

Brief Analysis of Security Protection Practice of Key Information Infrastructure in Communication Industry

Zhiliang Si *

Shanxi Communication Administration Bureau, Taiyuan 030012, China

* sizhiliang@122.gov.cn

Abstract. To solve the problem how to effectively identify critical information infrastructure challenges that the communications industry, improve pertinence and effectiveness of the security and protection work, this paper reports the legislative background of critical information infrastructure protection at home and abroad and the status quo, on the communications industry key information infrastructure security framework are discussed in this paper, by adopting the method of analytic hierarchy process (AHP), by calculating the key, Through the calculation of the critical degree, the paper proposes how to accurately identify the critical information infrastructure in the communication industry. This research is the latest practical exploration of the security protection work method of the critical information infrastructure in the communication industry, and is the urgent need of the current communication network security situation in China. It is hoped to take the implementation of the Regulations on the Security protection of Critical Information Infrastructure as an opportunity to publicize and promote the research method, continuously strengthen the security protection of critical information infrastructure, realize the high-quality development of the communication industry, and better empower the economic and social development.

Keywords: Critical Information Infrastructure; Network Security; Information and Communication Technology; Identification and Identification; Safety Protection.

1. Introduction

With the rapid development of information and communication technology, new technologies and businesses are fully integrated into political, economic, cultural, social and other fields. Communication networks are deeply integrated with public service, transportation, energy, finance, government and other industries, and all industries are increasingly relying on the critical information infrastructure of the communication industry. However, new Internet technologies and services are changing with each passing day, network attacks and sabotage methods are emerging one after another, and critical information infrastructure in the communications industry is facing increasingly prominent internal and external risks, and the security situation of communication networks and information systems is becoming increasingly severe. As the key support and core carrier of national economic and social development, it is related to the lifeblood of the country, economy and society. Once damaged or paralyzed, it will deal a fatal blow to the daily work and life of the public, the normal operation of economy and society, and even the core interests of the country and national security [1].

In recent years, the CPC Central Committee and The State Council have attached great importance to legislation on the security and protection of national critical information infrastructure. The General Secretary has repeatedly made important instructions to "strengthen the protection of critical information infrastructure and improve the ability to guarantee network security". On June 1, 2017, China's first laws and regulations related to critical information infrastructure "Network Security Law" [2] was formally implemented, which placed high emphasis on the security protection of critical information infrastructure from the national strategy for the first time. On September 1, 2021, the national special administrative rules and regulations of the critical information infrastructure security protection ordinance (hereinafter referred to as the regulations on the protection of) a formal, explicit protection category, the responsibility of the parties to the recognition rules and protection work department and operator has clear responsibilities, tasks, provides the relevant departments and fields with specific operational solutions, In particular, it points out the direction for the communication

industry to carry out security protection and provides a strong institutional guarantee for the in-depth development of critical information infrastructure security protection in China.

2021 is the first year of "difference" programming, the communications industry to implement the regulations on the protection as an opportunity, according to the strategy of "network power" and the central economic work conference, based on the new stage of development, carry out new development concept, build a new development pattern, should strengthen the communications industry key information infrastructure protection work, achieve high quality industry development, We will also empower all sectors of society to inject new impetus into high-quality economic and social development, and provide solid support for our high-quality development to get the 14th Five-Year Plan off to a good start.

In the spirit of the protection ordinance as guidance, this paper first introduces the status quo at home and abroad and the communications industry specific critical information infrastructure protection practice, probes into the key to the communications industry information infrastructure security framework of how to accurately identify that protect object, by calculating the key ways to determine whether the object belongs to the critical information infrastructure, The validity of the recognition method is verified by a practical case. In addition, the other four key protection links, such as security protection, detection and evaluation, monitoring and early warning and event disposal, are briefly analyzed, aiming to provide practical solutions with reference value for the development of the industry and further improve the pertinence and effectiveness of the security protection of critical information infrastructure in the communications industry.

2. Related Concepts

2.1 Definition of Critical Information Infrastructure

At present, there are two concepts in the world: critical infrastructure (CI) and critical information Infrastructure (CII). The definition of critical infrastructure (CI) is basically the same at home and abroad [3], which refers to the infrastructure providing essential public services for the country. These infrastructures are related to the national economy and people's livelihood. Once lost or damaged, they will cause serious economic losses or even disastrous consequences to families, society and the country. The concept of critical information Infrastructure (CII), as defined by the International Telecommunication Union (ITU), refers to the networks and information systems that support a country's critical infrastructure. Domestic latest definition of critical information infrastructure from September 1, 2021 formally implemented special administrative rules and regulations of the key information infrastructure security protection ordinance [4], CII refers to public communications and information services, energy, transportation, water conservancy, finance, public service, the electronic government affairs, national defense science, technology and industry, and other important industries and fields, And other important network facilities and information systems that may seriously endanger national security, national economy, people's livelihood, and public interests once they are damaged, lose their functions, or their data is leaked. In a large number of literatures, the boundary between CI and CII is fuzzy. Although CI is referred to in this paper, it is usually expressed by CII. Logically speaking, CII should be a part of CI. However, with the rapid development of information and communication technology and its continuous deep integration and application with all walks of life, THE network information security problems facing CI are becoming increasingly prominent. The focus of CI protection is gradually shifting from physical protection to network security and information system protection, making the concepts of CI and CII gradually converge. Mixed use of CI and CII occurs from time to time [5].

2.2 Definition of Critical Information Infrastructure for Communication Industry

According to the network security law and other relevant laws and regulations, the telecommunications ordinance in combination with the practical situation of the communications industry, the relevant departments to define key information communication industry infrastructure

refers to important areas once destroyed, is likely to harm public interests and national core interests and national security of information network, including computer room, passwords, network, security, infrastructure and important information system. General understanding of the communications industry key information infrastructure includes the communication network security and information system, is currently in a priority position and attack risk higher critical information infrastructure, including not only, the core network, access network, transport network and terminal and all kinds of support system and important physical facilities [6], asset size. To realize unimpeded communication, the security of communication physical facilities is the prerequisite. Traditional physical facilities in narrow sense include but are not limited to communication equipment, communication lines and supporting equipment that constitute communication network system. Among them, communication equipment refers to communication base station, microwave station, wireless local area network (WLAN) system, wired access equipment, communication terminals, etc. Communication lines refer to communication transmission media, including communication optical cables, cables, and sea cables. Auxiliary equipment refers to the equipment room, power environment equipment and other auxiliary facilities used to maintain the normal operation of the communication equipment.

3. Background

3.1 Domestic and International Situation

At present, the critical information infrastructure at home and abroad is facing a very severe network security situation, with frequent high-level persistent network attacks, threats and deterrence, extortion and other attacks, and network security has increasingly become a global issue [7]. In May 2021, a hacker group attacked the system of The Coronier Corporation, the largest refined oil pipeline provider in the United States. The national energy supply network was forced to shut down for a week, which dealt a huge blow to the energy supply of the East Coast of the United States. The US government was forced to declare an immediate state of emergency. The attack was the worst ever on the US energy system and the first time a national emergency was declared over a cyber attack. Less than a month after the attack, JBS, the world's largest US meat processing company, was attacked by hackers and shut down, which adversely affected the normal operation of the whole US industrial chain.

In recent years, a country has restricted the business development of a high-tech company in China by cutting off the supply of key components under the pretext of network security, aiming to hit the autonomous control ability of China's key information infrastructure. What is more serious is that some hacker organizations use network attacks to destroy critical information infrastructure, with the purpose of gathering intelligence and stealing information in order to obtain unfair competitive advantages. Since the outbreak of COVID-19, some foreign organizations have launched a series of cyber attacks and data theft against China. The Indian hacker group "White Elephant" took the opportunity of the COVID-19 outbreak to attack a Chinese government agency, and a hacker from a Spy agency in Taiwan used fake epidemic reports to obtain important domestic information.

In addition, major foreign organizations such as Iran's railway system, Chile's banking system and Ireland's health system have been exposed in a series of cyber attacks, and the communications industry, as an important carrier of critical information infrastructure in other industries, has been almost immune. Network attacks and data theft incidents are common in the communications industry of various countries, and communication network security risks are increasing day by day, triggering discussions and continuous attention in the field of security protection of key information infrastructure in various countries [8]. Most countries say it is urgent to strengthen the protection of critical information infrastructure in the communications industry to cope with the increasingly severe situation of network and information security.

3.2 Importance and Necessity

3.2.1 The Key Information Infrastructure of the Communication Industry is the Basic Guarantee

Nowadays, the communication industry plays a more and more prominent role in the basic guarantee of national economic development. With the rapid development of information and communication technology, information and communication technology *are* increasingly integrated and applied to all kinds of traditional industrial infrastructure, public service, energy, finance, e-government and other industries continue to improve the informatization degree. All kinds of key information infrastructure in the communications industry are rapidly evolving to be cloud-based, broadband-based and ubiquitous, playing an important role in supporting the development of the digital economy and society. The critical information infrastructure of the communication industry is increasingly becoming an essential part of the traditional industry infrastructure. Without the basic guarantee of the communication network, any other protection measures are empty talk. In view of the extreme importance of ICT in today's society, this paper proposes a critical information infrastructure industry model based on ICT, as shown in Figure 1. Information and communication technology application in all walks of life, the communications industry key information infrastructure and other critical information infrastructure interlocking, the people, life cannot leave the communication network, the government of the people's livelihood is dependent on the communication network, the national economic and social development is more inseparable from the communication network, all walks of life more and more dependent on information and communication technologies and the Internet. As we all know, in the event of major events, floods, earthquakes and other natural disasters, the priority is to ensure the smooth operation of communication networks. The "Protection Regulations" has identified the critical information infrastructure for communication as a national priority, which shows the importance of critical information infrastructure in the communications industry.

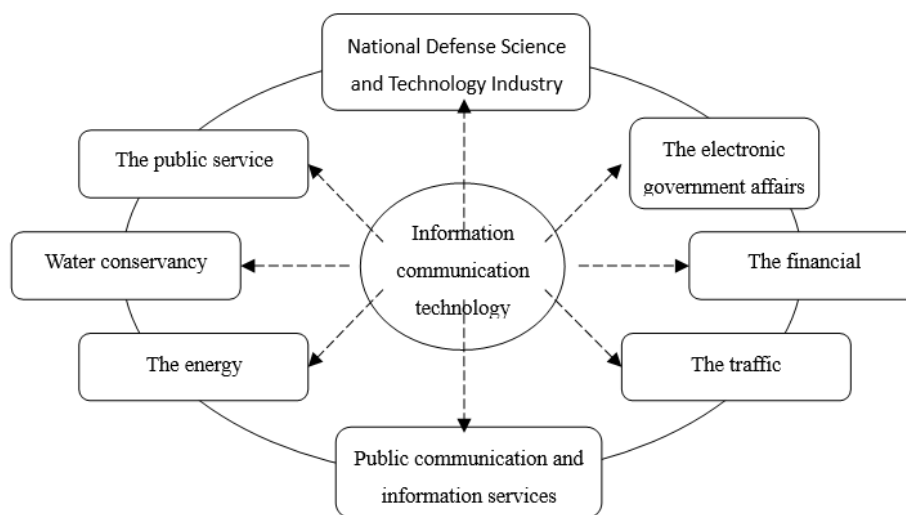


Figure 1. Critical information infrastructure industry model

3.2.2 Practical Needs of Implementing Major National Development Strategies

The "Network power" strategy and the construction of "digital China" are the major development strategies of China in the new period made by the CPC Central Committee from the overall development of the cause of the Party and the country, and both emphasize the necessity of strengthening the security protection of key information infrastructure. Under the impact of the third scientific and technological revolution, China's communication technology has led the world from the beginning of reform and *opening* to the present 5G network, and from the flying pigeon message and beacon fire message to today's omniscience and interconnection of smart phones and smart

devices, which cannot be separated from the national decisions and long-term strong support for the development of the communication industry. Since last year, the communications industry has faced up to the severe challenges of the COVID-19 epidemic by giving full play to the role of big data monitoring and analysis and supporting targeted epidemic prevention and control. It has played an important role in supporting COVID-19 prevention and control. As a strategic public infrastructure to promote China's economic and social development, it is a key area to maintain national network security, but it is also the target of attacks or threats by hackers and other illegal organizations. The more dependent the infrastructure of other industries is on ICT, the more it will be affected or damaged by malicious attacks. In particular, security incidents of key infrastructure in important industries and fields may seriously endanger public interests, national economy and people's livelihood, and even national security. As can be seen from the industry model of critical information infrastructure in Figure 1, other critical information infrastructure is heavily dependent on information and communication technology and critical information infrastructure in the communications industry. Once the communication network and information system services are damaged or data is leaked, it will cause a chain blow to related industries and the consequences will be unimaginable. Therefore, strengthening the security protection of key information infrastructure in the communications industry is very necessary to maintain national network security, is the inevitable requirement of implementing the overall national security concept, but also the practical need to implement the "Network power" strategy and build a "digital China".

4. The Status Quo

4.1 The Foreign

Countries all over the world attach great importance to the security protection of critical information infrastructure. The United States, the European Union, Japan and other developed countries are actively exploring the formulation of mechanisms and policies for the security protection of critical information infrastructure. This section focuses on the advanced experience and practices of the United States, the European Union and Japan.

4.1.1 The United States Actively Carries out Legislation on Critical Infrastructure

After more than 20 years of accumulation of practical experience, the us infrastructure security protection system has been basically formed [9]. As early as July 1996, the Then PRESIDENT of the United States issued the Critical Infrastructure Protection Order, pointing out that the normal operation of the country is extremely dependent on critical infrastructure, and the protection of infrastructure should become a new focus of national security protection. In particular, the outbreak of the "9·11" incident in the United States forced the American government to realize the necessity of improving the security protection of critical information infrastructure, and accelerated the legislation of critical infrastructure in the United States. In 2002, the government introduced the critical infrastructure information protection act, to the cognizance of critical infrastructure protection principles, procedures, conditions, measures and regulations on disposal treatment made a more detailed, and clear the key infrastructure for the department of homeland security, the administrative department of each relevant department in charge of the business to have a clear division of responsibilities, management system since its establishment is relatively stable. In terms of standard system, in February 2014, the U.S. government released "America's critical infrastructure network security framework", as a national information security industry guidelines, the specification will be the critical infrastructure security protection system is set to the five aspects of the life cycle of the prevention and control system, recognition, protection, detection, response, recovery, the main standard is information security management standard ISO/IEA27001 and international general information audit standard COBIT. In terms of the scope of protection, American laws and regulations clearly define the categories and scope of protection. For example, the Clinton administration identified eight categories of critical infrastructure, the Bush administration identified

18 categories of critical infrastructure, and the Obama administration identified 16 categories of critical infrastructure. The definition has always been relatively clear. In terms of implementation procedures, the US critical information infrastructure protection procedures are: first, identify risks and threats, second, identify network security needs, and finally select risk prevention and control measures. In recent years, with the increasingly severe situation of network security, the US government has significantly increased the financial support for critical information infrastructure, continuously strengthened the Critical information infrastructure protection Act and government intervention, dynamically adjusted the network security protection strategy, and continuously strengthened the security protection of critical infrastructure [10].

4.1.2 The EU Proposes to Strengthen the Protection of Critical Infrastructure from a National Strategic Perspective

It is reported that the European Union first proposed the critical infrastructure protection measures in 2004, defined the relevant concepts in a unified way, and then strengthened them through a series of policies and regulations. In 2005, the European Plan for the Protection of Critical Infrastructure was implemented, which set out the goals and requirements for the protection of critical infrastructure, identified responsible departments and competent authorities, and established an information sharing, evaluation and certification mechanism. In 2008, the Eu Directive on The Identification and Safety Assessment of Critical Infrastructure was issued to further clarify the assessment methods for critical infrastructure. The Directive on Strengthening the Protection of Critical Infrastructure in the Eu issued in 2009 refined the assessment method to identify and confirm critical infrastructure through specific assessment and ranking. The Eu Action Plan for the Protection of Critical Infrastructure provides specific protection measures for member states, including preparedness and prevention, detection and response, mitigation and recovery, etc. In the EU Security Alliance Strategy, the prevention and recovery capacity of critical infrastructure is taken as the top priority of network information security work [11]. Eu member States have formulated specific protection implementation plans in line with their national conditions and based on the protection work of eu critical infrastructure in light of local conditions. In 2005, Germany successively formulated the Regulations on the Protection of National Information Facilities and the National Strategy for the Protection of Critical Infrastructure, and put forward the protection strategic plan. In 2010 and 2011, the UK issued two National Infrastructure Strategies, defining the national critical infrastructure development plan and focusing on the protection of critical infrastructure.

4.1.3 Japan Focuses on Strengthening the Construction of Critical Information Infrastructure Protection System

The Japanese government has always been concerned about the protection of critical information infrastructure in key domestic areas and has focused on building secure and reliable critical information infrastructure. In terms of institutional construction, the Basic Law on Building an Advanced Information and Communication Network Society was implemented in January 2002 to clarify the definition of information and communication network security, formulate the policy of priority development of information and communication network, and provide policy guarantee for the security protection of key infrastructure [12]. In December 2005, the Action Plan on Information Security Measures for Critical Infrastructure was promulgated, stipulating that the basic information systems corresponding to 10 categories of critical infrastructure, including telecommunications, finance, electric power, railway, civil aviation, medical care, government affairs, water conservancy, gas and logistics, should be identified as critical information systems. In October 2013, the International Network Security Strategy Network Security Cooperation Plan was issued, which emphasized the coordination and cooperation among relevant departments and the international cooperation when necessary, as a specific action plan for the implementation of the policy [13]. In terms of organizational system, the Cabinet secretariat is the main responsible department, with a clear division of labor among protection departments. Among them, the Cabinet Secretariat has overall responsibility for critical infrastructure and cyber security, the Ministry of Interior and

Communications is responsible for information and communication network system security and related policy formulation, the National Police Agency is responsible for domestic cyber crime, and the Ministry of Defense is mainly responsible for cyberspace based national security. In the past 20 years, the Japanese government has basically established a key information infrastructure protection system based on legal system guarantee, with the structure of protection organization system as the key, and with technical support and human, financial and material support as the backing.

4.2 The Domestic

As the core base of normal economic and social operation, the key information infrastructure of communication industry is facing more and more prominent network risks and security situation. The CPC Central Committee and The State Council attach great importance to it. Relevant departments actively fulfill their duties, and all communication operators earnestly fulfill their main responsibilities to jointly escort the safe and reliable operation of key information infrastructure.

4.2.1 Actively Carry out Legislation on Security Protection of Critical Information Infrastructure

China continues to strengthen the top-level design of critical information infrastructure protection and actively carry out legislation. In February 2014, At the first meeting of the Central Cyberspace Leading Group, General Secretary Xi Jinping emphasized that critical information infrastructure is the basic guarantee for a cyber power, and the protection of critical information infrastructure should be strengthened to improve the capability of network security guarantee [14]. In June 2017, the Network Security Law was officially implemented, which for the first time clarified the concept of critical information infrastructure, the scope of protection and the relevant provisions for ensuring operation security from a legal perspective, and clarified that the state would focus on protecting eight major industries, including public communication and information services [15]. After four years of experience in the practice exploration and accumulation, special national administrative regulations, the critical information infrastructure security protection ordinance in September 1, 2021 formally implemented, earnestly to the network safety "information about critical infrastructure protection rules into effect, further illustrate its role in the position in national important strategy resource. Regulations on the protection of not only established the protection category, decision rules, clear responsibility, also stipulates that the operator's legal liability, etc, especially in view of the fact that communication network has the characteristics such as fundamental, overall, to establish communication key information infrastructure to be especially national priority protection key, provides the security and protection work has more practical and more specific legal basis.

4.2.2 Specific Practice in Communication Industry

As the base of critical information infrastructure, critical information infrastructure of communication industry provides network communication and information service for critical information infrastructure of energy, finance, public service and other important industries. Once it is attacked and damaged by network, it will inevitably lead to very serious consequences. In recent years, the Ministry of Industry and Information Technology, as a protection department, has been guided by the important idea of becoming a cyber power. On the one hand, we have stepped up efforts to build and protect key information infrastructure and actively promoted the building of digital China. At present, China has 16 national Internet backbone direct connection points as important national communication hubs, the total number of mobile communication base stations will soon exceed 10 million, and the completed 5G base stations will soon exceed 1 million. 5G networks now cover all prefecture-level cities, more than 95 percent of counties and 35 percent of towns and townships in China. China has the world's largest fiber-optic network and 4G network. The total length of fiber optic cable lines in China has exceeded 50 million kilometers. Fiber optic broadband is being upgraded to gigabit, and the capacity of network communication network services and supply has been further enhanced. On the other hand, strictly implement the "Network Security Law", actively perform the communications industry network information security supervision responsibilities. It

has continuously strengthened ecological governance of communication networks, promulgated more than 10 departmental regulations on communication network security protection, including the Management Measures for Communication Network Security Protection and the Management Provisions for International Communication Facilities Construction, issued more than 20 normative documents for the communication network industry, and implemented more than 300 standards for the communication network industry. We have actively organized and carried out special rectification actions in the Internet industry for many years, making the Internet environment clearer.

While the industry has made some progress in protecting critical infrastructure, the future looks promising. But the challenge is everywhere, such as communication industry key information infrastructure protection system to be perfect, that detailed rules for the implementation, monitoring and early warning, response, recovery system is not perfect, potentially dangerous threats of network security situation is still complicated, the communications industry critical infrastructure protection work a long way to go.

5. Practice and Discussion on Security Protection Framework of Critical Information Infrastructure in Communication Industry

In February 2014, the U.S. government released the ascending key infrastructure network security framework, the framework focuses on the network security risk control of the industry a "common language", based on industry standards and successful practice to control risk, network security has become the key information in the field of various industries infrastructure network security protection framework [16]. The core of the framework includes functions, categories, sub-categories and reference materials. It describes a large number of activities (categories) carried out to achieve network security objectives, provides valuable guiding cases or relevant literature as a reference, and shows a series of achievements in network security risk control. Functions are key elements at the core of the framework, including identification, protection, detection, response and recovery. Among them, identification function is the basis for effective use of the framework, protection function is to avoid potential network security events, detection function can discover network security events in time, response function is to contain the impact of potential network security events, recovery function can restore normal operation in time, reduce the impact of network security events.

In December 2019, China issued the Basic Requirements for Network Security Protection of Critical Information Infrastructure (draft for approval) [17] in Beijing, which proposed five key links, including identification, security protection, detection and evaluation, monitoring and early warning, and incident disposal. Among them, identification is the basis, the key to safety protection is to develop and implement safety protection measures, detection and evaluation focus on finding potential risks, monitoring and early warning is to send alarm signals before the threat comes, event disposal requires effective measures and timely restoration of normal services. The five key links are basically consistent with the five functions of the US security framework, providing a fundamental guide for us to carry out the network security protection of critical information infrastructure.

At present, there is a lack of specific identification methods for critical information infrastructure in the communication industry, and the implementation rules of security protection need to be improved. The existing similar methods are too macro and not specific enough [18]. To solve the problem how to effectively identify critical information infrastructure that the communications industry, improve pertinence and effectiveness of the security and protection work, this section is proposed in the national key information infrastructure network security protection basic requirements ", on the basis of discussing establishing the communications industry key information infrastructure security framework (see figure 3). This paper mainly analyzes how to accurately identify the critical information infrastructure of the communication industry, aiming to provide reference for the security protection of the communication industry [19].

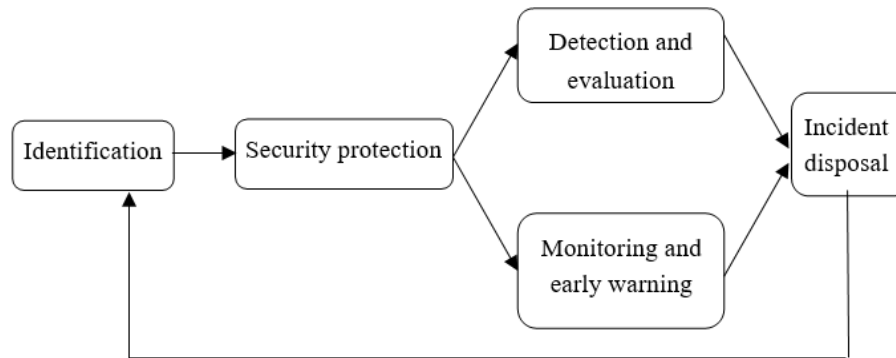


Figure 2. Security protection framework of critical information infrastructure in communication industry

5.1 Identification

First, it is necessary to accurately identify which infrastructure belongs to the critical information infrastructure of the communication industry, so that more targeted protection can be carried out. Developed countries such as the United States and Europe usually adopt consequence-based identification standards, which mainly consider such factors as human casualties, national economic losses and security impacts [20]. Work department of the protection ordinance provides protection in our country should combine actual industry areas, formulate their own critical information infrastructure that rules, in accordance with the rules of organization that work in the field of industry, and the clear rules should consider three factors, one is the network infrastructure and information system for the field of industry, the importance of key core business, The second is the harm caused by the destruction of key facilities and systems, and the third is whether there is no other associated impact.

Specific to the communication industry, combined with the actual situation of the industry and the field, according to the communication network managed by the communication management department and the Impact of network attack and system destruction on the national economy and society and the people to identify the communication key information infrastructure. In this paper, the identification object of critical information infrastructure in communication industry is analyzed from the perspective of communication network. If the network function is divided, the communication network can be divided into service network, transmission network and support network.

5.1.1 The Identification Process Includes Three Steps

The first step is to identify the identified object. 1) Business network identified objects.

Service network refers to the network that undertakes different communication services and mainly provides various communication services for the public. Switching node equipment is its core component. The service network mainly consists of fixed communication network, mobile communication network and Internet. The subdivided objects of fixed communication network include provincial long-distance network, local network gateway bureau, etc. Mobile communication network subdivision includes provincial long-distance network, core switching network, short message network, local network gateway office. Internet subdivision objects include domain name service system, information service system, online payment system, Internet data center (IDC) and so on.

2) Identified objects of transmission network

Transmission network refers to the transmission and transmission system, which provides transparent information transmission channels for the timely distribution of circuits required for interconnection between switching nodes or service nodes. The core elements of the transmission network mainly consist of plug - in multiplexer and digital cross - link equipment. Transmission

network subdivision objects include provincial synchronization network, provincial backbone optical transmission network.

3) Support network identification objects

The support network is the support system of the communication network. Provides signaling, management, and synchronization functions for the service network as required. The subdivision object of support network includes IP man, broadband access network, provincial message network, IT bearer network integrated network management system, etc.

4) Other identified objects

The identified objects should focus on the same business system, and the integrated management system should be identified according to its main purpose. In addition to all subdivision objects of business network, transmission network and support network, the identified objects should also include office support systems such as OA system and ERP system and auxiliary service systems such as official website and customer service call system.

5.1.2 The Second Step is to Calculate the Critical Degree of the Identified Object

Table 1. Subdivision description and specific assignment of key degree evaluation elements

the three evaluation	factors are subdivided to describe	the specific assignment
Importance	More than 10 million communication users	3
	More than 30 million communication users	4
	More than 50 million communication users	5
	The number of active users exceeds 10% of total registrations	3
	The number of active users exceeds 30% of total registrations	4
	The number of active users exceeds 50% of total registrations	5
	3000 standard rack or larger data centers	3
	5000 standard rack or larger data centers	4
	8000 standard rack or larger data centers	5
The harm	More than 5 million personal information leaks	3
	More than 10 million personal information leaks	4
	More than 15 million personal information leaks	5
	Leading to the disclosure of sensitive information about 500 organizations	3
	Leading to the disclosure of sensitive information about 1,000 organizations	4
	Leading to the disclosure of sensitive information about 1500 organizations	5
	Affecting 30% of personnel activities in the municipal administrative areas	3
	Affecting 30% of personnel activities in the provincial administrative areas	4
	Affecting 30% of personnel activities within the national administrative areas	5
Associated impact	Affects the normal operation of one or two other industries and fields	3
	Affect the normal operation of 3-5 other industries and fields	4
	Affect the normal operation of more than 5 other industries and fields	5
	Indirectly causing economic losses of more than 100 million yuan	3
	Indirectly causing economic losses of more than 200 million yuan	4
	Indirectly causing economic losses of more than 300 million yuan	5

The critical degree can be calculated according to the three evaluation factors of the importance, harmfulness and relevance of the factors considered in the identification rules of critical information Infrastructure Security Protection Regulations. The key is to assign values to the three evaluation elements of the critical degree, and then use the critical degree estimation formula to calculate the critical degree. In this paper, the assignment interval of critical degree evaluation elements is set at 3-5, and each evaluation element is independent of each other. If the identified object is lower than the subdivision description standard, the value can be assigned to 2 for estimation.

The critical degree estimation formula is as follows:

$$D = \text{Round} 2 \left\{ \text{Log}_2 \left\{ \left[a \times 2^I + b \times 2^H + c \times 2^R \right] \right\} \right\}$$

Where, D represents the critical degree value, Round2 { } represents the reserve of two decimal points after rounding, Log2 { } represents the log value based on 2, I represent the importance evaluation factor, H represents the hazard evaluation factor, and R represents the relevance impact evaluation factor. A, B, and C respectively represent the proportion of subdivision description of importance evaluation factors, subdivision description of hazard evaluation factors, and subdivision description of relevance impact evaluation factors. $A + B + C = 1$, and A, B, and C all ≥ 0 . For the convenience of calculation, it is assumed that the results are completely consistent through comparison of judgment matrices, and the weights a, B and C are all proposed to be 1/3, indicating that the three evaluation elements have the same importance.

5.1.3 The Third Step is to Determine Whether it Belongs to the Critical Information Infrastructure of the Communication Industry

The critical degree value D is estimated by the formula $D = \text{Round} 2 \left\{ \text{Log}_2 \left\{ \left[a \times 2^I + b \times 2^H + c \times 2^R \right] \right\} \right\}$. If $D > 3$, it can be determined that the identified object belongs to the critical information infrastructure of the communication industry; if $D \leq 3$, it can be determined that the identified object does not belong to the critical information infrastructure of the communication industry.

Taking a certain big data center of Shanxi Mobile as an example, the identification process of its infrastructure (system) is as follows: first, the identification object, namely a certain big data center of Shanxi Mobile, is identified as the object of Internet segmentation; The second is to calculate the size value D of the critical degree. First, the evaluation elements are subdivided and assigned specific values. Importance subdivision describes data centers with more than 3000 standard racks, so importance $I=3$. As a big data center of Shanxi Mobile is the main data center of major operators in the administrative region of Shanxi Province, 30% of personnel activities in the provincial administrative region may be affected by network attacks (hazard subdivision description), so the hazard $H=4$; The damage of a big data center of Shanxi Mobile may lead to the normal operation of two industries and fields, such as municipal public service and e-government, so the correlation impact $=3$; Now, we put the detailed description of the three evaluation elements into the formula $D = \text{Round} 2 \left\{ \text{Log}_2 \left\{ \left[a \times 2^I + b \times 2^H + c \times 2^R \right] \right\} \right\} = 3.42$, so it can be determined that a big data center of Shanxi Mobile belongs to the key information infrastructure of the communication industry.

After confirmation with experts and multi-party verification, a big data center of Shanxi Mobile really belongs to the critical information infrastructure of the communication industry, which verifies the validity of the calculation results.

This section on key information communication infrastructure that is in the critical information infrastructure security protection ordinance as importance, harmfulness and correlation rules to consider factors such as evaluation factors, the evaluative factors of the three types of subdivided descriptions and assignment, adopt hierarchical weighted decision analysis method (AHP), the combination of qualitative and quantitative, The systematic and hierarchical analysis is helpful to provide reference for the identification of critical information infrastructure in the domestic

communication industry. However, there are still some shortcomings in the specific practice, such as the lack of accurate data support for the specific assignment of subdivision description of each evaluation element. It is hoped that relevant departments can provide more accurate data for verification.

5.2 Security Protection

Various telecom operators' enterprise should be in strict accordance with the "law of network safety, the communication network security protection measures for the administration and other relevant laws and regulations, and actively carry out communication network security protection work, timely find security threat, eliminate safety hidden trouble, improve the overall level of the communication network security, safeguard social and economic developing positive health [21]. First, establish a communication network security management system to strengthen institutional guarantee. Formulate the communication network security protection system and standard system in a timely manner, clarify the management system, security strategy, implementation rules, technical measures and organizational guarantee for the network security protection of critical information infrastructure in the communication industry, and timely revise and adjust according to work needs. Second, improve working mechanisms and strengthen organizational support. Establish communication network security work leading group, set up full-time institutions, security management personnel, regularly organize and carry out education training and assessment. Establish and implement cybersecurity assessment and supervision and accountability mechanisms, include cybersecurity protection management in work assessment and performance assessment, and carry out supervision, inspection and assessment management on a regular basis. Third, improve the communication network security protection strategy, implement the "three synchronization" requirements of network security for critical communication information infrastructure, namely, synchronous planning, synchronous construction, and full-cycle synchronous security protection measures, and continue to enhance the capabilities of intrusion detection, antivirus, vulnerability mining and other key protection technologies. Establish a security protection system for critical information infrastructure in the communications industry covering physical facilities, network facilities, information systems and platform applications, and continuously improve the capability of in-depth defense against communications network security risks.

5.3 Detection and Evaluation

Accurate assessment of potential risks and main security risks of critical information infrastructure in communication industry is the premise of effective risk resistance. Various telecom operators enterprise should establish and improve the critical information infrastructure security testing evaluation system, the main test evaluation system and network security protection work to carry out the situation, will test evaluation throughout the communications industry key information infrastructure of the procurement, construction, operation, maintenance and so on various stages throughout the life cycle, but in the different stage, the emphasis should be different. During new construction, reconstruction, or expansion, test and evaluate the adjusted part of the new construction or adjustment to assess whether there are network security risks. Meanwhile, spot check and test the security risks of the communication network. If hidden security risks or risks are found, immediately rectify them. Based on the changes of communication network security threats and risks, timely detection and evaluation should be organized at least once a year to dynamically adjust communication network security policies. Regularly entrust third-party institutions to carry out risk assessment and compliance evaluation of network units, including but not limited to management status, assets, IP, network architecture and other information.

5.4 Monitoring and Early Warning

All communication operators should combine the actual situation of the industry, strengthen the security ability of continuous monitoring and timely warning, and make every effort to do a good job

in early warning and prevention of communication network security. First, actively formulate the industry monitoring and warning and information notification system, timely understand the operation status of communication critical information infrastructure and communication network security situation, analyze whether the current security strategy, implementation rules and control measures are reasonable and effective, and timely adjust according to work needs when necessary. Second, actively implement monitoring and early warning technical measures, timely understand the communication network security situation. If there are any signs of harm to communication network security and information system, the monitoring mechanism should automatically alarm by means of dialog box or email, and the security warning information should include basic information, harm and consequences, and specific countermeasures. After receiving the early warning information, it shall comprehensively analyze and judge the early warning information, take timely protective measures to respond to the early warning information, start the network security emergency plan when necessary, remove the early warning in time after controlling or eliminating security risks, and report to the relevant departments according to the relevant provisions.

5.5 Incident Disposal

Communication operators should strengthen the ability to deal with communication network security incidents, and the key is to make emergency plans. The emergency plan should specify the emergency maintenance items, handling process, and recovery time when the communication network is attacked or the information system fails. It should not only handle the communication network emergency of the organization, but also assist in handling the communication network emergency of other related organizations. Once a communication network security incident occurs, it is necessary to immediately handle the incident according to the emergency plan disposal process, conduct forensic analysis of communication network information security, and try to restore its damaged functions or services, so that the communication network and information system can be restored to normal in the shortest time. In the process of communication network event disposal, the whole process situation of event disposal shall be recorded in detail, relevant information shall be collected, details of event disposal shall be evaluated, causes of the event shall be analyzed, suggestions and matters for attention shall be put forward, and a complete event handling report shall be formed. After the communication network and information system are restored, experience and lessons should be summed up in time, event handling cases should be included in training procedures, and training of event handling ability should be strengthened to avoid similar damage or failure of communication network and information system again. The vitality of communication network security emergency plan also lies in regular assessment, revision and continuous improvement, and its effectiveness lies in irregularly organizing emergency drills. At least one network security emergency drill should be organized every year [22]. At the same time, sufficient human, material and financial support should be provided to provide a strong organizational guarantee for timely and effective disposal of communications network security incidents.

6. Conclusion

The key information infrastructure of the communication industry is fundamental, overall and pioneering, carrying other key information infrastructure, affecting the whole body. The promulgation of the Regulations on the Security protection of Critical Information Infrastructure is a specific measure to implement general Secretary Xi Jinping's strategy of becoming a "cyber power" and building a "digital China", and provides systematic guidance and work guidance for the communications industry to carry out security protection. However, rapid progress in information and communication technology, the communication industry in our country key information infrastructure security situation is still grim, the network security prevention and control ability are not enough to effectively resist high strength and the sustainability of network attack, and, once

organized attacks, is likely to cause significant network security events, even threatening economic society safe and stable and healthy operation.

It is hoped that the security Protection Framework of critical information Infrastructure in the Communication industry, especially the identification and identification method of calculating the critical degree, can effectively solve the identification and identification problems of critical information infrastructure, and improve the effectiveness and pertinence of the security protection work in the communication industry. At the same time, we also hope to get the attention and promotion of relevant departments. We can try to carry out pilot projects in some regions, and try to build a comprehensive defense system of key information infrastructure in the communications industry through more practices, to escort the strategy of becoming a cyber power and building a digital China.

References

- [1] DAI Yuanhao. Importance of Network Communication Security and Technical Maintenance Measures [J]. Digital Communication World, 2020,(2):100.
- [2] network security law of the People's Republic of China [EB/OL]. HTTP: // https:// baike.so. com/ doc/24210940-24838928.html.
- [3] He Yaozhong, GUO Xiaofeng. Network Security Technology and Application, 2017,(8):15-17. (In Chinese).
- [4] Of the State Council announced the critical information infrastructure security protection ordinance. [EB/OL]. (2021-08-17). https://www.guancha.cn/politics/2021_08_17_603249.shtml.
- [5] Zhou Yachao, LIU Jinfang. Analysis of scope and Characteristics of critical Information Infrastructure [J]. Cyberspace Security, 2018,(10):56-60.
- [6] LI Jiandong, ZHANG Yan, SHENG Min, et al. Science in China: Information Science, 2019, (8):949-962.
- [7] Chen Yuehua, Chen Faqiang, ZHANG Jinping, et al. Comparative analysis of foreign typical critical information infrastructure identification methods [J]. Confidentiality Science and Technology, 2020, (9): 63-68.
- [8] Zhang Li. Current Situation and Countermeasures of Communication Network Security [J]. Information System Engineering, 2017,(7):60.
- [9] Zhang Chi, Cui Zhanhua. Information Security Research, 2017,(8):736-746.
- [10] Yan Xiaoli, Meng Hongjie. Information Security Research, 2017, (10):941-945.
- [11] Liu C R, Sun B Y, ZHANG Z, et al. Interpretation and Review of eu Cyber Security Act [J]. Secret Science and Technology, 2019,(12):51-56.
- [12] Liu Jingjuan. Key Information Infrastructure protection legislation in the United States, Japan and South Korea [J]. Confidentiality Science and Technology, 2016,(7):16-20.
- [13] Zhou Ruijie. Research on the Institutional framework and Mode characteristics of Japanese Network security information sharing [J]. Science & Technology and Law.2020,(6):85-94.
- [14] Huang Daoli, Fang Ting. Journal of Network and Information Security, 2016, (3):10-16.
- [15] [Xie J, WANG Y S. Network Security Law effectively promotes the protection of national critical information infrastructure. Legal Review.2020,(29):130-131.
- [16] Luo Qiang, Wu Shaohuan, ZENG Mengqi. Communications Technology, 2017,(8):1816-1821. (In Chinese).
- [17] The information security technology key infrastructure network security protection basic requirements (draft) for [EB/OL]. (2020-02-24). <https://www.freebuf.com/articles/security-management/227378.html> The.
- [18] Gao Huanxin, Gao Yongqian. Information Technology and Network Security, 2018, (5):37-40.
- [19] Feng Yanchun. Accelerate the construction of national critical information infrastructure security guarantee system [J]. China Information Security, 2016,(11):42-46.

- [20] Feng Yanchun, Hu Rongquan, TAN Yuanyi, et al. How to identify the boundary of critical Information Infrastructure [J]. China Information Security, 2018,(12):99-101.
- [21] Gao Yue. Current Situation, Problems and Countermeasures of critical information infrastructure security protection in China [J]. Network Security and Informatization.2021,(4):21.
- [22] Wu Bo, Zhao Yong. Network security in the us and Europe series drill enlightenment on network security system construction in our country [EB/OL]. (2018-04-02). <https://www.secrss.com/articles/1786>.