US-China Relations Report, Vol. 1
The Fog Surrounding China's Cyber Security

Motohiro Tsuchiya
(Professor, Graduate School of Media and Governance, Keio University)

*This report is part of the research findings of "US-China relations and international relations centered on the United States and China" (US-China Relations Research Group), which is a sub-project of the fiscal 2015 Japan Institute of International Affairs project "Major Developments in the US and China and US-China relations amidst turmoil in the international order."

At the US-China Summit held in June 2013 in California, one of the topics on the agenda was cyber security. US President Barack Obama pressed the President of the People's Republic of China Xi Jinping to stop the cyber espionage originating from China (broadly speaking, cyber attacks) and, in particular, the industrial espionage by Chinese government agencies against US companies. However immediately prior to this summit, it was reported in the news that the US government had collected large amounts of communication-related information from a US communications company.[1] Based on this, President Xi Jinping retorted to President Obama that perhaps there were more cyber spies in the United States than in China, and the two countries failed to reach an agreement.

Although President Xi Jinping was unable to reach an agreement with President Obama at that time, China did respond to the United States the following February by forming the Central Leading Group for Internet Security and Informatization, of which President Xi Jinping himself would be chairperson (leader of the organization). Premier of the State Council Li Keqiang and First-ranked Secretary of the Central Secretariat Liu Yunshan were appointed vice chairpersons (deputy leaders). This Leading Group is an organization not of the Chinese government, but of the Communist Party of China. Under China's party-state system, the Communist Party has substantial authority over policy decisions and this Leading Group became responsible for the final policy decisions related to cyber security[2].

Prior to the creation of this Leading Group, whenever I asked researchers on China's cyber security, "Who is ultimately responsible for cyber security policy in China?" their answer was muddled. The State Internet Information Office had been previously established in 2011 and the politician Lu Wei was placed in charge, but this Information Office was a Chinese government organization and had no clear authority. It is thought that the Central Leading Group for Internet Security and Informatization held its first meeting in February 2014 and its second in January 2015. I asked a Chinese researcher what substantive meaning the Central Leading Group for Internet Security and Informatization has if it only meets once a year, to which the researcher responded that China had established this Leading Group within the Communist Party and appointed President Xi Jinping as its leader and had also clarified the position of Lu Wei's Information Office. He stressed that not to be overlooked is that the policy had become easier to implement with the Leading Group in the background.

Nevertheless these measures by China did not satisfy the United States. In May 2014, four months after the first meeting of the Central Leading Group for Internet Security and Informatization, Eric Holder, Attorney General of the United States, suddenly held a press conference and announced that five members of China's People's Liberation Army were being prosecuted *in absentia* on suspicion of cyber espionage against US companies and other organizations. These five suspects are believed to be in China, and reportedly they are connected with the People's Liberation Army Unit 61398 based in Shanghai. This unit was singled out in a report by the cyber security firm Mandiant as being involved in cyber espionage against such organizations as *The New York Times* in the United States.

The Chinese government responded that this problem was first an issue to be considered by the cyber working group set up between the US and Chinese governments, expressed its strong dissatisfaction at the sudden holding of the press conference, and declared that this inter-governmental working group was to be put on hold indefinitely. As of July 2015, the US-China cyber working group had still not been reconvened.

Subsequently, there was no end to the cyber espionage suspected of originating

from China. In February 2015, President Obama held a cyber security summit at Stanford University attended by people responsible for cyber security in private sector companies and then in April issued a new presidential executive order. Within this executive order, President Obama stated that "I find that the increasing prevalence and severity of malicious cyber-enabled activities… constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat."

Immediately after that, it was reported that there was evidence that the personal information of four million people had been stolen from the United States Office of Personnel Management (OPM) and that it was strongly suspected that China was responsible. Subsequently, it came to light that the number of people whose information had been stolen was as many as 22.1 million people. This is equal to 7% of the population of the United States, and greatly exceeds the 5.1 million people who have acquired security clearance from the United States government (including civilians). There were concerns that the detailed personal information that was stolen included that of people with security clearance, and lawmakers in the US Congress strongly condemned China.

How should we view the current situation in which the Communist Party of China and the Chinese government cannot stop cyber espionage against foreign countries despite the fact that President Xi Jinping was appointed head of China's cyber security organization and that it has begun to strengthen its cyber security measures? One of the hypothesis is that China is guilty of cunning duplicity. Another hypothesis is that the Communist Party of China and the Chinese government do not themselves possess the capability to stop the cyber espionage originating from within China. The fog that surrounds China's cyber security has not yet cleared away.

---

[1] Later it came to light that this news report was based on the top secret documents leaked in large quantities by Edward Snowden, a former contract employee of the United States National Security Agency (NSA), and subsequently the secret activities of the NSA were exposed one after another. In the second half of 2013, reporting based on the Snowden information continued intermittently.

[2] China has established leading groups for a variety of policy fields. For example, the Central Leading Group for Foreign Affairs (the Central Leading Group for National Security) is responsible for diplomacy and security (it is thought that the members of both organizations are to be believed the same).