Chinese Military Hacking and Espionage

Truc L Huynh, Master of Computer Science

Purdue University Fort Wayne

Chinese Military Hacking and Espionage

## The alleged activities carried out by the five Chinese military officers

According to the FBI, from 2006-2014, five Chinese military officers (Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui) were allegedly involved in a hacking conspiracy that targeted Westinghouse Electric Co.; U.S. subsidiaries of Solar World AG; United States Steel Corp.; Allegheny Technologies Inc.; the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial, and Service Workers International Union; and Alcoa, Inc. They were in Unit 61398 of the Third Department of the Chinese People’s Liberation Army.

## Damages inflicted on the victims

According to Chapple & Seidl (2023), the prosecutors alleged the attackers had stolen internal communications that could give Chinese companies insight into corporate strategies and vulnerabilities. Also, the prosecutors alleged the attacks occurred across an 8-year period from 2006 to 2014. According to the Office of the Attorney General (2015), there are 31 charges for:

* Conspiring to commit computer fraud and abuse
* Accessing (or attempting to access) a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain
* Transmitting a program, information, code, or command with the intent to cause damage to protected computers
* Aggravated identity theft
* Economic espionage
* Trade secret theft

## The Chinese government's response

According to Chapple & Seidl (2023), China has also said that it faces a major threat from hackers and accused the NSA and U.S. Cyber Command of targeting Chinese politicians and military. The Chinese government also accused Cisco had aided the NSA with intelligence gathering.

## The current status of the case

According to the FBI (2014), the FBI conducted the investigation that led to the charges in the indictment.  This case is being prosecuted by the U.S. Department of Justice’s National Security Division Counterespionage Section and the U.S. Attorney’s Office for the Western District of Pennsylvania. There is nothing has been updated since July of 19 of 2014.

References

Chapple, M., & Seidl, D. (2023). The Pandora’s Box: The Future of Cyberwarfare in *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 357–374). essay, Jones & Bartlett Learning. (1)

FBI (2014) Five Chinese Military Hackers Charged: *Indicted in Connection with Cyber Espionages Offenses Against U.S.* Retrieved from: <https://www.fbi.gov/news/stories/five-chinese-military-hackers-charged-with-cyber-espionage-against-us>

Office of the Attorney General (Jul 2015) U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage: *First-Time Criminal Charges Are Filed Against Known State Actors for Hacking*. Retrieved from https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor