Research on Cybersecurity Risk Prevention and Control of New Infrastructure

Lina Zhu¹, Zhentao Ma¹, Haibo Huang¹,²* and Min Yan³

¹ China Industrial Control Systems Cyber Emergency Response Team, Beijing, 100040, China
² College of Economics and Management, Beijing University of Posts and Telecommunications, Beijing, 100876, China
³ Trusted Computing and Information Assurance Laboratory, Institute of Software Chinese Academy of Sciences, Beijing, 100190, China

*Corresponding author’s e-mail: huanghaibo@cics-cert.org.cn; poehuang1@163.com

Abstract: Currently, the new infrastructure has entered the stage of intensive deployment. While driving the integration of innovative applications of new generation information and communication technologies such as 5G, and accelerating the process of digital transformation, new infrastructure is also facing the challenges of complex and diverse cyber attacks and increasingly severe security risks. This paper systematically analyzes the new infrastructure cybersecurity risks, summarizes the new challenges faced by new infrastructure, and proposes a risk prevention and control model METAD which combines monitoring and early warning, threat intelligence sharing, risk assessment, and intelligent defense.

1. Introduction

With the in-depth development of economic globalization, new infrastructure has become a new economic growth point for China in the future, and at the same time has become a driving force for countries around the world to seize the technological highlands and promote a new round of technological revolution and industrial transformation. However, the development of new infrastructure is still accompanied by severe new cybersecurity challenges.

On the one hand, through 5G networks, Internet of Things (IoT), artificial intelligence (AI) and other technologies, the new infrastructure has further accelerated the integration of cyberspace and physical space. It faces the risk of speeding up the spread of cyber attacks from digital space to physical space. On the other hand, due to the important strategic position of the new infrastructure, once it encounters a cyber attack, it can directly affect people’s lives, social stability, and even national security. At the same time, the new cybersecurity challenges have also put forward new requirements for cybersecurity protection[1].

Therefore, it is necessary to sort out and analyze the cybersecurity risks of the new infrastructure, and put forward countermeasures for early response and prevention of relevant risks.

2. Risks of New Infrastructure

2.1. Definition of New Infrastructure

On March 4, 2020, the Standing Committee of the Political Bureau of the CPC Central Committee
handed a meeting and pointed out the need to accelerate the construction of new infrastructure such as industrial internet, 5G network, and big data center. On April 20, 2020, the National Development and Reform Commission further defined the scope of the new infrastructure, mainly including three aspects: information infrastructure, converged infrastructure and innovation infrastructure[2].

(1) **Information infrastructure.** Mainly refers to infrastructure based on the evolution of new generation information technology, such as the communication network infrastructure represented by 5G, IoT, industrial internet, the new technology infrastructure represented by AI, cloud computing, and blockchain, and the computing infrastructure represented by data center, etc.

(2) **Converged infrastructure.** Mainly refers to the deep application of Internet, big data, AI and other technologies to support the transformation and upgrading of traditional infrastructure, such as intelligent transportation infrastructure, intelligent energy infrastructure, etc.

(3) **Innovation infrastructure.** Mainly refers to public welfare infrastructure supporting scientific research, technology development and product development, such as major scientific and technological infrastructure, science and education infrastructure, and industrial technology innovation infrastructure, etc.

### 2.2. Risks of New Infrastructure

At present, the development of new infrastructure is faced with cybersecurity risks such as becoming the key target of national hackers, the significant expansion of cyber threats, and the endless emergence of cyber attacks. Following is the risk analysis of three categories of new infrastructure.

#### 2.2.1. Risks of Information Infrastructure

Once the information infrastructure encounters a cyber attack, it will seriously threaten the safety of enterprise production and operation, trade secrets, and economic interests.

1) **5G technology expands the attack surface.** In November 2019, the European Union released the "ENISA threat landscape for 5G Networks"[3], pointing out that the new features and functions of the 5G network architecture will increase the overall cyber attack surface and the number of potential entry points. For example, the enhancement of network edge functions means that some functions of the core network can be integrated into other parts of the network, making the corresponding equipment more sensitive to cyber attacks. In addition, as 5G networks will be mainly based on software, potential attack paths will be increased. The report also pointed out that hackers with national background are most likely to launch persistent and complex cyber attacks on 5G.

2) **AI accelerates cyber attacks while faces the risk of new technology vulnerabilities.** On the one hand, intelligent malware will use AI to automatically find and exploit system vulnerabilities, and launch cyber attacks against specific systems. AI attack tools present a trend of weaponization. For example, the U.S. has been able to weaponize AI attack tools, attack the enemy's AI systems[4]. On the other hand, new technologies bring new vulnerabilities. Attackers may use "reverse AI" technology to destroy data, deceive machines or reverse engineering by obtaining algorithms.

3) **Industrial internet cyber attacks are characterized by high persistence, large-scale, and multiple channels.** With the deep integration of operation technology(OT) network and information technology(IT) network, hackers can not only directly attack OT system vulnerabilities, but also continuously attack and sniff through various channels such as downward penetration of IT system risks and upward penetration of edge computing node risks. It can directly hit important sensitive data. And the organization and scale of attacks are more obvious. For example, in July 2020, EKANS ransomware launched an attack aimed at the process and service of industrial control system, encrypted important data and demanded high ransom, which affected multiple industries including the U.S. and Europe countries, causing widespread system collapse.

4) **Cloud platforms face serious data security risks.** For example, in early 2019, the MongoDB and Elasticsearch databases that are widely used in China, have successively exposed serious security vulnerabilities, which may lead to data leakage risks. In April 2020, cloud backup service provider SOS Online Backup leaked 135 million customer data due to database configuration errors.
2.2.2. Risks of Converged Infrastructure
Converged infrastructure has become a key target of cyber attacks, which seriously threatens the safety of life and property and even national security.

(1) **Infrastructures such as water, electricity, and Internet have become the preferred targets of cyber warfare among countries.** In 2019 and 2020, Venezuela suffered several severe cyber attacks, with large-scale power and water cut-off throughout the country, resulting in problems such as national traffic paralysis, hospital operations interrupted, all communication lines interrupted, mass riots and so on. In June 2019, South American countries such as Argentina and Uruguay suffered cyber attacks. Large-scale power outages swept South America, affecting more than 48 million people and preventing them from working and living normally.

(2) **The nuclear power sector became a new target for advanced persistent threat (APT) attacks.** In September 2019, India's independent network nuclear power plant Kudankulam was attacked by APT organization Lazarus. India officially issued a statement saying that the server was infiltrated. Although this attack did not affect the key control systems, it also raised alarm bells: cyber attacks and nuclear deterrence are undergoing a dangerous "collision", and the serious consequences are immeasurable.

(3) **Intelligent connected vehicles (ICVs) expose new attack surfaces.** The integration and application of electronic and electrical components such as digital car keys (PKES) and automotive gateways have exposed new attack surfaces. Take the PKES system as an example. In the first 10 months of 2019, there were more than 14,000 vehicle thefts in the U.K. that initiated relay attacks against the PKES system, equivalent to one such theft case every 38 minutes.

(4) **New attack methods emerge in endlessly, seriously threatening traffic safety.** Since 2019, new types of attacks such as remote control hijacking attacks based on information leakage of in-vehicle communication modules have appeared in ICV, which can affect most vehicle companies. The new attack method can realize batch remote door opening and closing, start and close the engine and other control operations, which poses a serious threat to traffic order and driving safety.

2.2.3. Risks of Innovation infrastructure
Cyber attacks on innovative infrastructure are rampant, seriously threatening intellectual property rights and national sensitive data.

(1) **The APT group launched intensive targeted attacks against scientific research institutions to steal research results.** During the COVID-19 outbreak, targeted attacks against public health institutions became more intensified. The hackers use epidemic-related documents to conduct bait attacks and phishing attacks, steal intelligence or obtain economic benefits. For example, in July 2020, the U.K., the U.S., and Canada accused Russian intelligence agencies of launching continuous attacks against scientists and pharmaceutical companies to steal vaccine intellectual property.

(2) **Attack infiltrate important industry companies and steal sensitive national documents.** In March 2020, the U.S. defense supplier Visser Precision was attacked by ransomware, resulting in the theft of sensitive documents in the defense industry, posing a potential threat to intellectual property rights and national security.

(3) **Implement customized backdoor attacks to steal large amounts of confidential information.** In 2019, OceanLotus issued malicious files to target machines and used relevant machine attributes for customized encryption, which greatly increased the difficulty of payload decryption and was able to better evade detection by anti-virus software, increasing the chance of success in stealing confidential information.

3. New Infrastructure, New challenges
Different from traditional cyber attacks, cyber attacks in the era of new infrastructure will extend from the digital space to the physical space. For example, "5G+" telemedicine, IVC and electricity new infrastructure involve industrial security and personal safety. Therefore, the new infrastructure cybersecurity is no longer the traditional security of information, network, and system itself, but has
risen to a broader level such as national security, social security, and personal safety [5].

In general, the new cybersecurity challenges mainly include two aspects. First, the important strategic position of new infrastructure has made it a key attack target of national hackers, which has expanded the scope of threats and increased risks. Second, new attack methods emerge in endlessly, presenting features such as new attack targets, new attack paths, and expanded attack surface.

As the new infrastructure covers a wide range, this paper focuses on the analysis of 5G, industrial internet and electricity new infrastructure, which are the most representative and important new infrastructure. Among them, 5G is a key new infrastructure supporting the digital, networked and intelligent transformation of the economy and society. The industrial internet is a new ecological and application model that integrates a new generation of information technology and industry. Electricity new infrastructure related to national security and people's livelihood. The key research objects and the new cybersecurity challenges are shown in table 1.

| Key research objects       | New cybersecurity challenges                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------|
| 5G                        | The new network architecture brings new attack targets                                         |
|                           | New technologies introduce new attack paths                                                   |
|                           | 5G faces new threats of supply chain attacks                                                  |
| Industrial internet       | The cyber attack surface has expanded significantly                                           |
|                           | Data security risks have increased dramatically                                               |
|                           | Security threats are superimposed and enlarged                                                |
| Electricity new infrastructure | Network interconnection exposes new attack points                                         |
|                           | Cyber attack paths increase                                                                  |
|                           | Become a key target of national confrontation                                                |

Table 1. The key research objects and the new cybersecurity challenges

Specifically, the new cybersecurity challenges faced by 5G, industrial internet and electricity new infrastructure are reflected in the following aspects.

3.1.5G
1) **The new network architecture brings new attack targets.** The new 5G network architecture will make certain network equipment or functions more sensitive, and may become new attack targets, such as base station, management and orchestration and other key technical management functions.

2) **New technologies introduce new attack paths.** As the 5G network will be mainly based on software, there may be major security flaws in the software development process, and more attack paths are introduced.

3) **5G faces new threats of supply chain attacks.** 5G's heavy dependence on suppliers has aggravated the potential impact of loopholes or backdoors in the supply chain, and 5G is vulnerable to supply chain attacks initiated by hackers.

3.2.Industrial Internet
1) **The cyber attack surface has expanded significantly.** The ubiquitous interconnection of the industrial internet has broken the relatively closed and credible production environment of traditional industries, and has significantly expanded the attack surface. For example, edge access risks and IT system risks can extend to the core network.

2) **Data security risks have increased dramatically.** All kinds of key data of industrial internet, such as research and development design, production management and operation control, are distributed on cloud platforms, user terminals, production terminals and other facilities. Its high value attracts high attention of attack organizations, and the data security risks are further increased.

3) **Security threats are superimposed and enlarged.** Comprehensive interconnection makes the security issues of control layer, device layer, network layer, platform layer, data layer, and management and use layer superimposed, the organization and scale of attacks are more obvious.
3.3. Electricity new infrastructure

1) **Network interconnection exposes new attack points.** The application of electricity new infrastructure will promote changes in grid business. The “isolation network” will no longer be isolated, increasing the exposure of core production systems such as power monitoring system, and bringing new attack points.

2) **Cyber attack paths increase.** The introduction of new technologies has also increased the number of cyber attack paths, such as the introduction of the security access risk of massive power intelligent terminals, the power monitoring system may be exploited and attacked by the middleman, resulting in the tampering and disguise of communication protocols.

3) **Become a key target of national confrontation.** The cyber attacks can lead to major security incidents such as large-scale power outage, leakage of pollutants, and explosive damage. It’s becoming the target of cyber confrontations between countries and seriously threatening national security.

With the acceleration of new infrastructure, the magnitude of network equipment will increase geometrically. And the larger the number of facilities, the deeper the degree of integration and the wider the fields involved, the more likely that new infrastructure will be controlled and paralyzed. It is urgent to carry out research on cybersecurity risk prevention and control strategy research to build security infrastructure[6].

4. New Model of Resisting New Infrastructure Cybersecurity Risks

In order to enhance the new infrastructure cybersecurity risk prevention and control capabilities, this article proposes a risk prevention and control model METAD.

4.1. Strengthening monitoring, early warning technology and threat intelligence sharing

By improving monitoring, early warning methods and threat intelligence sharing mechanisms, timely capture cybersecurity risk information and strengthen cybersecurity assurance. The first is to strengthen the research and development of new infrastructure cybersecurity detection technology, and launch effective security products, such as malicious traffic detection, threat tracking and traceability, etc., monitor the security threat situation. The second is to accelerate the construction of cybersecurity situation awareness network, proactively detect malicious attacks, and timely warning and response. The third is to build threat intelligence sharing platform, such as vulnerability database, virus database, threat intelligence database, emergency response case database, etc., to timely share vulnerabilities, malicious attack sources, tactics, techniques and procedures (TTPs), and attacker portrait, etc.

4.2. Establishing cybersecurity risk assessment mechanism

In view of the cybersecurity risks faced by new infrastructure, conduct risk point extraction, risk possibility and risk impact analysis, build a risk assessment model, carry out reasonable classification and grading, determine the level of various risks, identify major cybersecurity risks, and gradually establish a comprehensive, effective and reasonable risk assessment mechanism. The first is to
systematically sort out the cybersecurity risk points and risk characteristics of various new infrastructure. The second is to evaluate and judge the extent and scope of the possible risk impact, analyze the risk impact on life and property safety, trade secrets, national intellectual property rights and national sensitive documents, and classify the risks according to the risk possibility, so as to identify the critical national cybersecurity risks. The third is to integrate dynamic risk identification and risk assessment methods into the full life cycle of new infrastructure, and continuously improve the risk assessment model in combination with the monitored risk information, so as to provide more effective guidance for the risk prevention and control of new infrastructure.

4.3. Speeding up the construction of cybersecurity intelligent defense system
Based on threat intelligence, situational awareness, big data analysis and other technologies, accelerate the construction of new infrastructure cybersecurity intelligent defense system to deal with new cybersecurity challenges. Combining the characteristics of new infrastructure cyber attacks, using cutting-edge technologies such as machine learning, AI, and blockchain, build an adaptive cyber security intelligent defense system for various levels of cyber security risks, automatically adjust defense levels and strategies, and focus on building a comprehensive protection system against national cybersecurity risks. Combining the cyber attack chain, using automated tools to quickly and effectively prevent cyber attacks, predict the overall cybersecurity risk trend, and provide corresponding protection strategies. In this way, to form strategic advantages in threat perception, anticipation of attack behavior, and rapid and effective threat identification and response, so as to realize proactive defense against new cybersecurity threats of new infrastructure.

5. Conclusion
This paper conducts cybersecurity risk analysis for three types of new infrastructure, and proposes risk prevention and control strategy to improve monitoring and early warning means and threat intelligence sharing mechanism, carry out cybersecurity risk assessment, and accelerate the construction of cybersecurity intelligent defense system. The risk prevention and control strategy provides an important reference for countries, industries and enterprises to optimize the cybersecurity risk prevention and control layout of new infrastructure.

Reference
[1] Wei L, Dai F.F., Zhao S. (2020) New infrastructure defines a new paradigm for cybersecurity technology innovation. China Information Security, 05: 38-40.
[2] ChinaDevelopment. (2020) The new infrastructure has a preliminary definition and scope definition. http://www.chinadevelopment.com.cn/2020/0422/1638526.shtml.
[3] The European Union Agency for Cybersecurity. (2019) ENISA threat landscape for 5G networks. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.
[4] Marcus C. (2019) AI's security vulnerability and what policymakers can do about it. Information Security and Communications Privacy, 10: 72-81.
[5] Xinhuanet. (2020) Cyber security should be the cornerstone foundation of new infrastructure. http://m.xinhuanet.com/cq/2020-09/16/c_1126491228.htm.
[6] Zhou H.Y. (2020) Safety infrastructure should be built simultaneously in new infrastructure construction. China Information Security, 06: 28-29.