DOI 10.15302/J-SSCAE-2021.02.015

Layout of Foreign Industrial Internet Security Industry and Its Enlightenment to China

Li Yangchun [1], Wang Hailong [1], Li Yuxiao [1], Chen Lei [2], Li Youping [3]

1. Chinese Academy of Cyberspace Studies, Beijing 100010, China
2. Center for Strategic Studies, Chinese Academy of Engineering, Beijing 100088, China
3. School of Computer Science and Engineering, Southeast University, Nanjing 211189, China

Abstract: The field of industrial Internet security is crucial for the healthy development of the industrial Internet. The layout of this industry in developed countries and regions is almost perfect; however, it requires optimization in China to strengthen the manufacturing, cyberspace, and digital sectors. This study investigates the development demands of the industrial Internet security industry using literature research and intelligence analysis. Subsequently, the current status of the layout in the United States, Germany, the United Kingdom, Japan, and other developed countries is studied from the perspectives of policy guidance, enterprise innovation, collaborative development, capital integration, and alliance ecology. On this basis, the international development trends are analyzed. Moreover, the current status and challenges faced by China are discussed in terms of the policies and standards, technology and products, market space, investment and financing, and regional layout. It is noted that the optimization of the industrial Internet security industry layout in China should draw on the useful experience of other countries. It is suggested that China maximize the advantages of its systems and mechanisms to coordinate the development of the security industry, adhere to independent innovation to create an internationally competitive brand, improve the security standards system to lead international rule making actively, strengthen the policies and financial support for small- and medium-sized enterprises to stimulate their innovation vitality, and build a collaborative development ecology to create an international and domestic dual circulation development pattern.

Keywords: industrial Internet security; industrial Internet security industry; industrial layout; balanced development; independent innovation

1 Introduction

A new round of global technological revolution and industrial transformation for in-depth development is underway at present. New-generation information technologies such as cloud computing, big data, fifth-generation mobile communications (5G), artificial intelligence (AI), and the Internet of Things (IoT) are rapidly being integrated into numerous fields, including energy, electricity, communications, chemistry, aviation, aeronautics, machinery, and automobile manufacturing. The industrial Internet is the key support as well as the focus of competition in the Fourth Industrial Revolution. In the form of critical integrated infrastructure through the secure interconnectivity and integration of humans, machines, materials, data, and applications, the industrial Internet aids in improving the level of digitalization, networking, and smartization of industries. Moreover, it is used to construct a novel manufacturing and service system that encompasses all factors, the entire industrial chain, and the entire value chain. In this sense, it has become a key path for promoting the deep integration of the digital and real economy, as well as a common option for the high-quality development of major economies [1].

As the scope of the industrial Internet continues to expand, the traditionally closed industrial manufacturing

Received date: January 15, 2021; **Revised date:** March 14, 2021

Corresponding author: Wang Hailong, senior engineer of Chinese Academy of Cyberspace Studies. Major research fields include cyber and information security, and industrial Internet security. E-mail: whl2000721@126.com

Funding program: CAE Advisory Project “Strategic Research on the Next-Generation Industrial Internet Security Technology” (2020-XZ-02)

Chinese version: Strategic Study of CAE 2021, 23(2): 112–121

Cited item: Li Yangchun et al. Layout of Foreign Industrial Internet Security Industry and Its Enlightenment to China. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2021.02.015

environment has been disrupted and endogenous security coexists with external risks. This makes the industrial Internet security issue ever more complex and creates disruptive challenges to existing security protection systems, product technical architectures, and coping solutions. Numerous countries and regions attach great importance to industrial Internet security and have actively implemented relevant measures to optimize and improve the development environment of the industrial Internet security industry. China, which boasts the most complete industrial system in the world, has experienced rapid transformation in industrial digitalization in recent years. With reference to the development experience and successful models of the industrial Internet powers globally, it is of great practical importance and far-reaching historical significance to analyze the risks and threats faced by China in related industries. This will enable the current dilemma in industrial Internet security to be solved, an industrial Internet security industry system that adapts to the cyberspace governance of China to be established, and the strategic construction of a manufacturing power, cyberpower, and digital China to be promoted.

Most available research has analyzed the development status of domestic and foreign technologies of industrial Internet security and existing security risks [2–8], with a focus on the enlightenment to China from security measures implemented for certain single initiatives such as the industrial Internet initiative of the United States (US) and Industry 4.0 strategy of Germany [9–14]. Nevertheless, systematic analyses and horizontal comparative research regarding the layout of security industries in several countries/regions have rarely been conducted. Based on a literature review, expert discussion, and program research, this study considers the layout of the foreign industrial Internet security industry as a starting point, probes and draws conclusions on the development demand of the industrial Internet security industry, and investigates the status quo and characteristics of the industrial layout in several developed countries in detail. Furthermore, through a horizontal comparison, assessment, and analysis of international development tendencies, as well as an overall consideration of the national realities and current challenges of China, suggestions are provided for optimizing the layout of the industrial Internet security industry in China.

2 Development demands of industrial Internet security industry

2.1 International competition

In recent years, there has been a high incidence of disorder and imbalance in international community development, which is a situation that has been further exacerbated by superpower politics and the COVID-19 pandemic. In this context, the industrial Internet has become an important approach for certain developed countries to contain the development of other countries and to coerce them into compliance through cyberattacks, thereby resulting in serious threats and huge losses to international order, national security and stability, economic development, and public life. For example, in 2018, the customer messaging systems of four natural gas pipeline companies were attacked and closed down for several hours; in 2019, Norsk Hydro, which was also a victim of cyberattacks, experienced production disruption and plant closure; in 2020, the trunk lines of the national grid of Venezuela were attacked, which resulted in a nationwide power outage; and since the emergence of COVID-19, in the first half of 2020 alone, as many as 1.356×10^5 million malicious cyberattacks on the industrial Internet of China have been detected, affecting 2039 businesses [15]. Thus, there is an urgent need to accelerate the development of the industrial Internet security industry to provide effective and reliable security protection and guarantees, thereby underpinning cooperation and competition among nations.

2.2 Technology convergence

The construction of the industrial Internet continues to expand in both depth and breadth. Although it helps to link the internal and external networks of businesses and realizes the convergence of information and operation technologies (IT and OT), it greatly increases the risk exposure of closed, exclusive industrial control systems (ICSs) with unknown hidden hazards. Furthermore, as IT systems are insecure and the integration problems in the connection of IT systems with ICSs remain to be addressed, the probability of cyberattacks on the industrial Internet is further increased. According to a report released by Dragos, which is an industrial control security company, in February 2020, among the 438 flaws that were disclosed in 2019, 77% of vulnerabilities were considered to be deep within a control system network, whereas over 50% could have led to both a loss of view (i.e., the inability to monitor or read the system state) or loss of control (i.e., the inability to modify the system state) [16]. Guarantees can be provided to tackle the aforementioned security technology problems only by consolidating the foundations of the industrial Internet security industry and enhancing technology convergence.

DOI 10.15302/J-SSCAE-2021.02.015

2.3 Market expansion

The global industrial information security market was valued at USD 16.401 billion in 2019 and it is expected to reach USD 29.76 billion in 2026. Global expenditure on security stood at approximately USD 380 million with an annual growth rate of 52% in 2019 and the market value is expected to reach USD 3.531 billion by 2025. As the number of industrial Internet facilities rapidly increases and the hidden hazards to security continue to be exposed, the demand for security protection solutions will increase. In the future, the market for industrial Internet security products and services is expected to become the fastest growing segment, which will subsequently drive the development of the entire cybersecurity industry and expand the market further.

3 Current layout of foreign industrial Internet security industries

Industrial powers such as the US, Germany, and the United Kingdom (UK) have obvious industrial advantages in industrial Internet security, whereas countries including China, Japan, and South Korea are also accelerating the process of informatization and industrialization with greater investment in the field. The status and characteristics of the industrial Internet security industry layout in major countries and regions are investigated according to the following five aspects.

3.1 Formulation of strategic security policies to lead industrial development

3.1.1 US

To gain global competitive advantages in the manufacturing industry, the US officially launched the Advanced Manufacturing Partnership (AMP) in 2011 to facilitate the formation of joint efforts among the government, academia, and industry. Joint investment in new-generation IT is encouraged to manufacture high-standard American products and to secure the leading position of the country in global manufacturing development. In October 2018, based on the AMP, the US introduced the Strategy for American Leadership in Advanced Manufacturing, which incorporated manufacturing cybersecurity as an important focus of strategic implementation and the orientation of industrial layout. A series of security policies and standards were released to ensure the secure and orderly development of the industrial Internet industry. In November 2018, the US established the Cybersecurity and Infrastructure Security Agency (CISA). The CISA, which is responsible for cyber and infrastructure security, prioritizes industrial control security. Together with the Department of Energy and other government agencies, the CISA focuses on cooperation with industry and strengthens the construction of information security in the industry and energy fields. Meanwhile, the US continues to propose sound legislation in industrial Internet security to provide legal support for the development of the security industry. In 2019, the *Internet of Things Cybersecurity Improvement Act*, *Securing Energy Infrastructure Act*, *Protecting Resources on the Electric Grid with Cybersecurity Technology Act*, and *Cyber Supply Chain Risk Management Guidance* were adopted [18], which provided an overall guarantee for the information security of critical infrastructure such as the IoT, energy, electricity, and medical care.

3.1.2 European Union

The European Union (EU) emphasizes strengthening the integration of cybersecurity resources and the promotion of multi-party collaboration in the industry. *Industry 4.0 Cybersecurity: Challenges and Recommendations*, which was released by the European Union Agency for Cybersecurity (ENISA), presented seven main challenges to the security of industrial IoT [19], on which basis the ENISA has directed the practices of industrial information security to lay foundations for the development of Industry 4.0 in the EU. Moreover, the EU established a network of computer security incident response teams (CSIRTs) to oversee information collection and sharing, the analysis of responses to industrial control security emergencies, the analysis of industrial security situations, and the coordinated implementation of plans to protect critical infrastructure. The EU also released a series of laws, regulations, and strategic documents, including the *Strategy for a Secure Information Society*, *National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace*, *EU Cybersecurity Strategy*, *Policy on Critical Information Infrastructure Protection*, *Directive on Security of Network and Information Systems*, and *General Data Protection Regulation* [2].

As a traditional manufacturing powerhouse, Germany has vigorously promoted its Industry 4.0 strategy at the national level, with the aim of improving industrial efficiency in a digitalized, network-based, and intelligent manner, thereby consolidating its leading position in the global manufacturing industry. In 2015, the German government led a program with associations and enterprises to launch the construction of an upgraded Industry 4.0 platform, which

included data security as one of the five themes. They successively released guiding documents including the *Industry 4.0 Security Guidelines*, *IT Security in Industry 4.0*, *Cross-Enterprise Secure Messaging*, and *Indicators of Secure Identity* [20,21], through which the hierarchical security management concept that was centered on the cyber-physical system platform was proposed. The German Federal Office for Information Security issued several recommendation papers on ensuring industrial control security, including the *Industrial Control System Security: Top 10 Threats and Countermeasures 2019*, to guide enterprises specifically to perform their role in industrial information security protection effectively.

3.1.3 Japan

In 2016, Japan proposed the concept of a super-smart society known as Society 5.0, which is rooted in AI technologies and provides personalized products and services as the core, with "connected industries' as an important part of the initiative. In the same year, the Industrial Cybersecurity Promotion Agency was established, specifically for defense against cyberattacks on critical infrastructure. In April 2019, the Ministry of Economy, Trade and Industry released the *Cyber/Physical Security Framework* together with a series of supporting action plans to ensure the overall security of the new supply chain and to determine the security countermeasures required for the industry comprehensively. Furthermore, Japan has proactively implemented several supporting action plans to strengthen the cybersecurity of supply chains, improve operations for cybersecurity, train security talents, and build an ecosystem for security businesses.

3.1.4 South Korea

In 2019, South Korea unveiled the *National Cybersecurity Basic Plan*. As required, the government will work to improve network repair and survivability, guide the optimization of the security environment for communication networks and information infrastructure, and intensify the R&D and promotion of new-generation security infrastructure for the effective improvement of the security of critical infrastructure. Furthermore, the Korean government has proposed the promotion of talent training, the organization of R&D activities, and the construction of an innovative ecosystem for the security industry.

3.2 Participation in security market competition for partner diversification

Market demand motivates more businesses to enter the industrial Internet security industry. Automation and traditional security companies as well as emerging industrial Internet security start-ups are now players in the field. Relevant businesses in the US, Germany, the UK, Japan, and other countries have participated in market competition through acquisitions, partnerships, and the development of cybersecurity businesses.

Automation companies, including Siemens AG, General Electric Company, Honeywell International Inc., and Schneider Electric Co., Ltd. have relied on their industrial market base to acquire or partner with cybersecurity businesses and to establish professional teams for the development of security products. These companies have strengthened cybersecurity guarantees for their own products and facilities, and have improved the credibility of their products and services, while expanding into the industrial security market by providing industrial Internet security products and services.

Traditional cybersecurity companies offer advantages in security technologies and are seasoned in the development of industrial Internet security products and services. However, as they lack an understanding of the industrial interconnectivity environment, they experience problems in integrating cybersecurity with functional safety, and thus, they cannot provide products that meet the security demands of industrial companies. Therefore, through acquisition or cooperation, companies can leverage their respective advantages to solve the bottleneck problems of the industrial information security guarantee.

Start-ups in the field of industrial Internet security, which are represented by Claroty, Dragos, and Nozomi, provide innovative technologies that can lead to the development of the industrial Internet security industry, as well as offer dual advantages in cybersecurity and industrial control. Although they lag far behind giant players in terms of scale, they have been drawing increasing attention from the capital market as independent industrial Internet security providers. Since 2011, more than 230 local or foreign institutions have invested in 165 Israeli cyber technology start-ups [22]. In June 2020, the Microsoft Corporation of the US acquired CyberX, which is an Israeli industrial cybersecurity start-up, for USD 165 million [23].

DOI 10.15302/J-SSCAE-2021.02.015

3.3 Bolstering development of small- and medium-sized enterprises for synergy of security guarantee

To promote factory smartization and the application of IoT in the manufacturing industry, Japan established the Smart Manufacturing Campaign Group to extend support for small- and medium-sized enterprises (SMEs) in terms of technologies, tools, and personnel. Furthermore, Japan offers proactive guidance in promoting the internationalization of standards, developing manufacture-oriented cybersecurity, training digital talent, and ramping up R&D investment.

South Korea formulated the Manufacturing Innovation 3.0 strategy to support the growth of SMEs with policies, capital, and technologies. The government strengthens financial support for SMEs with preferential interest rates and convenient loan services, thereby encouraging them to focus on the R&D of security products. Moreover, it advocates the sharing of R&D outcomes between large enterprises and SMEs, in a bid to create a favorable landscape for the collaborative development of industrial Internet enterprises.

With the aim of improving the R&D capabilities of SMEs, Germany deployed and initiated projects that were targeted at partnerships among SMEs and research institutions. In most cases, R&D institutions in Germany have different testing environments. By cooperating with these institutions, SMEs can receive support in terms of software, hardware, and technologies, as well as strengthen the training of their own employees in related fields. Moreover, SMEs can obtain subsidies directly from the government for their research into production automation, smart sensors, and other technologies.

In the US, focus has been placed on strengthening education and training for the labor force of SMEs. In 2019, the US Department of Defense allocated USD 10 million to manufacturing x digital (MxD) to train small- and medium-sized manufacturers with lower service levels to increase the use of financial models and easy-to-use tools, and for the creation of a more resilient industrial system. In particular, MxD implements the pilots of cybersecurity tools and carries out Jobs Taxonomy 2.0 to aid employees in analyzing specific job roles in-depth, organizing digital expertise workshops to promote digital identification programs, providing opportunities for technical internship, and conducting industrial IoT training to fuel the IoT-based manufacturing of SMEs.

3.4 Intensifying investment and financing to bolster basic innovation

In recent years, industrial Internet security start-ups have been increasingly favored by the capital market and cybersecurity enterprises. From 2017 to 2019, financing from industrial Internet security enterprises in the US, Israel, and France exceeded USD 340 million [17, 21]. In its continued efforts to increase investment in the industrial information security field, the US allocated a federal budget of approximately USD 11 billion for cybersecurity purposes in 2020. The budget for the industrial control security of the US Department of Homeland Security was mainly used to strengthen industrial control security training, malware analysis, vulnerability analysis of industrial control systems, incident response, and security assessment of emerging industries and industrial segments. The US Department of Energy provided a new budget of USD 156 million for cybersecurity, energy security, and emergency response to bolster preliminary research projects on power grid security and resilience. In February 2019, the EU announced that it would invest EUR 63.5 million into the Horizon 2020 program and launch a cybersecurity capacity building program, thereby injecting greater vitality into cybersecurity development in the industrial sector [17].

3.5 Promotion of standardization with industrial consortiums to build an international ecosystem for the development of industrial Internet security

Industrial alliance organizations such as the German Commission for Electrotechnical, Electronic & Information Technologies of DIN and VDE (DKE), the Industrial Internet Consortium (IIC) and the National Institute of Standards and Technology (NIST) of the US, and the Industrial Value Chain Initiative (IVI) of Japan have made proactive arrangements and promoted standardization in the industrial Internet security field [6].

In 2016, the IIC released the Industrial Internet Security Architecture, with the aim of standardizing corporate planning and practice in the security protection field. A series of security-related documents, including the *IoT Security Maturity Model (SMM): Practitioner's Guide*, *Endpoint Security Best Practices*, *Data Protection Best Practices*, and *Managing and Assessing Trustworthiness for IIoT in Practice*, were successively released [18], which guided research into and the practice of industrial Internet security. Furthermore, the consortium continues to strengthen collaboration with the International Organization for Standardization, open-source organizations, and standards development agencies to promote the conversion of research outcomes into unified standards. The NIST has issued *Capabilities Assessment for Securing Manufacturing Industrial Control Systems*, *Guide to Industrial*

Control Systems (ICS) Security, and several other documents, with the aim of leading the formulation of standards for secure industrial control systems.

The DKE introduced the *German Standardization Roadmap Industry 4.0* to make overall arrangements for the standardization work of Industry 4.0. With the support of the German government, the German Academy of Engineering Sciences, the Fraunhofer Society, Siemens, and other entities jointly established the Industry 4.0 Platform to accelerate the industrial layout regarding the security, architecture, roadmap, and other key factors of Industry 4.0 in the country. With security as one of the three important themes for the advancement of Industry 4.0, *IT Security in Industry 4.0* was released for the reinforcement and enhancement of equipment and system security. These entities targeted the key common problems in architecture, standards, security, and test beds to accelerate technical and industrial collaboration with the IIC.

The IVI of Japan was designed to create an open and secure manufacturing ecosystem led by a consortium of enterprises. It released the *Strategic Implementation Framework of Industrial Value Chain for Connected Industries*, in which a reference framework for the new-generation industrial Internet was proposed. The framework has become a top-level guide for industrial Internet development in Japan.

In summary, based on their own industrial level and the current state of IT development, countries such as the US, Germany, the UK, Japan, and South Korea have assigned different priorities in the layout of the industrial Internet security industry (Table 1). In terms of policymaking, developed countries or regions represented by the US and Germany occupy a dominant position. By continuously strengthening relevant legislation on industrial Internet security, the US, which exhibits obvious advantages in Internet technologies, focuses on improving legal protection and strategic guidance for industrial development. As the prime mover of Industry 4.0, Germany pays more attention to the construction of management systems for industrial information security, and arranges the construction of industrial control security in a coordinated manner, with the government taking the leading role. In contrast, other countries, which are relatively weak in terms of policies specifically designed for the industrial Internet security industry, focus more on the development of the industrial Internet at the current stage. In terms of corporate development, the US considers industrial Internet security as an important direction in the development of traditional security and industrial enterprises, whereas manufacturers in Germany, the UK, and other countries promote the development of the cybersecurity businesses of industrial enterprises through acquisitions and partnerships. In terms of supporting SMEs, Japan and South Korea invest even more vigorously in capital, and encourage SMEs to improve their innovation capabilities for rapid development by increasing the inputs into these enterprises. In terms of capital investment, the US and the EU continue to increase inputs into industrial information security. In terms of industry alliances, the US and Germany have established special industrial Internet industry alliances featuring numerous member entities, extensive international cooperation, and influence and disclosure power globally.

Table 1. Comparison of layout of industrial Internet security industry in major countries.

Country	Completeness of policies and standards	International competitiveness of leading enterprises	Level of support for SMEs	Level of capital input	Level of global influence of industry alliances
US	High	High	High	High	High
Germany	High	High	High	High	High
France	Medium	High	Medium	Low	Low
UK	Medium	Low	Medium	Low	Low
Japan	Medium	Medium	High	Medium	Medium
South Korea	Low	Low	High	Low	Low

4 Development trends of foreign industrial Internet security industry

4.1 Predominant role of government

Governments are faced with severe and complicated international situations such as geopolitical collision, technological competition, and manufacturing transfer, particularly as the industrial Internet has become an important aspect of national security. Thus, various governments are planning to enact and implement a series of strategic policies and relevant standards to play a predominant role in the industry, secure highlands in industrial Internet security, and ensure the international status and power of discourse of the country in the global economy.

DOI 10.15302/J-SSCAE-2021.02.015

4.2 Overall involvement of concerned enterprises

Both multinational technology enterprises that are represented by Internet enterprises and more traditional business tycoons that are represented by manufacturers have become aware of the promising market prospects of industrial Internet security in the transition from consumer Internet to industrial Internet. These enterprises are accelerating the entrance into the industrial Internet industry by means of acquisition, merging, and investment to consolidate innovation resources and integrate product services further. Meanwhile, the continuous development of the industrial Internet security industry has created a relatively favorable environment for the development and innovation of SMEs.

4.3 Increased visibility of technological convergence

The industrial Internet is being developed alongside emerging technologies such as 5G, AI, and the IoT. It is necessary to solve security problems that are posed by such emerging technologies while making use thereof to address security challenges for the development of the industrial Internet security industry. Hence, the fusion of technologies is expected to boost the innovative development of the security industry. Furthermore, the industrial Internet will continue to be integrated into many major fields of application, such as energy, electricity, transportation, aviation, and aeronautics, with the continual emergence of new technologies, products, services, and startup enterprises targeting specific industries.

4.4 Gradual unification of security standards

The trend of industrial globalization is increasingly apparent in the digital age. Data and service mobility are important aspects of industrial capacity. Unified security standards will be a prerequisite and safeguard to address the difficulties of integrating information security, IT and manufacturing technologies that are caused by the incompatibility among their principles, interfaces, and data structures, thereby attaining the capacity for industrial Internet to serve the world. In this sense, a framework of unified international security standards that encompass standard construction, development, integration, and operation is key to solving the problem.

5 Status quo of industrial Internet security industry in China

5.1 Strengthening top-level design to guide industrial development

In China, the industrial Internet security industry has exhibited comprehensive growth, with policies and standards increasingly being refined, information security construction in the vertical industry accelerating, security awareness of industrial enterprises generally being enhanced, and technologies safeguarding industrial information security being significantly improved. In 2017, the *Guidelines of the State Council on Deepening "Internet Plus Advanced Manufacturing Industry" to Develop the Industrial Internet* was released, with explicit requirements for improvement of the security protection capability, the establishment of a data security protection system, and the accelerated development of security technologies. In 2019, the industrial information security industry of China maintained a momentum of rapid growth in scale, with the industrial volume reaching RMB 3.83 billion, which was an increase of 51.62% year on year [17]. In 2020, the competent authorities of industrial information security and industry regulators issued the *Notice on Accelerating the Development of Industrial Internet* and the *Action Plan on "Industrial Internet Plus Secure Production" (2021–2023)* in addition to many other policies relating to industrial Internet security to guide security work.

5.2 Boosting innovation in technological products for greater industrial scale

Industrial Internet security products are becoming increasingly systematic, represented by border protection, terminal protection, monitoring and auditing, as well as increasingly diversified, with enhanced performance. New security products based on AI, big data, and commercial passwords are also undergoing accelerated R&D [24]. The major market players in the industrial Internet security industry of China include large automation enterprises, traditional integrated cybersecurity enterprises, and security startups that specialize in industrial control security. In the industrial automation field, since around 2009, companies such as Qingdao Moses Process Control Technology Co., Ltd., Beijing ForceCon Yuantong Technology Co., Ltd., and Hollysys Technology Group Co., Ltd. have expanded their business to industrial Internet security, carrying out the R&D and application promotion of industrial Internet security products. In recent years, numerous startups specializing in industrial Internet security have

emerged, such as Beijing Winicssec Technology Co., Ltd., Changyang Technology (Beijing) Co., Ltd., and Beijing Andian Science & Technology Co., Ltd. By leveraging their talent advantage in cybersecurity and industrial control, the main focus of the businesses is industrial Internet security. These companies have attracted international customers in the fields of energy, manufacturing, chemistry, and others and they continue to lead the development of the entire industry with technological innovation.

5.3 Enriching application scenarios for a larger market

Industrial Internet platforms have become an important support for industrial enterprises to construct new models, introduce new business formats, and foster growth momentum through network-based collaboration, scale customization, and service-oriented manufacturing. The market for industrial Internet security is shifting from product-oriented businesses featuring protection and management to service-oriented businesses that are represented by assessment and training. At present, industrial Internet security solutions have been applied extensively in the energy, electricity, manufacturing, transportation, petroleum and petrochemical, aviation, astronautics, and nuclear fields. The input of various industries into industrial Internet information security is also increasing year by year and the market scale continues to expand. For example, in 2021, the industrial Internet security market of China is expected to reach RMB 22.8 billion [25].

5.4 Boosting investment to enhance industrial competitiveness

As the government frequently releases favorable policies for the industrial Internet industry and public attention to cybersecurity continues to increase, relevant enterprises and investment institutions have also intensified investment and financing in the market. For example, Qianxin Technology Group Co., Ltd., Venustech Group Co., Ltd., Beijing Liufang Cloud Technology Co., Ltd., and other enterprises are making greater investments in the active promotion of the R&D of and breakthroughs in industrial Internet security technologies. As of the first half of 2020, the investment and financing scale of the industrial Internet in China had reached RMB 1.5 billion, among which industrial Internet security, data security, and cloud security had become investment and financing hotspots [15].

5.5 Deliberating regional layout for balanced industrial development

Based on the progress of industrial development and the status quo of the Internet security industry, the major economic regions of China have introduced corresponding development plans and policies to guide the layout of the industrial Internet security industry within the region. The Beijing–Tianjin–Hebei region has set a good example of coordinated development among regions by breaking through the core technologies of platform security. The Yangtze River Delta region has established a world-class advanced manufacturing cluster by building a secure and innovative platform with various functions. The Guangdong–Hong Kong–Macao Greater Bay Area has addressed security issues arising from the construction of new infrastructure by building a platform security support and service system. Efforts have been made to promote the transformation and upgrading of traditional industries by improving the basic supporting capacity of security technologies in the middle and upper reaches of the Yangtze River (Wuhan City, Chengdu City, and Guizhou Province). Based on pilot applications and demonstrations in key areas, Northeast China has strengthened the security of new industrial systems. By building secure enterprises and secure ecology, Northwest China has provided service guarantees for the growth of dominant industries.

It should also be noted that at this stage, the industrial Internet security industry of China remains in its infancy, with an imperfect industrial layout and severe challenges. First, the industry faces difficulties in insufficient coordination, unsound policy support, and imbalanced development among regions, industries, and enterprises. Furthermore, as core technologies are controlled by other countries, China has a relatively low level of technology autonomy without the effective fusion of function security and information security. As no security standard system is yet available and the layout of key industries remains ineffective, industrial Internet facilities and security products are not standardized in many aspects, including communication protocols and supporting specifications. Moreover, the industry does not offer guarantees in terms of capital, facilities, and other resource elements and exhibits a shortage of professional talents, and thus, SMEs do not have sufficient momentum to develop. Industrial ecology is yet to be improved, as industrial enterprises lack an understanding of security, the product design and production realities are not well integrated, and a synergy for development has not yet been formed.

DOI 10.15302/J-SSCAE-2021.02.015

6 Development of foreign industrial Internet security industry and its enlightenment to China

Developed countries and regions have been actively promoting the top-level design and application practice of the industrial Internet security industry, which can serve as a reference for China to implement industrial Internet security planning and deployment. The 14th Five-Year period (2021 to 2025) is crucial for China to implement the strategy of industrial Internet innovation and development in depth, as well as for the rapid development of the industrial Internet. To deal with the difficulties and challenges in a scientific and effective manner, suggestions from five aspects are presented for China to optimize the layout of the industrial Internet security industry.

6.1 Giving full play to institutional advantages in overall planning and balanced development

China should give full play to its institutional advantages to concentrate resources on major initiatives and form a synergy for the development of the industrial Internet security industry. First, the policy system should be improved to suit security industry development, the policy and institutional bottlenecks should be removed in the integration and penetration of related fields, the philosophy of innovative, independent, and controllable growth should be upheld, and a more favorable environment for industrial flourishing should be created. Second, China should strengthen the overall planning and coordination of various resources to promote the balanced development of the security industry among different regions, industries, and enterprises, thereby forming an industrial layout that features coordination between the east and the west, as well as balance between the south and the north, and optimizes the development of all regions. Third, a security regulatory system should be constructed to maintain the bottom line and avoid risks. Relevant lists should be formulated, including the negative, power, and responsibility lists. Focus should be placed on building an accountability system for industrial data security to promote the formation of an inclusive regulatory environment that supports industrial Internet development. Fourth, the security awareness of industrial enterprises should be comprehensively enhanced to enable joint construction, practice, prevention, and control of industrial Internet security.

6.2 Adhering to independent innovation for products with competitive edge

China should draw upon foreign technologies for industrial Internet security and their industrial innovation concepts, while avoiding simply copying technological systems and operation modes. First, it is suggested that the government, which is oriented toward the national demand to enhance strategic scientific and technological strength, promote the construction of innovation carriers such as national key laboratories, national engineering research centers, and national technological innovation centers of industrial Internet security, so as to create infrastructure and platforms that support high-level innovation for industrial Internet security. Second, China should boost innovation and breakthroughs in core technologies and basic theories of equipment, network, control, application, and data security. Moreover, full use should be made of cutting-edge technical facilities, such as satellite IoT and the BeiDou Navigation Satellite System, to aid in improving the security protection capabilities of the industrial Internet. Third, China should independently develop new security technologies, products, and services of international competitiveness as well as strengthen the application and promotion of such achievements. Fourth, industrial and security enterprises should be encouraged to match demands with one another, and to strengthen technological exchanges and complementary advantages to enhance cooperation in security technologies, products, and services, as well as carry out joint research into core technologies. In this manner, they can advance breakthroughs in industrialization and engineering approaches and introduce security protection solutions that are suitable for different application scenarios. Fifth, it is recommended that the authorities support efforts to mobilize public resources through mass testing and research, and innovate security technologies in fields such as cyberattack protection and vulnerability mining.

6.3 Strengthening domestic standards system to take lead in international rules

China can learn from the best practices and experiences of developed countries, improve the security standards and norms for application in the vertical industries of the industrial Internet, and plan the research and formulation of security standards in key areas such as energy, electricity, transportation, aviation, and aeronautics in advance. First, it is recommended that China build an industrial Internet security service and support platform featuring multi-party collaboration and covering various ministries, provinces, municipalities, and enterprises, to coordinate the construction of the overall system architecture, establish national unified standards and interfaces for system access,

and develop a set of guidelines for secure and integrated applications. Second, a national-level database of industrial Internet security information can be established and continuously optimized, covering the information that is required by the development of the industrial Internet, such as asset catalogs, communications protocols, security vulnerabilities, malicious codes, and defense strategies. Moreover, mechanisms for intelligence sharing and incentive sharing should be established. Third, the authorities should accelerate the application and promotion of existing national standards such as the *Uniform Content Label Format Specification* (GB/ T35304-2017). With a focus on the security demands in terms of industrial Internet facilities, as well as for the control, network (including identification analysis systems), platforms, and data, China needs to accelerate national and industrial standards development in security protection, testing, assessment, and others areas to foster a favorable environment for the verification of security technology and standards. Fourth, in the development of industrial Internet security standards, Chinese decision-makers should follow international practices, and align with international standards with a more open attitude and greater participation of international enterprises or experts. Fifth, Chinese experts should be supported to assume posts and to undertake projects in relevant international standards organizations. Professional institutions, and industrial and security enterprises should be encouraged to participate actively in the development of international standards, so as to promote Chinese standards to "go global" at a higher level.

6.4 Stimulating vitality of SMEs with stronger support

The first suggestion is to stress and encourage the reform and innovation of SMEs in the industry and security fields, as well as to introduce favorable policies and increase capital support for SMEs to improve their operational and management capabilities. Second, the government should support SMEs in carrying out basic research and scientific and technological innovation, and in participating in the R&D of core technologies and implementing key national science and technology projects. Third, innovation and entrepreneurship bases, business incubators, and science and technology incubators for SMEs should be built with scientific planning to promote the industrial agglomeration development of SMEs. Fourth, the government should improve the diversified investment and financing systems, trial-and-error tolerance, and risk hedging mechanisms for application pilots, as well as give full play to the role of trust, insurance, and other investment funds. Fifth, the industry should strengthen the coordination of upstream and downstream players in the supply chain and industrial chain, with industry leaders playing their roles effectively. Leading enterprises in areas with a solid economic basis should pilot the transformation of security research outcomes, evaluate the application efficiency, and drive the development of supporting SMEs along the chain. Sixth, several regions should be provided with technical support, service transformation, and technical guidance for the upgrading and innovation of SMEs by introducing relevant projects. Seventh, SMEs can upgrade their hardware and software, train professionals in related areas, introduce advanced innovation, and gradually build core competitiveness under official guidance and support. Thus, a regional layout that features the collaborative development of various types of enterprises can be established.

6.5 Constructing collaborative ecology and pattern of "dual circulation"

China should strengthen its top-level planning for the establishment and improvement of its industrial Internet security industry system. Moreover, China should guide key stakeholders in the industrial system, including local governments, industrial enterprises, scientific research institutions, and security enterprises, for their precise positioning, targeted efforts, and coordinated development to contribute jointly to the ecology of the industrial security industry of China. First, it is suggested that China build an intelligent, collaborative, and grid-based platform framework for domestic and foreign markets, industrial chains, and supply chains in different fields, with the aim of improving the overall security and risk control. It is also recommended that China promote the deep integration of "government, industry, university, research and application" by leveraging the force of industrial alliances, high-end think tanks, and others and cultivate numerous specialized industrial bellwethers with the capacity for industrial integration. A talent development plan should be designed for the industrial Internet security industry. A security talent pool, expert pool, and innovative joint cultivation mechanism should be established. Furthermore, efforts should be made to tap into and cultivate comprehensive and practical talent that is urgently required by the country and enterprises. International events in the field of industrial Internet security should be supported and promoted with innovative forms, enhanced recognition of awards, and wider participation by foreign competitors. Moreover, to strengthen international cooperation and the regional layout, the government should focus on serving the Belt and Road Initiative while deepening its exchanges with developed countries. Industrial and security enterprises are also encouraged to raise the level and performance of their "go global" initiatives.

DOI 10.15302/J-SSCAE-2021.02.015

References

[1] Xu X L. Industrial Internet is an important engine of high quality economic development [N]. Science and Technology Daily, 2019- 12-09(01). Chinese.

[2] Zhang N, Liu L R, Tian Z H, et al. Progress and trend of industrial Internet security [J]. Journal of Guangzhou University (Natural Science Edition), 2019, 18(3): 68–76. Chinese.

[3] Kang S Y, Hu W L. Research on industrial Internet security technology and analysis on the development of industrial Internet security industry in China [J]. Secrecy Science and Technology, 2020 (5): 27–31. Chinese.

[4] Wang X X, Li X, Chen Y, et al. Analysis of industrial Internet security problems and countermeasures [J]. Intelligent Building & Smart City, 2020 (3): 76–77. Chinese.

[5] Li X, Wang X X, Chen Y. Research on key technologies of industrial Internet security [J]. Intelligent Building & City Information, 2020 (4): 101–102. Chinese.

[6] Zheng Z B, Wang C D. The situation and development trend of industrial Internet security technology [J]. Value Engineering. 2020, 39(32): 190–191. Chinese.

[7] Zhang J, Zhu C M, Wei K Y. Research on industrial Internet security situation and protection countermeasures [J]. Digital Technology and Application, 2020, 38(11): 163–165. Chinese.

[8] Zhang F, Guo Z M, Sun X H, et al. An overview on industrial Internet security and evaluation [J]. Science & Technology Vision, 2019 (25): 120–121. Chinese.

[9] Wang C H, Li J, Chen X H. Research on industrial Internet platform security protection [J]. Netinfo Security, 2019 (9): 6–10. Chinese.

[10] Liu X M, Dong Y, Zhang Y, et al. *The IoT security maturity model practitioner's guide* and its enlightment for China [J]. Information and Communications Technology and Policy, 2020 (2): 57–60. Chinese.

[11] Liu X M, Quan X R, Li S. An overview on the development of foreign industrial Internet security [J]. Secrecy Science and Technology, 2020 (5): 20–26. Chinese.

[12] Liu X M, Jin W J, Li N. The advancement of American industrial Internet security and its enlightenment to China [J]. Information and Communications Technology and Policy, 2019 (8): 81–84. Chinese.

[13] Fu Y. Security situation and threats analysis of industrial Internet in China and abroad [J]. Journal of Information Security Research, 2019, 5(8): 728–733. Chinese.

[14] Xiao L L. A comparative study on the industrial Internet of Things platform at home and abroad [J]. Information and Communications Technologies, 2018, 12(3): 27–31. Chinese.

[15] China Academy of Information and Communication Technology, Alliance of Industrial Internet. Report on industrial Internet security situation for the first half of 2020 [R]. Beijing: China Academy of Information and Communications Technology, Alliance of Industrial Internet, 2020. Chinese.

[16] Chinese Academy of Cyberspace Studies. World Internet development report 2020 [M]. Beijing: Publishing House of Electronics Industry, 2020. Chinese.

[17] National Industrial Security Industry Alliance. White paper on the development of China's industrial information security industry (2019—2020) [R]. Beijing: National Industrial Security Industry Alliance, 2020. Chinese.

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

[19] European Union Agency for Cybersecurity. Industry 4.0 cybersecurity challenges and recommendations [R/OL]. Brussels: European Union Agency for Cybersecurity, 2019. (2019-05-20) [2021-03-14]. https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations.

[20] Alliance of Industrial Internet. Industrial Internet platform security white paper (2020) [R]. Beijing: Alliance of Industrial Internet, 2020. Chinese.

[21] Shanghai Trusted Industrial Control Platform Co., Ltd., Cyber Research Institute. White paper on industrial Internet security [R]. Shanghai: Shanghai Trusted Industrial Control Platform Co., Ltd., Cyber Research Institute, 2019. Chinese.

[22] Beacon Lab. Network security power: Development path of industrial control safety in Israel [EB/OL]. (2020-06-22) [2021-03-14]. http://plcscan.org/blog/2017/01/development-path-of-icscybersecurity-in-israel/. Chinese.

[23] Official Microsoft Blog. Microsoft acquires CyberX to accelerate and secure customers' IoT deployments [EB/OL]. (2020-06-22) [2021-03-14]. https://blogs.microsoft.com/blog/2020/06/22/microsoft-acquires-cyberx-to-accelerate-and-secure-customers-iot-deployments/.

[24] Alliance of Industrial Internet. Industrial Internet typical security solutions case collection V3.0 [R]. Beijing: Alliance of Industrial Internet, 2020. Chinese.

[25] CCID Consulting Co., Ltd. White paper on China's cyber security development (2019) [R]. Beijing: CCID Consulting Co., Ltd., 2019. Chinese.