5 in China Army Face U.S. Charges of Cyberattacks

nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html

Michael S. Schmidt, David E. Sanger May 19, 2014

Continue reading the main story

WASHINGTON — In the Obama administration's most direct confrontation with China over its theft of corporate secrets, the Justice Department on Monday unsealed an indictment of five members of the Chinese People's Liberation Army and charged them with hacking into the networks of Westinghouse Electric, the United States Steel Corporation and other companies.

The indictment named members of Unit 61398, which was publicly identified last year as the Shanghai-based cyberunit of the People's Liberation Army, including its best-known hackers known online by the noms de guerre "UglyGorilla" and "KandyGoo."

The F.B.I. and American intelligence agencies electronically tracked the activities of the hackers, one official said, and "put them inside the Datong Road headquarters" of the cyberunit, a heavily guarded 12-floor military tower near the Shanghai airport.

The move by the Justice Department was almost certainly symbolic since there is virtually no chance that the Chinese would turn over the five People's Liberation Army members named in the indictment.

Since 2006, and as recently as last month, the indictment alleged, the hacking unit invaded the networks of American corporate targets, systematically copying their emails and, in some cases, infecting their computers with malware.

Image

The Justice Department sought to shame officials with the People's Liberation Army by displaying wanted posters on Monday.Credit...Charles Dharapak/Associated Press

The indictment said that "Chinese firms hired the same P.L.A. unit" to "build a secret database to hold corporate intelligence." In one instance, the hackers broke into Westinghouse's network to learn the company's strategy for negotiating with one of China's state-owned enterprises. The hackers stole roughly 700,000 pages of emails, including some from its chief executive.

After a year in which the dialogue between the two countries was derailed by Edward J. Snowden's disclosures about the United States' own spying efforts in China, the charges leveled by the Justice Department marked an effort by the Obama administration to return the debate over to grounds they think are more favorable to the United States: intellectual property theft.

Until now, President Obama and Defense Secretary Chuck Hagel have tried relatively quiet diplomacy with the Chinese. They have attempted to engage the Chinese in a dialogue over norms for operating in cyberspace, a careful diplomatic dance that has gone on for several years. But Monday's action by the Justice Department marked an attempt to publicly shame the Liberation Army that included a "most wanted list" of cyberattackers with photographs of several marked with the Dillinger-era label "Wanted by the F.B.I."

But it is a legal and diplomatic gamble whether this approach is more likely to halt attacks that a classified American report circulated last year said were directed at more than 3,000 American companies.

At the core of the indictment is the argument that while large countries routinely spy on each other for national security purposes, it is out of bounds to use state-run intelligence assets to seek commercial advantage. “When a foreign nation uses military or intelligence resources and tools against an American executive or corporation to obtain trade secrets or sensitive business information for the benefit of its state-owned companies, we must say, ‘Enough is enough,’ ” said Attorney General Eric H. Holder Jr.

Image
Attorney General Eric H. Holder Jr. said that while nations routinely spy on one another for national security purposes, it was out of bounds for China to use state espionage operations to gain commercial advantages.Credit...Evan Vucci/Associated Press
But the Chinese, with their vast state-owned enterprises, many run by the People’s Liberation Army, have often argued that economic security and national security are one, and they have used Mr. Snowden’s disclosures about the National Security Agency to make the case that the position of the United States is hypocritical because it also conducts attacks on Chinese firms. One such attack on the giant Chinese telecommunication firm Huawei was described in detail in the documents disclosed by Mr. Snowden, though it appeared aimed at penetrating Huawei’s technology in order to monitor the networks of countries that buy the Chinese-made equipment.

Within hours of Mr. Holder’s news conference in Washington, China denounced the indictment, saying it was based on “fabricated facts” and that it “grossly violates the basic norms governing international relations and jeopardizes China-U.S. cooperation.”

In what the Chinese suggested would be only the first step in its response to the Obama administration’s action, it cut off dealing with a joint United States-China working group on cyberattacks that the administration has until now said was evidence that the two countries were trying to resolve their differences.

The government’s case focuses on industries, like steel and solar, where trade tensions have been mounting in recent years. Rising steel and solar exports from China have created friction with American companies and officials over worries that Beijing unfairly subsidizes its domestic players. The indictment also described how the Chinese unit broke into the systems of the United Steelworkers union, which has long pressed American officials to crack down on Chinese trade practices that it views as harming American workers.

The F.B.I. director, James B. Comey, said in an interview that federal authorities, who filed the 31-count indictment in Pittsburgh, had not brought the charges to generate publicity.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

TATES OF AMERICA

v.

Criminal No. 14-118

UNDER SEAL

FIL

MAY -

CLERK US DI
WEST. DIST. OF

INDICTMENT MEMORANDUM

AND NOW comes the United States of America,

s, David J. Hickton, United States Attorney

Indictment Memorandum

The Justice Department said that the men were indicted on May 1 by a federal grand jury in Pennsylvania and charged with conspiring to commit computer fraud and accessing a computer without authorization for the purpose of commercial advantage.

“If we fabricated all this, then come over to Pittsburgh and embarrass us by forcing us to put up or shut up and we’ll put up,” Mr. Comey said, a reference to the fact that the targets named in the indictment were largely in Western Pennsylvania. “I welcome them to come over and enjoy the remarkable protections of our criminal justice system where they will have lawyers, the charges will have to be proved beyond a reasonable doubt and they will have to be convicted by a 12-person jury.”

In a separate case, prosecutors also announced the arrests of 90 people in connection with their use of software called Blackshades, which allows hackers to remotely control a computer. Mr. Comey said that the cases showed that the federal government would pursue cybercrimes, regardless of whether they were perpetrated by groups or nations.

James A. Lewis, a cybersecurity expert at the Center for Strategic and International Studies, said that “China will be tempted to retaliate” for Monday’s actions. He said that the Chinese could punish United States firms operating in China or seek countercharges against American officials based on the Snowden leaks, but it is unclear a broader trade war would benefit either nation.

It was significant that the indictment dealt almost exclusively with Unit 61398 — also known as Comment Crew — but did not detail the case against another roughly 20 Chinese hacking groups, some associated with the military, that the United States regularly tracks. That suggested that the Obama administration may be holding other cases in reserve as leverage in case the Chinese retaliate.

The indictment also did not touch on Chinese attacks aimed at the Defense Department or major defense contractors, perhaps because the administration did not want to invite Chinese revelations about American attacks on similar targets in Beijing, Shanghai and Hong Kong.

Security officials say Monday's indictment has been in the works for two years. A major challenge, officials say, was convincing the targeted corporations to step forward. Many feared loss of revenues from their operations in China or retaliation by the Chinese state.

"They had to gather really strong evidence that these companies had been hacked and then had to convince the companies to go public, despite fear of retaliation," Mr. Lewis said. The indictment, he said, is not about what the United States will do with these hackers, but what China will do with them. "The indictment is meant to send a clear public message to China that they need to take action," he said. "They need to get these P.L.A. entities under control."