# CYBERSECURITY AS A MAJOR FACTOR IN CHINA'S NATIONAL SECURITY

**Azimova Guli Nodirbek qizi**
Koreya xalqaro universiteti
E-mail: guly.azimova1@gmail.com

## ABSTRACT

Over the past two decades, the People's Republic of China has paid special attention to ensuring the information security of the state and society. The rapid development of information technology has added a new aspect to the national security system of the People's Republic of China - cybersecurity.

**Keywords:** China, cybersecurity, security, law, information, Internet.

For China, the implementation of approaches to ensure the safety of its own digital data has two important directions: firstly, it is necessary to ensure social stability and control over internal state processes, and secondly, to conduct industrial and economic espionage against foreign companies and enterprises.

In the regulatory and legal aspect of ensuring China's cybersecurity, it is necessary to note the following documents, which are key:

In 2000, the National People's Congress of China (NPC) attempted to determine the classification of possible offenses in the information sphere. In the same year, the "Resolution of the NPC on the protection of the Internet space" was published, which highlighted those areas in which violations could occur: economic, educational, the sphere of maintaining social stability and protecting citizens.

In 2003, the Office of the Central Committee published the "Resolution of the State Informatization Leading Group for Work on Strengthening Information Security". In 2006, the "State Strategy for the Development of Informatization for the period from 2006 to 2020" was adopted. This document identifies the importance of focusing on the field of information technology.

On December 27, 2015, the National People's Congress adopted the Anti-Terrorism Law of the People's Republic of China. It was supposed to decrypt Internet traffic, use administrative measures to seize information from foreign companies and enterprises if it is suspected of being used for terrorist purposes.

China has adopted and implemented the Cyber Security Law (2017). The main purpose of the adoption of the law is to protect the national "cyber sovereignty" of the People's Republic of China. Only on June 10, 2021, the Standing Committee of the

National People's Congress passed the Data Security Law of the People's Republic of China, which entered into force on September 1, 2021, marking the acceleration of the legislative process in China's legal system on network information security.

In the state apparatus of the People's Republic of China for ensuring cybersecurity, a special role is played by the Military Council of the CPC Central Committee and the Military Council under the State Council of the PRC.

In the National Cyber Security Strategy, the government highlights aspects important to China's interests:

- the arms race in cyberspace and the hegemony established by Western countries in it threaten the international balance of power, preventing joint and effective prevention of common cybersecurity problems;

- the national cybersecurity system must be constantly updated and supplemented with new technologies and cyber equipment;

- the need to establish uniform standards in the field of information technology for the entire global cyberspace, ensuring the openness of IT markets in order to bridge the gap between countries in the development of digital technologies;

- systematization and integration at the national level into a unified legislative framework of issues of ensuring the security of cyberspace;

- establishing uniform standards in the field of international cyber cooperation and cybersecurity, and these activities should ensure personal privacy and human rights.

In this document, the Chinese side for the first time outlined its position and understanding of cybersecurity, the prospects for transforming the system of government management of the network space and the possibility of building a unified Internet community. The country's leadership sees successful management of cyberspace in comprehensive compliance with the following rules: ensuring fair distribution of basic Internet resources; multilateral management of servers and various objects of information and communication infrastructure from China; promoting the development of the digital economy and investing in the development of network culture.

The structure of the State Council of the People's Republic of China includes relevant ministries (Ministry of Industry and Information Technology, Ministry of Science and Technology of the People's Republic of China, Ministry of State Security), which can be involved in the development of appropriate protective measures in the information space, and leading small groups specializing in important strategic issues.

As of 2015, the 3rd Department occupies a special place in the structure of the military apparatus of the PRC. Its functions include leading intelligence activities on the Internet, searching for vulnerabilities in information systems and working out the actions of cyber troops to conduct cyber attacks against civilian and military targets.

The military apparatus also includes research institutes and centers specializing in information security, information and certification center, which is a unified structure for introducing ideological control over civilian information technologies into the civilian sector.

For the PRC, there are a number of main threats that influence the formation of a unified policy in the field of cybersecurity. The policy of the People’s Republic of China in this area can be divided into internal and external. The first direction includes restricting access to certain information and news Internet resources, a ban on the use of foreign software and means of transmitting voice and text messages.

The external direction of the policy in the field of cybersecurity of the PRC includes cyber attacks and other actions of specialized government units in the information sphere to cause damage or damage to the critical infrastructure of enemy forces in the event of a likely information war or conflict.

The People’s Republic of China lags behind Western countries in cyberattacks against foreign technology companies. Despite China’s significant economic development, since the beginning of the reform and opening-up policy in the 80s. XX century It is the knowledge-intensive sector that needs serious modernization. It is worth noting that the production part has a dual conversion: military and civilian. Therefore, the theft of technical documentation can be used by state industrial corporations for their own interests.

As of 2022, the number of Internet users in China is 855 million people (about 60% of the total population). Moreover, in relation to adult citizens, this figure is estimated at more than 93%. Up to 600 million people regularly shop online, and annual online retail sales in China amounted to US$2.2 trillion in 2021.

The above factors allow the competent authorities responsible for ensuring the national security of the PRC to freely introduce new technologies to control citizens by imposing various services that require an Internet connection, the use of a smartphone and a bank card to access.

At the same time, despite the high level of development of information technology in the PRC, the beginning of the full functioning of the Social Credit System in 2023 is considered unlikely, since the system is currently in the testing stage in certain cities of the country. It is expected to reach the provincial level by the end of 2023. And the most likely date for the launch of a unified intelligence and information space on a national scale is called 2025–2027.

Cybersecurity has gradually become a critical aspect of the national security of the People’s Republic of China, so the authorities are increasingly paying attention to the implementation of protective measures on the Internet. The basic goal of such actions is to ensure the legitimacy of the current government, as well as to perform representative functions of the Communist Party of China on the Internet.

In the regulatory and legal system of the PRC, there is a tendency to replace the current restrictive model with a model of gradual "opening" of the Chinese information segment. This is due to the need to include China in global information and financial processes. At the same time, information technologies are gradually being introduced into the production process and the lives of citizens.

In the state apparatus of the PRC, the leading place in ensuring cybersecurity is occupied by the Military Council under the Central Committee of the CPC. Despite the formal division of the government into the civilian and military sectors, all power belongs to the Chairman of the People's Republic of China, Xi Jinping.

The ideological component is also important for China's cybersecurity. The concentration of all power in one hand increases the importance of the ideological factor for the political course in the information space. The "fifth generation" of Chinese leaders has repeatedly noted the importance of cybersecurity for the stability of the state.

Also in this area, an attempt is being made to implement the Belt and Road initiative, which consists not only in promoting foreign economic policies, but also in using propaganda leverage on foreign countries.

Overall, the Data Security Act covers a strong and clear national security framework, with relevant implementation measures to be clearly communicated in the future. However, it is important for domestic enterprises to consider data compliance measures as a key factor in the product design and market placement agenda. An important part should be coordination with the government to create a system for classifying and protecting data and establishing an internal control mechanism for data management.

## REFERENCES:

1. Chang A. Warring State. China's Cybersecurity Strategy. December, 2014 // CRYPTOME.ORG: информационный портал. https://cryptome.org

2. Chen Gang, Lim Wen Xin. Xi Jinping‘s Economic Cybersecurity Agreement with Barack Obama http://ippreview.com/index.php/Home/Blog/single/id/35.htm

3. Cohen N. Hong Kong Protests Propel FireChat Phone to Phone App. Available at: http://www.nytimes.com

4. China Voice: China allows no compromise on cyberspace sovereignty. http://news.xinhuanet.com/english

5. Lindsay Jon R., Cheung Tai Ming, Reveron Derek S. China and Cybersecurity Espionage, Strategy, and Politics in the Digital Domain. Oxford, Oxford University Press Publ., 2015, 379 p.

6. Harwit E. WeChat: social and political development of China's dominant messaging app. Chinese Journal of Communication, 2016, vol. 10, issue 3, pp. 1—16. (In Eng.)

7. Kashin V. Novyy oblik drakona [A new appearance of the dragon]. www.lenta.ru/articles

8. The 39th Statistical Report on Internet Development in China. January, 2017 // CNNIC.COM.CN: официальный сайт некоммерческой организации China Internet Network Information Center. http://cnnic.com.cn

9. The 40th China Statistical Report on Internet Development. July, 2017 //
CNNIC.NET.CN: официальный сайт некоммерческой организации China Internet Network Information Center. URL: http://www.cnnic.net.cn

10. Ventre D. Chinese Cybersecurity and Defense. London: Wiley ISTE, 2014. 301 p.