**The war without gunpowder is endangering humanity**

Source: [China.com](http://opinion.china.com.cn/opinion_40_118440.html)

Author: Ji Mingkui

Editor: Wang Chi

2015-01-04

<https://politics.rmlt.com.cn/2015/0104/366507.shtml>

At the beginning of the new year, we are talking about such a heavy topic as cyber security because it is so important. The Internet has brought a new era of technological development to human society, and also brought convenience and a sense of closeness to human beings. At the same time, the Internet has also brought hidden dangers that are difficult to guard against. Washington called the "four-star spy chief behind the North Korean hacker attack" the planner of the hacker attack, the director of the Reconnaissance General Bureau, Kim Yong-chol.

North Korea has accused the United States of being the "black hand" behind the paralysis of its Internet and mobile 3G networks, saying that "the United States, as big as a country, is like a child playing hide-and-seek with a runny nose, shamelessly playing tricks to harass North Korea's main websites."

**The war without gunpowder begins**

On December 19, the FBI said that North Korea launched a cyber attack and issued a threat to Sony Corporation because Sony Pictures filmed the funny movie "The Interview" about the CIA hiring assassins to assassinate North Korean leader Kim Jong-un.

Under the threat of hackers, major theaters in the United States refused to show the movie "The Interview", and Sony also cancelled the release of "The Interview". CNN quoted hackers as saying that they welcomed Sony's cancellation of the release, and they also warned Sony not to release the film in any form. After analyzing the malicious attack software used in the relevant cyber attacks, the United States confirmed that hackers had stolen sensitive information from Sony's computers earlier, which is threatening the network security of the United States at all times.

White House spokesman Josh Earnest said that U.S. officials are discussing the cyber attack on Sony every day and consider it a serious national security incident. Obama said, "We will decide to respond at the appropriate time, background and method. The prelude to a war without gunpowder was sounded at the New Year's bell.

On December 22, North Korea's Internet experienced its darkest moment in 2014, suffering a DDoS attack that caused users to be "unable to connect" to the Internet and completely disappear. Affected by the cyber attack, North Korea's elite, state media and public opinion propaganda system were paralyzed.

During the Iraq War, the United States regularly sent false information to the computers and mobile phones of suspected al-Qaeda members to confuse them or frame them for attacks. During the 2008 Olympics, the United States also launched a cyber attack on Iran's nuclear enrichment facilities, paralyzing a large number of Iranian centrifuges and delaying Iran's nuclear weapons development process.

The United States has not commented on the cyberattack. The National Security Agency said relevant questions should be asked to the White House and the National Security Council. The U.S. Cyber ​​Command did not immediately respond to a request for comment.

North Korea officially issued a statement: "denying involvement in the cyber attack against Sony Corporation", saying that it is "groundless" to link North Korea with hacking. Sony Corporation "took advantage of the hostile policy of the United States toward North Korea to produce a film that instigates terrorist acts and denigrates the dignity of the supreme leader of North Korea."

**US identifies North Korean hackers as responsible**

The United States says the Reconnaissance General Bureau was established in 2009. At that time, the Korean People's Army merged its Reconnaissance General Bureau with the Operations Department of the Central Committee of the Workers' Party of Korea. The merged intelligence and military special operations teams are under the control of the supreme leader of North Korea. The above-mentioned organizations of the People's Army and the Workers' Party have a long history of engaging in extreme secret operations and overseas espionage. Since Kim Yong Chol took over as the head of the Reconnaissance General Bureau in 2010, he has been closely monitored by the US and South Korean intelligence agencies. Kim Yong Chol's identity as the director of the Reconnaissance General Bureau was kept secret until April 2013, when it was not made public until he became a member of the Central Military Commission in September.

According to a report released by the Center for Strategic and International Studies, the Reconnaissance General Bureau of North Korea includes Bureau 121 and Laboratory 110, which employs about 5,900 cyber warfare experts. Bureau 121 is the main cyber attack group of the Reconnaissance General Bureau of North Korea, "currently has considerable cyber action capabilities, and the mission it is assigned is another form of realistic provocation."

"The action against Sony was the first of its kind by North Korea in terms of the targeting and sophistication of the hacking attack," the center's researchers wrote in the report. Several hacking groups at the agency have been identified, with Bureau 121 and Lab 110 being the code names for the cyber attack groups.

The North Korean government responded by saying that the U.S. claim that the hacker attack used a code that North Korea usually uses is "nonsense" because the relevant programming code is "widely used". The U.S. determination that North Korea was behind the attack on Sony Pictures is groundless.

President Obama even said he was considering putting North Korea back on the list of state sponsors of terrorism, but Pyongyang strongly denied any involvement in the attack.

**my country is a victim of cyber attacks**

Chinese Foreign Minister Wang Yi previously discussed the cyber attack on Sony Pictures Entertainment with US Secretary of State John Kerry, expressing "opposition to all forms of cyber attacks and cyber terrorism."

On December 23, Chinese Foreign Ministry spokesperson Hua Chunying said at a press conference that China had "noted" the remarks made by the United States and North Korea on the incident and believed that the two sides should resolve the issue through dialogue. At the same time, she refuted reports that China was involved in the paralysis of the North Korean Internet, calling such remarks "irresponsible" and calling on the United States and North Korea to communicate on the hacking of Sony Pictures' website.

Strengthening prevention is imperative

In the era of big data, cybersecurity has become a common challenge faced by mankind. my country is also a victim of cybersecurity, which is becoming increasingly prominent, and computer systems are seriously infected and damaged by viruses. Computer hacking activities have become a major threat; information infrastructure faces challenges in cybersecurity; information systems also have many weak links in terms of prediction, response, prevention and recovery capabilities; and cyber political subversion activities are frequent.

All countries have elevated the cybersecurity industry to the national strategic level for planning and construction. Following the demonstration effect of the United States, more than 50 countries have formulated and announced national security strategies and entered the stage of deploying the core content of security strategies.

The Internet penetration rate in my country has reached 46.9%. With more than 600 million Internet users, China has become a major Internet power, but it is also a "potential fertile ground" for information theft and cyber attacks, and network security is facing tremendous pressure. Relevant data show that in the first half of 2014, 6.25 million computers in China were infected with Trojan viruses; 19,000 hosts outside China controlled 6.19 million computers in my country; in 2014, the China Internet Illegal and Bad Information Reporting Center received a total of 954,268 reports from netizens on illegal fraud, pornography, violent and terrorist audio and video and other harmful information.

The development of informatization has entered the "big data, intelligence, mobile Internet and cloud" stage. The network security issues of big data, intelligence, mobile Internet and cloud computing are becoming increasingly prominent, and their connotations are also constantly expanding.

President Xi Jinping stressed at the first meeting of the Central Cyberspace Security and Informatization Leading Group this year that without cybersecurity, there is no national security, which once again demonstrated the determination of China's top leaders to ensure cybersecurity, safeguard national interests, and promote the development of informatization. The issue of "maintaining cybersecurity" appeared for the first time in this year's government work report, indicating that cybersecurity has risen to the national strategic level.

There are still many problems that restrict the maintenance of my country's network security. Strategic planning and top-level design are relatively lacking. Network security has long been operated under a multi-management system of "fragmentation" and "multiple policies". Although the blueprint for my country's cyber power has been drawn, there is still a long way to go in the practice of network security. It is especially necessary for all parties to work together, adhere to the concept of open development of network security governance, and take comprehensive measures to maintain my country's network order.

We are still subject to certain limitations in technology. Some core technologies have not been broken through, and our independent and controllable progress is limited. In addition, we are simplistically adopting things, which has caused us to gradually lose the foundation for sustainable technological development.

There is a lag in management, passiveness, low decision-making level, lack of institutional constraints, and even no awareness of network security. It is necessary to change the concept of network security and recognize that network security is a kind of technical security, dynamic security, and checks and balances security. Therefore, it is necessary to establish its own core network.

We must enforce the process of replacing domestic information technology products and build a phased plan that covers all areas.

We should build cyber forces as a new type of security capability, and build a network defense team with reconnaissance, monitoring, protection, and counterattack capabilities. At the same time, we should shape the rules of cyberspace, strengthen international cooperation in the Internet field, actively put forward my country's network security construction plans and propositions, and expand the space for international cooperation with a more positive and open attitude.

The cyber war without gunpowder is becoming increasingly fierce, and security threats are everywhere. It is necessary to improve the "National Cyber ​​Security Plan" and speed up the introduction of a series of relevant laws and regulations. In the research and development of information technology and its key products, we should provide relevant industrial policies with advanced awareness and establish a technical team that is both defensive and offensive and compatible with information security.