ıge Credit: U.S. Department of Justice

China's Response to the US Cyber Espionage Charges

China is furious over charges brought against 5 PLA officers – and things could get worse before they get better.

By Shannon Tiezzi
May 21, 2014

On Monday, the U.S. Justice Department announced a landmark case: five officers in China's People's Liberation Army (PLA) have been indicted on charges of hacking and economic espionage. According to Attorney General Eric Holder, the case is the first time the United States has brought charges against state actors for cybercrimes targeting U.S. companies.

China, which has always denied any state involvement in cyber espionage (economic or otherwise), angrily denounced the charges. A statement from the Foreign Ministry called the charges "purely ungrounded with ulterior motives." China immediately called off its participation in the U.S.-China Cyber Working group, citing a "lack of sincerity on the part of the U.S. to solve issues related to cyber security through dialogue and cooperation."

China has also summoned U.S. officials to personally decry the indictment. U.S. Ambassador to China Max Baucus was summoned for a dressing-down from China's Assistant Foreign Minister Zheng Zeguang. The Foreign Ministry also made representations to U.S. Deputy Assistant Secretary for East Asian and Pacific Affairs Kin Moy, who is in China on a visit. Moy was told that "the Chinese government, Chinese military and relevant personnel have never engaged or participated in cyber theft for trade secrets." Chinese officials have repeatedly urged that the U.S. "revoke" the indictment of the PLA officers.

China has also rolled out a media campaign denouncing the move, with a slew of articles in *Xinhua* providing China's

point of view. Based on these articles, and the statements made by Chinese officials, China's response can be summed up in two key points:

First, China says the charges are false. China has always denied any state involvement in cybercrimes, and this instance is no different. Beijing dismisses the charges out of hand and has always insisted there is no evidence to back up American claims of cyber espionage. That's part of what makes this court case so interesting—it implies that the U.S. does in fact have solid evidence against the PLA officers (a point explicitly made in the press conference announcing the charges).

Second, China denounces the charges as hypocrisy, calling the U.S. "the biggest cyber bully." Prior to 2013, China refrained from directly accusing the U.S. of cyberattacks, instead merely pointing out that China had been repeatedly victimized by cyberattacks from unknown parties. However, since then two things have changed: the Obama administration grew more aggressive in its response to China's cyber espionage (culminating in this week's indictment), and Edward Snowden made information on U.S. cyber espionage public knowledge.

Accordingly, China has shifted tactics and no longer shies away from directly accusing the U.S. of cybercrimes. In response to the charges brought against the PLA officers, the National Computer Network Emergency Response Technical Team Coordination Center of China released data on U.S.-based cyberattacks against China. Among other things, the report said that "from March 19 to May 18, a total of 2,077 Trojan horse networks or botnet servers in the U.S. directly controlled 1.18 million host computers in China." The report did not mention any evidence tying these attacks to the U.S. government, however.

While the U.S. government does not deny its cyber espionage activities, the Obama administration has repeatedly tried to draw a distinction between espionage in the name of national security and espionage for economic gain. China has generally ignored this distinction, but now Beijing is attempting to compare apples to apples by specifically accusing the U.S. itself of economic espionage. Citing a decade-old European Parliament report, *Xinhua* alleged that the NSA had used information gathered in its espionage activities to help Boeing beat Airbus "for a multi-billion dollar contract." *Xinhua* also pointed out Brazilian President Dilma Rousseff's accusation that U.S. spying against the state-owned oil company Petrobras was for economic reasons.

Besides a war of words, China has several options should it wish to respond more forcefully to the indictment. In a move that is possibly intended as retribution for the charges, China has banned Microsoft's Windows 8 operating system from being used on government computers. China said the move was made due to security concerns, including worries that the U.S. government would be more easily able to access computers running Microsoft's OS. Other U.S. technology companies could also be affected by bans.

Such indirect responses would provide plausible deniability for China, as "security concerns" rather than retribution would be the official reason behind the moves. However, this would give real economic teeth to China's displeasure, which is important given that this case is motivated by economic concerns. Until recently, U.S. companies had largely decided that the benefits of doing business in China's massive market outweighed the costs, including losses due to economic espionage and old-fashioned IP theft. China may be hoping to convince companies to return to this attitude, which would dissuade them from participating in future court cases. If China wants to move beyond mere rhetoric, this is its most likely move.

More conventionally, China could cancel or suspend diplomatic meetings, as it has already suspended the activities of the U.S.-China Cyber Working Group. China has hinted that military-to-military relations will be the next to be affected, potentially derailing three years of slow but steady progress at building up formal ties. There is also speculation that China could curtail this year's Strategic and Economic Dialogue, to be held in Beijing in early July. An outright cancellation of the S&ED is unlikely, but China could refuse to discuss certain issues, including cybersecurity.

If China wishes to up the ante even further, it could bring charges of its own. Such charges could be symbolic, as the U.S. charges are, by accusing people who have little chance of ever actually appearing in court. Specific NSA employees or even government officials overseeing U.S. cyber programs would be viable options. However, China could also charge Americans actually living in China, meaning they would be subject to arrest. Companies such as Microsoft, Cisco, and Apple, all of which have been implicated in the NSA's spying activities, have large footprints in China. Beijing could conceivably find evidence to tie some China-based employees to NSA spying activities, and bring charges accordingly.

Should China pursue this option, it would cause a major incident in U.S.-China relations. Since its own citizens are not actually at risk of being arrested, it's unlikely Beijing is prepared to go so far as to arrest Americans—but it's not impossible.