# CYBER ATTACKS AGAINST THE UNITED STATES: TITAN RAIN

## Introduction

The Federal Government of the United States extended the name “Titan Rain” to a series of attacks on computer systems in the U.S. since 2003. The attacks took place between 2003 and 2004, although some claims were that they were ongoing for three years. While the real identity of the attackers was masked by proxy and spyware, the attacks were believed to be of Chinese origin and the name ‘Titan Rain’ was given due to the persistent nature of the attacks. The hackers targeted most of the defense contractor computer networks in the U.S. due to the sensitive information they contained. The hacking attacks created tensions between the US and the Chinese government and created a need for more cautiousness to avoid such attacks.

## The Titan Rain Attack

The Titan Rain attack was directed towards different departments in the U.S. that contained sensitive information. The attacks began in 2003 and were labeled as corporate espionage or state-sponsored espionage, where the United States believed that the attacks came from the People’s Liberation Army (PLA) and not freelance hackers from China. The main reason that the attack was attributed to the PLA was because the attackers left no evidence of the attack and the conclusion was that a highly disciplined military organization was behind the attacks. The main victim of the attacks was the Department of Defense through the Defense Intelligence Agency. Other agencies affected by the attacks included Sandia National Laboratories, Lockheed Martin, NASA, and Redstone Arsenal. The probable motivation of the attack was to gain as much information as possible that would project a picture of the strengths and weaknesses of the U.S.

On the nature and sophistication of the attacks, the attackers wanted all the files that were available, and they did this through penetration of secure computer systems owned by defense contractors, military bases, and aerospace companies. The type of program used in the attack is referred to as the scanner program where the hackers would first search different military networks to find any computer with vulnerabilities that the hackers would later exploit. The program was successful in finding vulnerable computers, and this began the hacking process where the attackers would gain entry and leave between 10 and 30 minutes. The scanner program was simple but yet modified enough to fit the needs of the attackers, after which they used with complete efficiency against different US networks. Following the scans, the hackers would return after one or two days to steal the data that would be available.

As one security analyst from Sandia noted, the attackers were speedy and would gain access to a hidden part of the hard drive, take the maximum number of files and transmit them to way stations in Taiwan, Hong Kong, or South Korea. The files would then be sent to China from the way stations. The attackers would wipe their fingerprints and leave a beacon that would enable them to re-enter the system at will. The attack would take between 10 and 30 minutes, and the attackers never made a mistake.

With the attackers looking to gain as much information as possible and with the attack being linked to China, one of the desired outcomes of the attack was to have a considerable advantage over the U.S.. The attacks are linked to China’s need to become a leading player in cyber and information warfare, where the country published doctrines, theories, and policies linked to the aggressive and defensive use of the cyber space. After the U.S.’ success in the first Gulf War, this was seen as a success of new technologies where dominance in information and information technologies is seen as capable of providing total control in the battlefield. From this perspective, it is believed that military experts in China are looking for this control by having dominance over the cyberspace. As such, the desired outcome of the attack was to have as much information as possible that would help China gain an informational dominance and have control over the cyberspace while placing its victims at a disadvantage.

Following the attack, China did not take any responsibility for the attacks, and neither has the information been used against the victim. Further, the cyber warfare and information warfare capabilities that China has amassed over the years remain unknown, but there is a consensus that China is gaining superiority and power in the cyber sphere. The consideration may be that China was successful in gaining an advantage over its victim by having access to information that portrays the country’s strengths and weaknesses. Despite the success of the hackers in penetrating defense agencies in the country, the U.S. claimed that the hackers did not have access to classified information.

From the reports by security analysts in the United States, the attackers were very efficient in their attacks and would make silent escapes. The silent escapes were such that the attackers would wipe their electronic fingerprints and also leave a beacon that was undetectable for re-entry purposes. As part of their efficiency, the attack would last between 10 and 30 minutes, and no mistakes were made. The attackers left little evidence of their acts or the source of attacks, and though the U.S. blamed China, there was little evidence to support the claims or make any retaliatory action. Regardless, the event brought about increased friction between the two countries. Further, the event highlighted the need for the U.S. to increase its cyber security standards to avoid such events that leave the country’s defense vulnerable.

## Conclusion

The Titan Rain was a cyber attack carried out by Chinese hackers against the defense system of the U.S. The hackers targeted most of the defense contractor computer networks in the United States due to the sensitive information they contained. Importantly, the motivation and reason behind the attack was to gain as much information as possible that would give China an advantage on information and cyber warfare. Although the attackers never gained access to classified information, the information gained was enough to portray the strengths and weaknesses of the U.S.

## **Bibliography**

Bradley, Graham."Hackers Attack via Chinese Web Sites." *Washington Post,* August 25, 2005.

Homeland Security News. *The lesson of Titan Rain: Articulate the dangers of cyber attack to upper management*. December 2005.

Information Warfare Monitor. *Tracking Ghostnet: Investigating a cyber espionage network,* March 29, 2009.

Thornburgh, Nathan. “The Invasion of the Chinese cyberspies.” *Time*, August 29, 2005.

Ventre, Daniel. “Chinese information and cyber warfare.” *E-International Relations,* April 13, 2010.

Walton, Timothy. *Treble Spyglass, Treble Spear: China’s “Three Warfares,”* 2010.