key problems in key industries such as energy and transport, integrate the resources of "government, industry, university, research, and application," maximize the institutional advantages of concentrating on major tasks, form a system for tackling key core technologies, cooperate in the research and development of high-end security products and solutions, and establish a national industrial Internet security enterprise. Guided by problems, China should speed up the establishment of a system of key common technologies, lay out technical weaknesses and the next generation of cutting-edge technologies, and make breakthroughs as soon as possible to address key core technology bottlenecks and ensure self-control.

China should focus on the cultivation of leading enterprises and guiding the continuous reform of safety manufacturers' new business models, strengthening the integration of network security resources, multi-industry cooperation, and accelerating the construction of industrial ecology. The reconfiguration of production based on the user needs industry chain, the industrial Internet security industry chain, and upstream and downstream enterprises should work together to accelerate the pace of capital integration and strategic cooperation. China should focus on the construction of an open network security ecology, radiating security capabilities to more partners and practicing the development concept of win-win cooperation.

We should optimize the industrial ecological environment, give full play to the guiding and supporting role of government management departments and industry associations, and broaden the channels for enterprises toward technology introduction, investment and financing, along with talent introduction. We propose that laws, regulations, policies, and standards on the information security of industrial enterprises should be implemented speedily, the security needs of enterprises should be considered, and market vitality should be stimulated. It is also important to coordinate basic research, technological innovation, and application deployment and enhance the collaborative interaction effect between upstream technology R&D and downstream promotion and application to construct a collaborative industrial ecosystem.

5.4 Maintenance of the security and stability of the supply chain, strengthening the coordination, joint assessment, risk early warning, and other mechanisms

In recent years, with the upsurge of counter globalization and the outbreak of COVID-19, the uncertainty of the global supply chain has intensified further. Against the background of increasingly fierce games among big countries and intensified competition among advanced technology industries, it is imperative to strengthen supply chain safety supervision and establish a comprehensive supply chain safety management system.

China should strengthen top-level design, integrate supply chain security into the overall framework of national security, formulate policies and regulations on supply chain security management, and speed up the introduction of strategic planning in the field of industrial Internet supply chain security. It should strengthen implementation; form a scientific, standardized, and effective system; promote the development of supply chain safety management standards for specialization and refinement; and provide a basis for relevant departments and institutions to

identify, evaluate, and reduce supply chain risks.

It is necessary to strengthen the risk identification and assessment of the global supply chain system, establish an entire lifecycle supply chain risk management system, form a management system of information tracking, risk identification, and crisis response, and improve the prevention and control ability of global supply chain risks.

China should perform supply chain security assessment and review, address the key weak links in the industrial field, and perform risk early warning and risk control for the industrial basic supply chain in key areas. It should also create a supply chain risk assessment sharing service, strengthen the review and supervision, and establish an adaptable, sustainable, and safe supply chain.

5.5 Strengthening personnel training and team building and establishing a cross-border safety personnel training system

The government, colleges and universities, scientific research institutes, industrial enterprises, and security enterprises are encouraged to cooperate to strengthen collaboration, jointly develop industrial Internet security discipline, cultivate professional talents, and promote the organic combination of industry, post, and teaching chains in this field. We should develop ways to integrate advantageous resources and construct professional laboratories, characteristic curriculum systems, and practice training bases. In addition, we should maintain the organic combination of theoretical learning and practice, comprehensively improve the level of industrial Internet security discipline, and cultivate high-level talents with application possibility in the field of industrial Internet security in batches. For instance, security enterprises and industrial enterprises can jointly set up industrial control security testbeds and network ranges to enable students to perform virtual confrontations and improve their combat effectiveness and operability. We should also support and encourage enterprises engaged in industrial Internet security to set up relevant education and training institutions. There is a large gap in industrial Internet security talent in China, especially defensive talents. Large-scale vocational training and education through social forces is an effective way to quickly compensate for the shortage of talent. We should strengthen financial support, set up a special talent training fund, and actively cultivate high-end talent relying on key innovative topics.

References

[1] Ministry of Industry and Information Technology of the People's Republic of China. Policy interpretation on *Notice of the General Office of the Ministry of Industry and Information Technology on accelerating the development of the industrial Internet* [EB/OL]. (2020-03-21) [2021-01-05]. http://www.gov.cn/zhengce/2020-03/21/content_5493935.htm. Chinese.

[2] Editor of China Information Security. An enterprise perspective and practice on industrial Internet industry security [J]. China Information Security, 2019 (6): 66–77. Chinese.

[3] Alliance of Industrial Internet. Industrial Internet security framework [R]. Beijing: Alliance of Industrial Internet, 2018. Chinese.

[4] Prospective Industry Research Institute. 2018 industrial information security industry market status and development trend analysis, technology improvement is the key [EB/OL]. (2019-04-23) [2021-01-08]. https://www.qianzhan.com/analyst/detail/220/190422-71978700.html. Chinese.

[5] Yao Y. Industrial Internet innovation development needs to strength the cyber security [EB/OL]. (2021-02-06) [2021-02-08]. https://www.china-aii.com/index.php?m=content&c=index&a=-show&catid=29&id=41. Chinese.

[6] Network Security Administration. Interpretation of *The guidance on strengthening industrial Internet security* [J]. China Informatization, 2019 (9): 19–20. Chinese.

[7] National Industrial Security Industry Alliance. White paper on industrial information security standardization (2019 edition) [R]. Beijing: National Industrial Security Industry Alliance, 2019. Chinese.

[8] National Industrial Security Industry Alliance. White paper on industrial information security standardization (2017 Edition) [R]. Beijing: National Industrial Security Industry Alliance, 2018. Chinese.

[9] Alliance of Industrial Internet. China industrial Internet security situation report (2019) [R]. Beijing: Alliance of Industrial Internet, 2020. Chinese.

[10] National Industrial Security Industry Alliance. White paper on industrial information security situation (2017) [R]. Beijing: National Industrial Security Industry Alliance, 2019. Chinese.

[11] China Cybersecurity Industry Alliance. China network security industry analysis report (2020) [R]. Beijing: China Cybersecurity Industry Alliance, 2020. Chinese.

[12] Kang S Y, Hu W L. Research on industrial Internet security technology and analysis of China's industrial internet security industry development [J]. Secret Science and Technology, 2020 (5): 27–31. Chinese.

[13] National Industrial Security Industry Alliance. White paper on industrial information security standardization (2019—2020)

DOI 10.15302/J-SSCAE-2021.02.007

[R]. Beijing: National Industrial Security Industry Alliance, 2020. Chinese.

[14] China Academy of Information and Communication Technology, Alliance of Industrial Internet. Overview of the industrial Internet security situation in the first half of 2020 [R]. Beijing: China Academy of Information and Communication Technology, Alliance of Industrial Internet, 2020. Chinese.

[15] National Industrial Security Industry Alliance. White paper on industrial information security standardization (2018—2019) [R]. Beijing: National Industrial Security Industry Alliance, 2019. Chinese.

[16] Information Policy Institute of China Industrial Control Systems Cyber Emergency Response Team. Analysis of the industrial information security situation in 2018 [R]. Beijing: Information Policy Institute of China Industrial Control Systems Cyber Emergency Response Team, 2019. Chinese.

[17] Wang L J. Strengthen the construction of industrial information security and escort the work of the Belt and Road [J]. China Informatization, 2019 (4): 8–10. Chinese.