Advances in Social Science, Education and Humanities Research, volume 195
International Seminar on Education Research and Social Science (ISERSS 18)

Research on the Cooperation Path of Industrial Information Security Industry between China and "One Belt and One Road" Countries

Qi Feng
Northeast Normal University
Changchun, Jilin Province, China

Liu Xiqiao
Northeast Normal University
Changchun, Jilin Province, China

***Abstract*—General Secretary Xi Jinping stresses that it is necessary to "accelerate China's right for international discourse and rulemaking in cyberspace", and industrial cooperation has been strengthened. With the gradual deepening of the "One Belt and One Road" strategy, China's "going out" major equipment facilities and intelligent factories have become the new targets of cyber-attack, and enormous threats to industrial information security have been in the face. At the same time, in the process of industrialization along the route, there is a huge market demand for industrial information security, and it matches the status quo and strength of China's industrial development. Therefore, we should actively promote the industrial information security industry to "go out" to the countries along the route through cooperation, assistance, and services, and complement the "short board" of industrial capacity cooperation to achieve "co-business, co-construction and co-sharing" in the field of industrial information security.**

Keywords—industrial information security industry, One Belt and One Road, going out

I. THE NECESSITY OF INDUSTRIAL INFORMATION SECURITY INDUSTRY COOPERATION BETWEEN CHINA AND "ONE BELT AND ONE ROAD" COUNTRIES

A. Industrial information security has become a new commanding height in the global network security industry competition.

Under the strategy of "National Advanced Manufacturing National Strategic Plan", "German Industry 4.0", and "Made in China 2025", the deep integration of the manufacturing industry and the Internet has been pushed forward all over the world, and the cyberspace and industrial physical space are gradually integrated. According to the statistics of the National Industrial Information Security Development Research Center, as of the first half of 2017, more than 90,000 industrial control systems were exposed to the Internet and widely used in the important fields such as industrial manufacturing, energy, and municipal administration. Cyber-attacks have also gradually shifted from virtual space to physical space. Ukrainian power grid has been attacked, cyberattack "sandstorm" has assaulted Japan's critical infrastructure, North American DDoS attack has caused large-scale network disconnection, and Kemuri water plant purification system has been charged, which have brought serious impacts to the global economy and society and have attracted great attention of all countries. The United States, the European Union, Japan, Australia and other countries and regions have introduced relevant policies to strengthen the protection of information security of key infrastructure and the layout of industrial information security industry, and have increased the investment of industrial information security. In April 2016, the Australian government planned to spend A$230 million on attack protection of important national infrastructure [1].

B. There is huge market space in the countries along the "One Belt and One Road"

According to statistics, as of 2016, only 9 countries along the "One Belt and One Road" had broken industrial output value by 100 billion US dollars, and industrial output value accounted for more than 40% of GDP, that is, only 6 countries reached semi-industrialization, most of the countries were in the early stage of industrialization. Half of the countries had industrial output value of less than 10 billion US dollars and had enormous industrial development power and space. In the current era, global industrialization and information integration development have become the mainstream, and industrial control system is gradually interconnected, open and intelligent. The industrialization process of countries and regions along the "One Belt and One Road" is indispensable to add the informatization elements. For example, India put forward the concept of "digital India" in the "Made in India" strategy, and Kazakhstan set up a network system that were able to make industrial enterprises interconnected in the cities in the industrial innovation policy. The industrial control system and the development of products will bring immense market space for industrial information security. According to the data of the survey company Micro Market Monitor, at present, the network security market in the Asia-Pacific region accounts for 17.21% of the global market share, and will increase to 21.16% by 2019.

Due to the influence of technological foundation and industrial environment, the development of industrial information security industry in the countries along the "One Belt and One Road" relatively lags behind other countries, and the strength of enterprises is not strong enough. In the 2016 Q4 Top 500 Network Security Innovation list released by Cybersecurity Ventures in the United States, only 32 companies in the countries along the "One Belt and One Road"

are on the list (in which Israel accounts for 75%), accounting for about 6% of the total, and the less are involved in the field of industrial information security.

C. China's "going out" major equipment and intelligent industrial facilities urgently need to strengthen security protection

The construction of the "One Belt and One Road" has brought new opportunities for the output of China's capacity. The "going out" results of major equipment and facilities such as high-speed rail and nuclear power, as well as the intelligent and automatic production bases and parks are remarkable, but the safety risks are also increased. It is urgent to speed up the exportation of industrial information security industry and strengthen security protection.

High-speed rail is an important label of "going out" of China's high-end manufacturing industry. In the countries along the "One Belt and One Road", many projects have been signed and implemented, such as Russia's Moscow-Kazan high-speed rail, Indonesia's Yawan high-speed rail, China-Thailand high-speed rail, and China-Malaysia "super railway", etc. Relative to traditional railway projects, high-speed rail has higher scientific and technical contents and more precise control requirements, which greatly increases industrial information security risks. The "7•23" motor vehicle accident was caused by the failure of the communication signal system, and resulted in huge losses. If a similar incident occurs in China's high-speed rail trains built in Thailand or Malaysia, the consequence will be disastrous. Nuclear power is also an important area of China's industry "going out". China has cooperation with countries along the "One Belt and One Road" such as Pakistan, Turkey and Romania in the field of nuclear power. At present, nuclear power plants have become an important target of industrial information security attacks. In 2010, Iranian Natanz uranium enrichment plant was attacked by "Stuxnet". Although it did not cause nuclear leakage and other major events, it also sounded an alarm for us. At the same time, under the guidance of the "One Belt and One Road" strategy, Chinese enterprises have established 56 economic and trade cooperation industrial parks in 20 countries along the "One Belt and One Road". There are intelligent production bases, such as the refrigerator factory built by Haier in Russia, which also face the risk of industrial security attacks.

II. THE DIFFICULTIES OF INDUSTRIAL INFORMATION SECURITY INDUSTRY BETWEEN CHINA AND "ONE BELT AND ONE ROAD" COUNTRIES

China and the countries along the "One Belt and One Road" have a good space for cooperation in the industrial information security industry, but there are still some barriers to "going out" of enterprises, technologies and standards.

The first one is that China's industrial information security enterprises are mainly small and medium-sized enterprises, and the ability and competitiveness of "going out" are relatively weak. At present, the fields of China's industrial information security industry are all in their infancy. In 2016, the scale of the national information security industry reached 82.5 billion Yuan, and the market scale of industrial control system information security was only 300 million Yuan (see Fig. 1). The industrial scale was small, and the growth rate was slow. It is different from the development of industrial information security for large enterprises in the field of foreign industrial control, the industrial information security enterprises in China mostly extend from the traditional network security enterprises to the industrial field, and the enterprises are mainly small and medium-sized enterprises. Therefore, it is very difficult for these enterprises to "go out" relying solely on their own strength and market expansion capabilities.

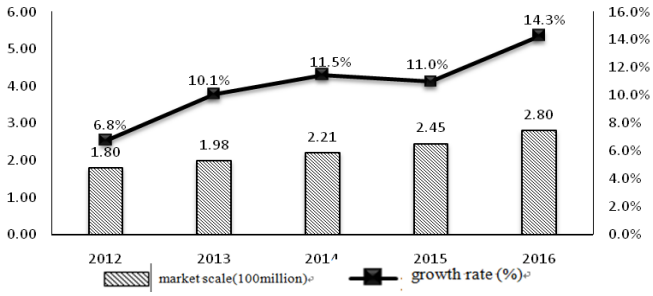

Fig. 1. China's industrial information security market scale and growth rate in the past years of 2012-2016

Source: National Industrial Information Security Development Research Center.

The second one is that there are some barriers to the introduction of safety technologies and products of the countries along the route. Among the countries along the "One Belt and One Road", Russia, Singapore, Israel and other countries have higher information security strength and more difficult industrial output. Some countries in Central and Eastern Europe basically adopt EU information security products and services, and the introduction of China's technologies, products and standards is insufficient. In the ASEAN ICT2020 Strategy, ASEAN proposes developing its own information security standards and emergency response mechanisms. India has strong strength in the field of IT, and is strict with the introduction of foreign IT technologies and products [2].

The third one is that the developed countries such as Europe and the United States have stepped up their abroad layout and seized development opportunities. Developed countries such as Europe and the United States have a head start in the field of industrial information security. They make full use of their dominant position in security technology, and actively strengthen the international influence of standards, guidelines and industry norms to produce an effect on the framework of global industrial information security protection system and seize the industry development opportunities. At present, countries and regions along the "One Belt and One Road" often adopt international standards with great influence issued by the international standardization organizations and European and American authoritative standardization institutions, and carry out relevant standards formulation and promotion work in combination with the domestic reality. NIST SP800-82, published by the National Institute of Standards and Technology (NIST), has become the most widely used, most influential and most advanced industrial

information security standard in countries and regions along the "One Belt and One Road".

China is at the initial stage in the field of standards. In 2016, China issued the Guidelines for Industrial Control Systems Information Security Protection and a series of industrial control safety standards. It is planned to gradually form a comprehensive industrial control information safety standard system covering safety management, system safety protection, product safety assessment and so on. However, at present, most of the standards are in the draft or consultation stage.

III. SUGGESTIONS FOR THE COOPERATION PATH OF INDUSTRIAL INFORMATION SECURITY INDUSTRY BETWEEN CHINA AND "ONE BELT AND ONE ROAD" COUNTRIES

At this moment, it is a great opportunity for China to carry through "consultation, contribution and shared benefits" of the industrial information security industry with the countries along the route. It can be used as a hitting point to build a regional security destiny community and rebuild the global industrial information security pattern. Therefore, from the two dimensions of international cooperation and domestic industrial development, the following suggestions are proposed:

A. Cooperation with countries along the route

The first one is to speed up the "aid-style" output. The economic strength of the countries along the "One Belt and One Road" is relatively weak. In addition to a few countries that have cooperation space in the field of industrial information security, most countries need China's assistance to establish their own industrial information security protection system. Therefore, it is suggested that industrial information security products and technologies should be included in the scope of national "One Belt And One Road" strategic assistance products and be exported to countries and regions along the route. When major projects and industrial products "going out", industrial information security products, enterprises, related services should be bundled. The industrial information security enterprises that invest and construct factories along the "One Belt and One Road" countries should be provided financial and policy support.

The second one is to enhance the "service-oriented" extension. At present, the trend of service orientation in IT industry is prominent. While exporting products, technologies and standards, it is necessary to do well in service extension and guarantee. It is recommended that industrial information security enterprises should make use of the Internet, cloud computing and other technologies to encourage and support remote security services to countries along the "One Belt and One Road", and promote the "going out" of industrial information security testing, certification, evaluation, intellectual property protection and other services. A public service platform for industrial information security should be created to comprehensively gather domestic industrial control system security service capabilities and human resources, and provide one-stop service for risk warning, safety diagnosis and assessment, safety consultation, safety emergency, and safety protection for industrial enterprises in the countries along the route.

The third one is to make a good job in "cooperative" development. Win-win cooperation is the theme of the strategy implementation of "One Belt and One Road". It is suggested to make full use of the existing bilateral and multilateral mechanisms and platforms to sign bilateral and multilateral industrial information security field memoranda, planning and other cooperation documents, and build a new cooperation platform. It would be better to cooperate with countries along the route to jointly build research institutions, implement "One Belt and One Road" industrial control test range, test bed and other projects to carry out industrial information security testing, verification, evaluation and other common technical capabilities research and development sharing and to improve risk detection, analysis, prevention and other industrial control security guarantee capabilities. Notification and sharing of industrial information security risk loopholes, security incidents and solutions should be promoted through the formulation of legal policies, improvement of organizational structures and perfection of operational mechanisms. Industrial information security emergency drill should be jointly carried out to improve the emergency response capability of network attack on key infrastructure. Industrial information security regional standard system should be collectively formulated to enhance international discourse power and influence.

B. Domestic industry improvement

The first one is to pay close attention to the "double creation" opportunity, rapidly improve the industrial technologies, products, standard strength, and strengthen the right of international discourse. It is suggested that all kinds of SMEs support funds, "double creation" enterprise support policies, SMEs public service platforms and other resource conditions should be fully utilized to tilt the industrial information security industry technologies, products and standards. The National Industrial Information Security Industry Development Alliance should be relied on to cultivate the industrial ecological circle, and build a double creative platform of industrial information security industry with complementary resources and advantages. In the network security industrial park, a "double creation" base for industrial information security will be set up to increase support. Communication with international standards organizations should be strengthened to promote the establishment of international standards in the field of industrial information security.

The second one is to rapidly improve the comprehensive testing, evaluation, certification and other service capabilities. It is suggested that the national industrial control system and product safety and quality supervision and inspection center, industrial information safety technology product safety review center and key laboratory should be set up to provide inspection and certification services for "going out" industrial information security enterprises, products and technologies. Information security strategy research, education and training services capabilities should be improved [3].

The third one is to strengthen the protection of intellectual property. It is suggested that the intellectual property protection center of industrial information security industry should be set up, and the public service platform of intellectual property

should be built to provide services such as intellectual property law, consultation, information, application proxy, commercialization, judicial identification, training and so on, and accelerate the authorization, approval and protection of intellectual property. The collaborative innovation center for patent technology in the industrial information security industry should be constructed, and the intellectual property operation fund should be explored to establish. At the same time, the transformation of scientific and technological achievements, the commercialization of innovation results, and the operation and development of enterprise intellectual property should be promoted.

IV. CONCLUSION

In recent years, information technologies such as Internet, Internet of Things and cloud computing have continuously infiltrated the industrial production activities. Cyber-attacks have moved from virtual space to physical space. The network attacks on key national infrastructure, industrial control equipment and intelligent products have become a new object of network security attack and defense all over the world.

The report of the 19th National Congress called on people of all countries to work together to establish a community of human destiny and build a world of universal security. It is necessary to "set up a common, comprehensive, cooperative and sustainable new security concept" and "make plans for traditional and non-traditional security threats." Globally, industrial information security development is still in its infancy and has broad space for cooperation and development. It can be realized to promote "introduction" and "going out", build a multilateral, democratic and transparent international management system of industrial information security, and achieve a greater progress in the field of industrial information security through the establishment of international cooperation mechanisms for industrial information security technologies, products, platforms and services. Among them, cooperation with countries along the "One Belt and One Road" will become an important breakthrough.

The report of the 19th National Congress called for "actively promoting the international cooperation of the 'One Belt and One Road' and striving to achieve policy communication, facility connectivity, unhindered trade, accommodation of funds, and common aspiration of the people." With the deepening of the "One Belt and One Road" strategy, China's major equipment and intelligent factories have achieved remarkable results in "going out" and have grown up to be a new target of cyber-attacks, facing huge security risks. At the same time, there is a low degree of industrialization for countries along the "One Belt and One Road". In the development of industry, it will bring great opportunities for China's industrial information security enterprises, products, technologies and standards "going out" while generating huge security need.

To this end, on the basis of vigorously developing the industrial information security industry, China should actively accelerate the promotion of the industrial information security industry "going out" along the route through cooperation, assistance and services.

REFERENCES

[1] Yin Libo. World Cyber Security Development Report (2016~2017)[M]. Social Sciences Academic Press, 2017(6).

[2] Ministry of Industry and Information. Industrial Control Systems Information Security Protection Guide [Z]. 2016(10).

[3] Paulo Shakarian, Jana Shakaria, Andrew Ruef. INTRODUCTION TO CYBER-WARFARE: A Multidisciplinary [M] Wu Yujun et al. Beijing: Jincheng Press, 2006 (7).