China’s main Cyber-security Threats and Challenges

China, which has the world’s oldest tradition of public administration, became one of the countries that best understood the role of information technology in the rapid change of the world towards the end of the 20th century. The development of information technology marked the beginning of a new revolutionary era, such as the agricultural revolution of 10,000 years ago and the industrial revolution of 300 years ago. Able to assess the role of the Internet in economic development, China began to build its economy on the information economy. The main strength of the information economy is information and knowledge.[1] For China, which has built its economy on the information economy since the 1980s to integrate into the international system, ensuring information security is as vital as any other major economy in the world. As a result, cyber-security has become one of the key issues in China’s foreign policy and domestic security.

China, which is trying to build its economy on information and knowledge, naturally faces different problems and challenges in the field of cyber-security. For example, the fact that a large part of economic income comes from the information and economic system makes China an open target against cyber-attacks in this area. Thus, as one of the countries with the best application of the information economy system, in 2019 the digital economy accounted for 36.2 percent of China’s GDP.[2] One of the main reasons for the growing share of the digital economy in GDP is the rapid development of e-commerce in the Chinese market. From 2006 to 2018, the number of online shoppers increased significantly, from 34 million to 610 million, respectively[3] and this latest figure was 73.6 percent of China’s online population.[4] In addition, the total number of Internet users in China reached 904 million in March 2020, most of which, or 896.9 million, are mobile Internet users.[5]

The rapid spread of the Internet in China and the fact that it is more accessible to a large

part of the population pose two major threats to China in terms of cyber-security. First, a strong cyber-attack on the rapidly digitalizing Chinese economy could soon do great damage to the Chinese economy, which will have two different effects, both economically and politically. Economically, online shopping among the population can be damaged, which means a huge financial loss. Because gaining the trust of customers and building a loyal customer base is the basis of online shopping.[6] For example, in 2011, in China's largest ever public data breach, the information (username, password and email address) of 6 million users stored on the Computer Software Development Network in China was leaked and published on the Internet.[7] Politically, it can lead to distrust of the population against the central government. This will lead to the Chinese Communist Party losing its credibility over time and losing control over the Chinese economy. The second major cyber-security problem is cyber-attacks that can be carried out directly against government agencies, military facilities, and projects. In this case, the safe implementation of projects of state importance is not only difficult and sometimes even impossible. Chinese government agencies and companies are heavily dependent on the technology of American firms such as Microsoft and Intel, and in addition, some Internet infrastructures, such as the Internet Corporation for Names and Numbers (ICANN), are located on American soil. This dependence is increasing sensitivity in China, and as a result, the development of the potential for cyber warfare by the United States is adding to the concern.[8] For example, the Stuxnet virus, created in 2010 against Iran's nuclear enrichment facilities, infected 60,000 computers around the world, half of which were in Iran, and damaged Iran's nuclear facility by achieving its main goal.[9] This attack on Iran's nuclear facility shows that all countries of the world are in danger and could be subjected to the same type of attack at any time. In connection with our research, we can say that some of the infected computers were in China. This does not mean that China is only indirectly facing such attacks. Thus, in 2019, the total number of cyber-attacks directly against China was more than 62 million, and more than half of foreign attacks were from the territory of the United States.[10]

China faces difficulties in combating the threat of cyber attacks for various reasons. First, the rapid spread of Internet use in China, both economically and in general, makes it difficult for Chinese officials to establish and enforce cyber-security laws and strategies. On the other hand, in developed countries such as the United States, there is close cooperation between private companies and government agencies in the field of cyber-security. However, both information and communication companies operating in China have little experience in developing cyber-security strategies, and the Chinese government, which lacks specialists in combating cyber-attacks,[11] has to carry this burden on its own. The third and main difficulty is that with the rapid spread of the Internet all over the world, crossing the country's borders creates a comfortable environment for people to easily share and disseminate the ideas and information they want. In this regard, states find it difficult to strike a balance between ensuring people's right to freedom of information and ensuring cyber-security. Although it has an undemocratic structure, this problem is also important for China, which has the largest number of Internet users in the world. Because it is very difficult to keep track of what information so many users are spreading and, most importantly, what activities they are doing. Most importantly, the information spread on the Internet has the power to unite the Chinese population against the central government. The Arab Spring is a shining example of the role of the Internet and communication technologies in uniting people for political struggle.[12] China also has many reasons to be concerned. For example, documents leaked to the press by former US intelligence contractor Edward Snowden provided dramatic public evidence that Western intelligence services were aggressively infiltrating Chinese networks. Some of Snowden's documents show that the National Security Agency (NSA) entered Huawei's headquarters in Shenzhen to exploit routers and switches used by a third of the world's Internet population.[13] This example reinforces the possibility that China, like the Arab Spring, will one day experience the Chinese Spring. Therefore, China is trying to both increase its overall security and be prepared for threats from the United States and other powerful countries, and most

importantly, to develop its capabilities in the field of cyber security, both as a regional power now and as a global power in the future.

[1] Tai, Zixue. The Internet in China: Cyberspace and Civil Society, Routledge, 2006, p. 86.

[2] Shijia, Ouyang. Cybersecurity challenges to pose concerns, China Daily, 2020, https://www.chinadaily.com.cn/a/202008/18/WS5f3b31c5a310834817260edc.html

[3] Ma, Yihan. Number of online shoppers in China 2009-2020, Sep 30, 2020, https://www.statista.com/statistics/277391/number-of-online-buyers-in-china/#:~:text=The%20number%20of%20online%20shoppers,edged%20close%20to%2045%20percent.

[4] Number of online shoppers in China hits 610 million, China Daily Hong Kong, March 02, 2019, https://www.chinadailyhk.com/articles/62/250/44/1551506282401.html

[5] Lin, Wan. China's internet users reach 900 million, live-streaming ecommerce boosting consumption: report, the Global Times, 2020, https://www.globaltimes.cn/content/1187036.shtml

[6] Olenski, Steve. The Effect of Cyber Crime On Online Shopping, Forbes, 2016, https://www.forbes.com/sites/steveolenski/2016/08/03/the-effect-of-cyber-crime-on-online-shopping/?sh=20b9efbc2b87

[7] Austin, Greg. *Cyber Policy in China*. Polity Press, 2014, p. 77.

[8] Lindsay, Jon R. "China and Cybersecurity: Controversy and Context." *China and*

Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, edited by Jon R. Lindsay et al., Oxford University Press, 2015, p. 3.

[9] James P. Farwell & Rafal Rohozinski. Stuxnet and the Future of Cyber War, Survival, 2011, Vol 53, No 1, pp. 23-40, http://dx.doi.org/10.1080/00396338.2011.555586

[10] Feng, Coco. More than half of foreign cyberattacks against China in 2019 originated in the US, China report says, South China Morning Post, 2020, https://www.scmp.com/tech/policy/article/3097070/more-half-foreign-cyberattacks-against-china-2019-originated-us-china

[11] Wei, He. Talent key to cyber-security, say experts, China Daily, 2019, http://www.chinadaily.com.cn/a/201907/15/WS5d2bd1dba3105895c2e7d5dd.html

[12] Mark I. Wilson and Kenneth E. Corey. The role of ICT in Arab spring movements, NETCOM, 2012, 26-3/4, pp. 343-356, https://journals.openedition.org/netcom/1064

[13] Sanger, David E., and Nicole Perlroth. "N.S.A. Breached Chinese Servers Seen as Security Threat." *The New York Times*, 22 Mar. 2014, www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.