ATLANTIS PRESS
*Advances in Social Science, Education and Humanities Research, volume 385*
**3rd International Conference on Education, Economics and Management Research (ICEEMR 2019)**

# How to Cooperate with One Belt and One Road Countries on industrial information Security Industry

Peng Hou
Northeast Normal University
Changchun, Jilin Province, China

Xinzhu Cai
Jilin Agriculture University
Changchun, Jilin Province, China

***Abstract*—Industrial cooperation is an important step to faster the promotion of China's global voice and rule-making power in cyberspace. With the gradual deepening of the Belt and Road Initiative(BRI), the major equipment and facilities, intelligent factories as well, that went global from China become new targets of cyber attacks, facing a tremendous threat to industrial information security. At the same time, during the industrialization process, countries along the BRI routes face huge market demand for industrial information security, which fits perfectly with China's industrial development status and strength. In that case, they should actively promote industrial information security industry to go out to countries along the routes through cooperation, assistance, services and other channels, so as to complement the short blank in industrial capacity cooperation, and ultimately to pursue shared growth through discussion and collaboration in the field of industry information security.**

***Keywords—the Belt and Road Initiative; industrial information security industry; industrial cooperation; share***

## I. INTRODUCTION

From a global perspective, the development of industrial information security is still in its infancy, with broad space for cooperative development. To promote the introduction of industrial information security greater progress has been made in opening up and cooperation in the field of industrial information security, among which, cooperation with countries along the Belt and Road will be an important breakthrough. The report of the 19th National Congress of the Communist Party of China (CPC) called for the Belt and Road to actively promote international cooperation and strive to achieve policy, infrastructure, trade, financial and people-to-people exchanges. With the further development of the Belt and Road strategy, China's major equipment and intelligent chemical plants have made remarkable achievements in going out, become new targets of cyber attacks, and face huge security risks. At the same time, the low degree of industrialization in the countries along the Belt and Road will produce huge security demand while the industry develops. Therefore, on the basis of vigorously developing industrial information security industry, China should actively promote the industrial information security industry of Belt and Road to go out through cooperation, assistance and service.

## II. REASONS FOR CHINA TO COOPERATE WITH COUNTRIES ALONG THE ROUTES IN THE INDUSTRIAL INFORMATION SECURITY INDUSTRY

### *A. Industrial information security has become a new highlight*

Driven by national strategies such as National Strategic Plan for Advanced Manufacturing of the USA, Industry 4.0 initiated by Germany and China's Made in China 2025, the entire world is promoting the deep integration of manufacturing and Internet, and the boundary between the cyberspace and the physical space in industry exist no more. According to statistics of CICS-CERT (China Industrial Control System Cyber Emergency Response Team), by the first half of 2017, more than 90,000 industrial control systems, which were widely operated in industrial manufacturing, energy industry, municipal management and other important fields, had been exposed online[1]. Cyber attacks are thus shifting from virtual space to physical life, and a series of accidents has exerted serious impacts on the global economy and society, attracting high-level attention of the world. Consequentially, America, EU, Japan, Australia and other countries and regions have issued relevant policies to strengthen protection of key infrastructure information security, to advance their layouts of industrial information security industry, and to increase their investment in industrial information security. For instance, in April 2016, the Australian government set a plan to spend AUD 230 million on attack protection for their vital infrastructures[2].

### *B. Huge market potential in countries along the routes of BRI*

Statistically, as of 2016, only 9 countries along the routes had achieved an industrial output of over 100 billion US dollars, accounting for over 40% of GDP of the host countries. Among them, only 6 are semi-industrialized, half the countries along the routes were with an industrial output of less than $10 billion, and the majority of them were still in their initial stages of industrialization. Yet currently, the integration of industrialization and informatization in global wide has become the mainstream of development, it is an era that industrial control system is increasingly inter-connecting, opening and intelligent sizing. In that case, it is essential to integrate informatization elements with the industrialization process of countries and regions along the BRI routes. The development of industrial control system and products will

 

generate much market demand for industrial information security. According to data from Micro Market Monitor, a market research firm, the Asia-Pacific network security market stands for 17.21% of the global share, which, however, will increase to 21.16% in 2019[3].

Nevertheless, the industrial information security industry in countries along the routes is relatively lagging and the enterprises related are not strong enough, due to technological basis, industrial environment and other factors. According to the Cybersecurity 500 issued by Cybersecurity Ventures in the 4th quarter of 2016, only 32 companies in countries along the routes were listed (Israel companies holds 75% of them), occupying approximately 6% of the total and companies related to industrial information security were even less.

### *C. It is urgent to strengthen the safety protection of major facilities that went out from China*

The Belt and Road Initiative has brought new opportunities for China's output of production capacity. Owing to that, notable achievements have been made in "going global" of major equipment and facilities such as high-speed railway, nuclear power facilities, as well as intelligent and automatic production bases and parks.

High-speed rail is an important label for China's high-end manufacturing industry to go global and a great many projects about it have been signed and implemented with countries along the routes, such as the Mosko-Kazan high-speed railway in Russia, the Jakarta-Bandung high-speed railway in Indonesia, the China-Thailand high-speed railway and the China-Malaysia "super railway". Compared with traditional railway projects, high-speed railway requires higher technology content and more accurate control, which greatly increases the hidden danger of industrial information security. The Wenzhou High-speed Train Accident happened on 23rd July 2011 was due to the communication signal system failure and caused massive losses. Consequences are unimaginable if similar incidents take place in our high-speed railway projects undergone in Thailand or Malaysia. Meanwhile, the nuclear power industry is also a key field to China's industrial going out and a series of projects within it have been underway with countries along the routes like Pakistan, Turkey and Romania. While currently, nuclear power plants have become major targets of industrial information security attacks. The uranium enrichment plants in Natanz of Iran, for example, suffered attacks of Stuxnet Worm in 2010. Despite the fact that no nuclear leakage or other vital consequences were triggered, an alarm ought to be sounded anyway. In addition, under the guidance of the Belt and Road Initiative, 56 economic and trade cooperation industrial parks (like the Great Stone) have been established by Chinese companies in 20 countries along the routes, among which there are some intelligent production bases (such as the refrigerator factory built by Haier in Russia), which are also facing the risk of industrial security attack.

## III. DIFFICULTIES IN INDUSTRIAL INFORMATION SECURITY COOPERATION BETWEEN CHINA AND COUNTRIES ALONG THE BRI ROUTES

In spite of the positive prospects for cooperation between China and countries along the routes in the industrial information security industry, barriers still exist during the going out of our companies, technologies and standards.

Firstly, China's industrial information security entities are mainly small and medium-sized enterprises, meaning the capacity and competitiveness of going out is still relatively weak. Indeed, the industry of industrial information security in China is in its initiative stage, in 2016, the entire industry scale reached 82.5 million yuan, among which the industrial control system information security only held 300 million yuan. With relatively small scale and slow growth, the industry in China is mainly made up of small- and medium-sized companies and most of them were developed from traditional network security enterprises, which is quite different from foreign giants for the latter is transformed from industrial control sector into information security. Therefore, it is difficult for enterprises to go out with the competitiveness and market expansion ability of their own.

Secondly, countries along the routes have certain barriers to the introduction of security technologies and products. Among them, information security has been well developed in countries like Russia, Singapore and Israel, making it hard to output our technologies and products to them. Besides, some central and eastern European countries have basically adopted EU information security products and services, lacking interest to introduce Chinese ones. In the ASEAN ICT Masterplan 2020, ASEAN countries proposed to develop their own information security standards and emergency response mechanism. India, as well, with its strength in IT industry, exerts strict review to the introduction of foreign IT technologies and products [4].

Thirdly, the United States and developed countries in Europe are stepping up their overseas distribution to seize development opportunities. With head start in the industrial information security industry, these countries are making full use of the leading position in security technology and are actively strengthening the international influence of their standards, guidelines, industry norms and other documents, so as to influence the global industrial information security protection system architecture, and to seize the development opportunities. At present, countries (regions) along the BRI routes mostly adopt influential international standards issued by ISO and other authoritative standardization organization in Europe and America, and carry out the formulation and promotion of relevant standards based on their domestic realities. For instance, the NIST SP800-82 issued by NIST(National Institute of Standards and Technology) has become the most popular, influential and promoted industrial information security standard [5].

China is still at the beginning stage in this regard. In 2016, together with a series of industrial safety standards, Guide for Information Security Protection of Industrial Control Systems was issued by the Ministry of Industry and Information Technology of the PRC, aiming to gradually form a

comprehensive industrial control information security standard system covering safety management, system safety protection, product safety assessment, etc. But currently, most of the standards are still in the draft or for comment.

## IV. Possible ways for China to cooperate with countries along the BRI routes in industrial information security industry

It is currently the finest time for us to achieve shared growth through discussion and collaboration in industrial information security industry with countries along the routes. Taking that as the hitting-point, a community of shared future for regional security can be built and reshaped the global industrial information security landscape. To achieve that, suggestions are from the two dimensions of international cooperation and domestic industry development as follows:

### *A. Cooperation with countries along the routes.*

Firstly, speed up aid-style exports. The economic strength of countries along the routes is relatively weak, in addition to several that have room for cooperation in the field of industrial information security with China, our assistance will be vital to help those countries to build up their industrial information security protection systems. In that case, they propose to cover industrial information security products and technologies into the range of BRI strategic assistance product, and export the products to those countries. While they are promoting the going out of our major projects, programs and industrial products, industrial information security products, enterprises and related services could be affiliated. In addition, financial and policy support should be provided for companies in the industry who will invest and build plants, and carry out cooperative production in BRI countries.

Secondly, enhance the service-oriented extension. At present, service in the IT industry has become the highlighted trend, and thus service extension and guarantee should be well provided while ensuring the output of products, technologies and standards. It is suggested to encourage and support the service modal that industrial information security enterprises to use the Internet, cloud computing and other technologies to provide remote security services for countries along the BRI routes. Also, the government needs to promote the going out of industrial information security testing, certification, assessment, intellectual property protection and other services. Building a industrial information security public service platform is another feasible option, by which they can comprehensively pool our strength and human resources in the field, and provide industrial enterprises in countries along the routes with one-stop services covering risk warning, safety diagnosis and assessment, safety consulting, emergency responding and safety protection implementation[6].

Thirdly, they need to develop cooperatively for win-win cooperation is the theme of the Belt and Road Initiative. It is recommended that, on the basis of making full use of existing bilateral and multilateral mechanisms and platforms, cooperation documents in the field of industrial information security, including bilateral and multilateral memorandums and plans, can be signed and new cooperation platforms can be built. They can establish research institutes with these countries; develop projects like industrial control test ranges and testbeds, and share research and development of common technical capabilities of the field such as testing, verification and evaluation, so as to improve industrial control security capabilities such as risk discovery, analysis and prevention. Meanwhile, with the perfection of laws and policies, organizational structures and operation mechanisms, they can advance the notifying and sharing of risk vulnerabilities, security incidents and settle schemes. Also, they can improve the emergency response capacity of critical infrastructure to cyber-attacks by joint drill and enhance the international voice and influence by the joint formulation of a regional standard system for industrial information security.

### *B. Feasible ways to upgrade domestic industry in this regard*

First and foremost, they need to grasp the opportunities created by mass entrepreneurship and innovation, thereby enhancing rapidly the strength of industrial technologies, products and standards, and winning more say for China in the international arena. They suggest making full use of our resources and conditions, ranging from support fund for small- and medium- companies in all sectors, favorable policies for entrepreneurship and innovation enterprises, to public service platforms for these enterprises, and focus more on the technology, products, and standards of industrial information security industry. Besides, relying on the national industrial information security industry development alliance, they can cultivate industrial ecological circle, and build a cooperation platform of massive entrepreneurship and innovation, by which resource sharing and advantage complementation in the industry can be achieved. They can set up a base for industrial information security entrepreneurship and innovation in cyber security industrial park to provide stronger support. At the same time, they can better our communication with ISO so as to promote the establishment of international standards in the field of industrial information security.

Secondly, the capacity to provide service likes comprehensive testing, evaluation and certification need to be improved rapidly. To certificate and guarantee the quality of the exports of our industrial information security enterprises, products and technologies, certain bodies are suggested to be set, such as national supervision and inspection center for the safety and quality of industrial control system and product, safety review center of industrial information security technology products and some key labs. Also, they need to improve our ability to carry out strategic research and to provide education and training in this regard.

Last but not least, they need to better protect the IPR(intellectual property right). They can accelerate the pace of authorization, verification and safeguarding of IPR by setting up an IPR protection center in this industry, building a public service platform of IPR, and providing service of legal consulting, information, agency for application, commercialization, judicial expertise and training related to IPR. In the meantime, they can establish technology collaborative innovation center for patents in IISI, and explore to set up operating funds for IPR. In that case, they can promote the transformation of scientific and technological achievements and the commercial application of innovative

achievements, and benefit the operation and development of enterprises in their IPR part.

## V. CONCLUSION

In recent years, with the continuous permeation of information technologies, such as the Internet, IoT(Internet of Things) and cloud computing, in industrial production activities, cyber-attacks have infiltrated into our life from virtual space. And cyber attacks on national key infrastructure, industrial control equipment and intelligent products have become a new subject of cyber security attack and defense in the world.

In the report of the 19th National Congress of the Communist Party of China, they call on the people of all countries to work together to build a community with a shared future for mankind, to build a world that enjoys lasting peace. They will foster new thinking on common, comprehensive, cooperative, and sustainable security, and will coordinate responses to traditional and non-traditional threats. Globally, the development of industrial information security is still in its infancy, with broad space and great potential for cooperation and development. By establish international cooperation mechanisms on industrial information security technologies, products, platforms and services, they can advance our "bringing in" and "going global" strategy, build a multilateral, democratic and transparent international governance system for industrial information security, and ultimately achieve greater process in the opening up and cooperation in the field of industrial information security. To obtain that, cooperation with countries along the BRI routes can serve as a key point to breakthrough.

The report claims that China will actively promote international cooperation through the Belt and Road Initiative. In doing so, they hope to achieve policy, infrastructure, trade, financial, and people-to-people connectivity. With the deepening of the BRI, notable achievements have been made during the "going global" of China's major equipment and intelligent factory. However, they also turned out into the new targets of cyber attacks, facing tremendous security risks. Meanwhile, the low level of industrialization in countries along the routes can generate huge demand for security service, offering great opportunities for the going out of China's enterprises, products, technologies and standards in industrial information security industry.

Therefore, China should vigorously develop the industrial information security industry on the basis of active cooperation, assistance and services accelerate the promotion of the going global of industrial information security under the framework of BRI.

## REFERENCES

[1] LB. Yin, "Annual Report of World Cyber Security(2016-2017)," [In Chinese]. Social Sciences Academic Press, 2017.

[2] P. Shakarian, J. Shakaria, and A. Ruef. "Introduction to Cyber-warfare: A Multidisciplinary," [In Chinese], translated by YJ. Wu, et al. Gold Wall Press, 2006.

[3] Ministry of Industry and Information Technology of the People's Republic of China, "Guide for Information Security Protection for Industrial Control Systems," [In Chinese] Publishing House of Electronics Industry, 2016.

[4] Y. Sun, "Belt and Road strategy and China's industrial security: mechanisms, factors and paths," [In Chinese]. International Trade, 2016, pp. 25-28.

[5] T. Wang, and Q. Li, "Research on the way of Chinese industrial information security industry going out under the Belt and Road strategy," [In Chinese], Telecommunication technology, April 2018, pp. 20-24.

[6] Y. Li, and Q. Liu, "A study of the economic contribution of the information industry in the countries along the Belt and Road," [In Chinese].Guide to China's Economy and Trade, August 2018, pp. 8-10