Research on International and Domestic Internet of Things Security Policy

Zhan-Hui Gang
Monitoring and Emergency Institute
China Industrial Control Systems Cyber Emergency Response Team
Beijing, China
gangzhanhui@cics-cert.org.cn

Chang-Yue Yu*
Industry Management Promotion Center
China Electronics Standardization Institute
Beijing, China
*yuchangyue@aliyun.com

Hai-Bo Huang
Department of Economics and Management
Beijing University of Posts and Telecommunications
Beijing, China
poehuang1@163.com

Li-Jun Wang
Monitoring and Emergency Institute
China Industrial Control Systems Cyber Emergency Response Team
Beijing, China
wlj0228@163.com

***Abstract*—With the vigorous development of the Internet of Things (IoT) industry, the cybersecurity issues of the IoT are emerging. Putting the IoT cybersecurity issues into priorities has become a common practice in many countries around the world. In this paper, we expound on the relevant strategies, regulations, standards, guidelines, and other policy documents released by domestic and foreign governments in recent years. Firstly, the paper focuses on the content and characteristics of the IoT security policies of the US, EU, UK, Australia, then summarizes the development of China's IoT security policies. Based on these, the paper gives some suggestions for the development of IoT security in China.**

Keywords - Internet of things; security; policy; consumer

I. INTRODUCTION

The Internet of Things (IoT) has entered a new stage of leading development, as critical infrastructure, the IoT is aimed at realizing all things interconnected and intelligent in the construction of new infrastructure. It is expected that the utilization and expansion of cyberspace focusing on IoT will be a critical factor which determines national competitiveness [1]. The IoT is concerned about the technological competition and international pattern of significant countries, has been incorporated into the strategic planning of economic development in many countries, which has used to consolidate and enhance the competitive advantage of the IoT security industry in the world. With the development of 5G networks and the popularity of IPv6, the number of network attacks using IoT devices is increasing, and cybersecurity issues have become an essential factor for the practical application and sustainable development of the IoT. Many countries worldwide have attached great importance to the top-level design of IoT security and the construction of the policy environment. They promote the national IoT security and industry development from the perspective of multi measures, supervision of the IoT supply chain and consumer IoT security protection. By analyzing the characteristics of the IoT security policies in developed countries, such as the US, EU, UK, Australia, it can assist relevant institutions and enterprises in China to understand the development trend of foreign IoT security and accelerate the development of China's IoT security.

II. ANALYSIS OF MAJOR FOREIGN COUNTRIES' IOT SECURITY POLICY

A. US: Adhere to top-level strategic planning and policy guidelines

As one of the leaders and pioneers of the IoT technology, the development of national-level IoT security research and the strategic plan has become an essential reference to guide the development of the IoT in the US. At the end of 2016, the "10.21 Internet Outage" incident prompted the US to raise the security issue of the IoT to the height of homeland security, the US Department of Homeland Security issued a set of "Strategic Principles for Securing the Internet of Things (IoT), Version 1.0" the following month [2]. From the perspective of the federal government's responsibility to ensure the security of the IoT, the white paper defines cross-departmental cooperation, the promotion of national security awareness, the promotion of incentive measures, and the development of international standards. These principles stressed approaches and suggested practices to fortify the IoT's security and would equip stakeholders to make responsible and risk-based security decisions when they design, manufacture, and use internet-connected devices or systems. Since then, the US federal government has accelerated the development of IoT security policy documents to strengthen the top-level design of IoT security management, improve the management mechanisms, enhance the management and control capability. Since 2017, the US IoT security-related policies and regulations are shown in Table I.

TABLE I. THE US IOT CYBER SECURITY RELATED POLICIES AND REGULATIONS

Time	File Name	IoT security-related content
June 13, 2017	Promoting Stakeholder Action Against Botnets and Other Automated Threats	Seek broad input from private industry, academia, and civil society, and other security experts to strengthen the security protection capabilities of IoT terminal devices.
Sep 28,	SB-327 Information	Mandatory stipulates the necessary safety

978-0-7381-1141-4/20/$31.00 ©2020 IEEE
DOI 10.1109/ITCA52113.2020.00115

2018	privacy: connected devices	standards of consumer IoT devices in terms of safety, privacy, and trustworthiness.
June 25, 2019	Managing IoT Privacy, Cybersecurity Guidance	Update IoT devices, data, and personal privacy security policies and procedures in time.
Dec 10, 2019	2019 Federal Cybersecurity Research and Development Strategic Plan	Consider the security issues of the IoT in the process of building a reliable distributed digital infrastructure, increase investment in the research and development of IoT security, and enhance the strategic capabilities of IoT security.
Feb 5th, 2020	IoT Security Policy Principles	All stakeholders should take the overall IoT ecological security, focus on the broader ecosystem as opposed to device security alone, develop and utilize industry-driven core baseline capabilities and standards, avoid regulatory fragmentation, Promote global harmonization.
May 29, 2020	IoT Device Cybersecurity Capability Core Baseline	Proposed six aspects of the IoT device cybersecurity capability core baseline for securable IoT devices, including device identification, device configuration, data protection, logical access to interfaces, software update, and cybersecurity state awareness.

After three years of polishing, the "IoT Cybersecurity Improvement Act of 2020" was signed by Trump into law On December 4th, 2020. The bill proposed to improve the federal government's IoT cybersecurity by establishing a benchmark for internet-connected devices purchased or used by the federal government. The bill started from the source of product design to avoid the supply chain risk of the federal government, which stems from insecure IoT devices. The passage of the bill means that the US has taken an essential and due step in improving the security of the IoT.

B. EU: Strengthen the safety supervision of the IoT supply chain

Although there is a particular gap in the development of the IoT compared with the US, the EU is the first institution in the world to systematically propose the action and management plan of IoT [3]. It released the "Consumer Internet of Things Cybersecurity", which is the first international standard, expected to lay a benchmark for European and global IoT certification programs. Since the establishment of the IoT Innovation Alliance in 2015, the EU has paid great attention to the safety supervision of the IoT supply chain. In 2016, the European Commission, starting from the entire network and cloud, established a government certification framework, to ensure the privacy and security of the IoT by formulating laws and regulations, and compelling companies to comply with security standards and other authentication processes. In 2017, the European Commission released the "Cybersecurity Strategy for the European Union," proposing integrating the concept of "security by design" into the whole lifecycle of the IoT systems and components, providing a basis for the security supervision of the IoT supply chain. In 2019, the European Union Agency for Network and Information Security (ENISA) stressed the importance of embedding security protection capabilities into the manufacturing process of IoT devices. On November 9th, 2020, ENISA released the "Internet of Things Security Guidelines," which defined the IoT supply chain security from the whole lifecycle of demand design, product delivery, operation and maintenance, and disposal, to make better security decisions for stakeholders when building, deploying or evaluating IoT technology. Besides, the EU has launched an antitrust competition inquiry into the sector of IoT, and the 4th IoT Security Conference, which is around the integrity of IoT supply chain and the development of laws and regulations improved the security of the IoT supply chain and the robustness of the ecosystem.

C. UK: Focus on the security protection of consumer IoT

The UK is the first country to apply consumer IoT security regulations. The world's first IoT security practice guidelines launched by it, which provides a sufficient basis for the development of other countries' IoT security-related documents, and lay the foundation for the development of EU's first consumer IoT security global standard. Since 2018, the UK government has issued several security policy documents around the design of consumer IoT devices and software services, providing a practical basis for consumer protection. For example, the "Code of Practice for Consumer IoT Security" starting from the safety protection of smart products, 13 non-mandatory proposes based on results are put forward to strengthen consumer privacy and security protection. The practice of establishing a security benchmark for Internet-connected products and future IoT certification programs, it has incorporated into the "General Data Protection Regulation." To further combat the insecure factors of the IoT, the UK government has also formulated more stringent security regulations from the perspective of consumers, such as unique device passwords, easy contact with manufacturers, and explicit device lifetime. In July 2020, the UK government issued "Proposals for regulating consumer smart product cyber security - call for views," pointed out that slow processes and poor security in the safety reform of consumer smart products are still a commonplace phenomenon. The plan, which aims at improving the safety standards of consumer smart products, can establish a cybersecurity baseline for UK smart product market.

D. Australia: Guide the development of the IoT cybersecurity industry with policy.

Since 2017, the development of the IoT in Australia has gradually entered a burst period from the exploration period. To deal with the security problems in the IoT industry's growth, the Australian government has proposed the "Cyber Kangaroo" scheme [4], which plans to point out the security problems of their products through the safety rating system to remove obstacles for the development of IoT industry. In 2019, based on the IoT cybersecurity proposals and relevant standards of the UK, EU, and other countries, the Australian government started to formulate a series of voluntary IoT security practice guidelines, which provide the best practice guidelines for the industry of design IoT devices with embedded network security functions. Besides, to avoid the consumer market and the enterprise market from breaking the dividend bubble due to security issues in the development of the IoT industry, in September 2020, the Australian Cyber Security Center based on the 13 recommendations of the UK "IoT Security Practice Guidelines," made requirements to the end-users in the purchase, configuration, use, and maintenance of IoT device. The IoT security-related policy documents issued by the Australian government in recent two years, can be regarded as the necessary steps to improve the industrialization of Australian IoT cybersecurity. In November 2020, the Australian Government Department of Home Affairs issued the "Code of Practice Securing the Internet of Things for

Consumers," which will bring the most extensive security benefits in the short term. The Code of Practice is committed to improving people's awareness of security safeguards associated with devices, build greater consumer confidence in IoT technology and allow Australia to reap the benefits of greater IoT adoption.

III. CHARACTERISTICS OF FOREIGN IOT SECURITY POLICY

A. Device security capabilities and consumer privacy protection become the focus.

With the acceleration of the global 5G commercial and the popularization of IPv6, the IoT is exponentially growing towards an ecosystem interconnecting tens of billions of smart products [5]. The security issues of the IoT are also increasingly prominent. The security in the process of manufacturing, integrating, selling and using IoT device is becoming more and more critical. In the formulation of IoT security policies, the US, EU, UK, Australia and other developed countries, have taken on the trend of strengthening the security protection of the consumer IoT. The content focuses on changing the default passwords, advancing security updates and vulnerability management, minimizing exposed attack surfaces, ensuring the integrity of consumer data and device parameters, simplifying consumer operation procedures, and possessing secure communication and legal verification capabilities, etc. They can provide useful guidance for protecting the organization's IoT devices, consumer data and ecosystems.

B. Group collaboration to formulate policy standards becomes the first choice.

Throughout the foreign IoT security policy formulation agencies, most of the formulation work of the IoT cybersecurity strategy was based on the concept of win-win cooperation. For instance, the US relies more heavily on the private sector for IoT policy development, such as companies, and industry groups, academic institutions, professional societies, consumer groups, and other kinds of private sector organizations [6]. EU underlines the importance of cooperation and trust-building through public-private partnerships, and they stated that it would work with international partners and organizations, the private sector, and civil society to support national cybersecurity capacity building. The Department for Digital, Culture, Media & Sport is supported by 45 agencies and public bodies to develop the UK IoT security policy document. The working mechanism involving all social forces provides a fundamental guarantee for the promotion and application of documents.

C. The vulnerability management strategy has become a hot spot.

In the IoT cybersecurity practice guidelines, management guidelines, core baselines, and other policy documents establish a vulnerability disclosure policy and report management were more and more emphasized. Vulnerability management strategy mainly needs to provide a clear and transparent vulnerability disclosure police, establish a vulnerability reporting system for consumers, stipulate the reporting process of security researchers and other personnel clearly, and update the vulnerability disclosure strategy continuously. Besides, stakeholders or competent national authorities will collect, disclose, and share vulnerability information and track manufacturers to identify and rectify vulnerabilities.

IV. CHINA'S IOT SECURITY POLICY DEVELOPMENT

A. Development status

In 2009, the IoT became one of China's five critical development strategic emerging industries, and the cybersecurity issues of the IoT have gradually attracted attention. Regardless of the development plans, guidelines, safety regulations that have issued, or the technical standard specification that is being formulated, the security issues of the IoT are taken into consideration.

In 2014, the Ministry of Industry and Information Technology of the People's Republic of China (MIIT) mentioned that it is necessary to establish and improve the security guarantee system of the IoT and strengthen the formulation and implementation of security standards for the IoT [7]. The "13th Five-Year Plan" clearly pointed out that security is the prerequisite and guarantee for the development of the IoT. At the same time, it's necessary to adhere to the principle of safety and controllability. It was considering the development trend of IoT security, the "White Paper on Internet of Things Security," [8] published in September 2018 by the MIIT. It analyzed the security risks, proposed establishing a security protection strategy framework, and pointed out the future development direction and suggestions. In the same year, security technical standards for IoT such as the "Security Technical Requirements for the Perceptive Layer Gateway" and the "Technical Requirements for the Security of Data Transfer in the Internet of Things" were published successively. On August 11, 2020, the MIIT said that it would make a layout in critical areas such as 5G and IoT, by combining new-generation information and communication technology. And they will formulate relevant data security standards in variety with the development of the field itself and the demand for data security protection.

B. Underdevelopment

From the perspective of the development process and policy documents of the IoT cybersecurity in China, compared with the technical development, China's IoT cybersecurity policy specifications are still relatively slow, industry barriers and information islands still exist. There are still gaps in the formulation of laws and regulations, core baseline, standards and specifications related to the IoT security, and the deficiencies in the safety supervision and implementation of the IoT device is still insufficient in China. Simultaneously, due to the long chain of the IoT industry, a range of stakeholders have not fully participated in constructing the IoT cybersecurity ecosystem. Cross-domain and cross-industry interoperability and application coordination are not smooth, limiting the large-scale application of the IoT cybersecurity industry in China. However, with the substantial increase of industrial IoT device and consumer IoT device access, it also brings a large space for the development of China's IoT security policy documents and safety supervision.

V. Suggestions on Promoting the Security Development of IoT in China

According to analysis, the US, EU, UK, Australia carry out strategies from the perspectives of IoT cybersecurity policy, combined with the current development of China's IoT cybersecurity policy. The following suggestions are put forward for the development of IoT cybersecurity in China.

A. Give full play to the advantage of the government functions and formulate a national IoT security guidance document.

The government could give full play to the advantages of overall planning and top-level coordination, learn from the practical experience of the IoT security strategy, policies, regulations, and technical standards in foreign developed countries, and formulate a national IoT security development strategy, which integrated with China's development plan. We will strengthen the coordination of various government departments in policy and standard formulation, infrastructure construction and cybersecurity assurance. Improve the relevant legal systems and standards, form an IoT security baseline, which can be widely recognized by the government and industry is needed, and then promote the implementation of policy documents. Realize the use of law to arm the security of IoT, and provide a suitable environment for the safe, healthy, and orderly development of IoT.

B. Converge the strength of the IoT industry chain to build a secure ecosystem of the IoT.

The IoT industry could rely on the IoT Security Alliance, to organically connect the upstream and downstream stakeholders of the IoT industry chain. They should reach a consensus on integrating security covers the entire lifecycle of product design, development, production and deployment. We will jointly follow the best practices and requirements of IoT cybersecurity, strengthen the risk management of the supply chain, and collaboratively promote the construction of a domestic security ecology in terms of the IoT security requirements, solutions, standards and specifications, testing and certification, and application demonstrations, to promote the transparency of the entire IoT ecosystem.

C. Enhance the effectiveness of IoT safety supervision and accelerate the security layout of consumer IoT.

We should actively draw lessons from the typical characteristics of the UK, EU, and other countries in consumer IoT security supervision, and take the diverse needs of China's IoT security into account, adhere to the static policy and dynamic technology, and formulate the IoT security baseline and standard of China's consumer. Strengthen the safety supervision of IoT device manufacturers and suppliers, focusing on device configuration, data protection, vulnerability repair and other aspects. It is necessary to improve IoT consumers' awareness of security needs, encourage companies to provide available security components to the market, break the status quo of "ignoring security and eager to go public," and further enhance the governance ability and level of IoT device security and consumer privacy protection in China.

D. Implement a vulnerability disclosure policy of IoT and standardize the disclosure and disposal of vulnerability information

Base on the "Network Security Vulnerability Management Regulations (Draft for Comments)," we could develop the IoT security vulnerability management measures. According to the development of the IoT industry, the security level of various IoT devices stipulated. From the response time, submission interface, information sharing and other aspects of the IoT vulnerability disclosure process and disposal measures. With the help of relevant national vulnerability database platform, establish vulnerability reporting reward mechanism, encourage social forces to join in vulnerability management of IoT, and improve maintenance efficiency.

References

[1] Kyoung-Sik Min, Seung-Woan Chai, Mijeong Han, “An International Comparative Study on Cyber Security Strategy,” International Journal of Security and Its Applications, Vol. 9, 2015, pp. 13-20.

[2] DHS. 2016. Strategic Principles for Securing the Internet of Things (IoT), Version 1.0.. Washington, DC: US Department of Homeland Security.

[3] Li Xiangwen. “Europe, America, Japan and South Korea, and China's Property Development strategy of IoT——Global Development of IoT,” RFID, 2010, pp. 49-53.

[4] Johnson SD, Blythe JM, Manning M, Wong GTW, “The impact of IoT security labeling on consumer product choice and willingness to pay,” PLoS ONE, vol. 15, 2020, pp. e0227800.

[5] S. Ziegler, et al. "IoT6 – Moving to an IPv6-Based Future IoT," The Future Internet, vol. 7858, 2013, pp. 161–172.

[6] US National Institute of Standards and Technology, 2018, Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things, Gaithersburg: US Department of Commerce.

[7] MIIT, 2014, Critical points of Internet of things of the Ministry of industry and information technology in 2014, Beijing: Ministry of Industry and Information Technology of the People's Republic of China.

[8] CAICT, 2018, White paper on Internet of things security, Beijing: The China Academy of Information and Communications Technology.