Written by **Bob Adelmann** on May 20, 2014

U.S. Accuses China of Spying; China Calls Charges Hypocritical

On Monday the U.S. Justice Department filed indictments against five Chinese military officers for hacking into the computer networks of six American companies to obtain trade secrets and other sensitive business information. Although China has been engaging in espionage against the United States since the end of the Second World War, this is the first time charges have been levied on nationals living on foreign soil.

U.S. Attorney General Eric Holder told a news conference:

> 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.

The indictments were very specific, naming the exact location of the computer network used in the attacks, the group conducting and directing the attacks, and the individuals primarily responsible for carrying them out. It named the six American companies targeted as well: Alcoa, Westinghouse, United States Steel, Allegheny Technologies, SolarWorld, and the United Steel Workers union.

Each of the attackers was hit with 31 criminal counts of a conspiracy carried out by the Peoples' Liberation Army over the last eight years. Added Holder, "This is a case alleging economic espionage by members of the Chinese military and represents the first-ever charges against a state actor for this type of hacking."

In the past when the Chinese government has been accused of cyber spying, it has scoffed at the charges, demanding details. As Assistant Attorney General John Carlin explained:

> They responded [to such charges] by publicly challenging us to provide hard evidence of their hacking that could stand up in court. Well, today we are. For the first time, we are exposing the faces and names behind the keyboards in Shanghai used to steal from American businesses.

The response from China's Foreign Ministry was immediate and predictable. Ministry spokesman Qin Gang claimed Holder's charges were "made up" and would "damage Sino-American cooperation and mutual trust." He added:

> The Chinese government, military and associated personnel, have never engaged in online theft of trade secrets….
>
> China [instead] is a victim of severe U.S. cyber theft, wiretapping and surveillance activities.

Zheng Zaguang, China's assistant foreign minister, summoned Max Baucus, the U.S. ambassador to China, to tell him that his government "protested" the indictments, saying the U.S. attitude toward

internet security was “overbearing and hypocritical.” Further, the indictment “seriously violated norms governing international relations” and “slandered the image of the Chinese army.”

According to the U.S. indictment, at the time when SolarWorld (a German solar panel maker with branches in the United States) was trying to compete with Chinese competitors who were selling similar products below cost, these Chinese military officials were “stealing cost, pricing and strategy information” from the company through its computer networks.

In another specific, the hackers stole designs from Westinghouse at the same time that it was “negotiating with a Chinese state-owned enterprise over the construction of nuclear power plants” in China.

Chinese espionage against the United States has been going on for decades. Larry Wu-Tai Chin worked for the U.S. intelligence community for 35 years while providing China with sensitive classified information. He was initially recruited by a Chinese Communist official in 1948 but wasn’t brought to justice until 1986.

Katrina Leung was recruited by the FBI to work in Chinese counterespionage in 1982, but instead was able for 18 years to provide highly sensitive information on U.S. nuclear, military, and political issues to China.

In the early 1980s, Peter Lee and Chi Mak worked for U.S. companies while providing highly sensitive information on U.S. nuclear weapons development technology to the Chinese.

There are the cases of Ko-Suen “Bill” Moo, Wen Ho Lee, Bo Jiang, and Hua Jun Zhao dating back years. Just three years ago, the *New York Times* and the *Wall Street Journal* suffered cyber-attacks. The Chinese government denied involvement, despite proof that these attacks were instigated when the papers published articles critical of China’s policies, and the attacks were attempts to find out who in the Chinese government leaked the information to the papers.

When it was revealed that the recent Shanghai espionage operation was just one of many, and not the most sophisticated of them, the question must be raised: Why issue the indictments now? What purpose will they serve? Is this another distraction to draw peoples’ attention away from other, more pressing and embarrassing issues faced by the administration?

In the first place, there is scant likelihood that any of the six people charged will ever be brought to justice in the United States. They may have to be careful where they travel in the future, avoiding countries with extradition treaties with the United States, but that’s all.

Is it a response to China’s increasing aggressiveness in Asia, as exemplified by its deployment of an oil rig off the coast of Vietnam? Is this an excuse for the Obama administration to continue to “pivot” its emphasis from Western Europe to East Asia? As suggested by Kevin Rudd, Australia’s former prime minister, “Without such a move, there [is] a danger that China, with its hard-line, realist view of international relations, would conclude that an economically exhausted United States was losing its staying power in the Pacific.”

Or are the indictments an attempt to prop up a sagging image of the president? That’s what Professor June Dreyer, a China specialist at the University of Miami, thinks: “From Obama’s perspective, this will hopefully take some of the heat, the criticism, off him that he’s been totally wimpy.”

Whatever the reason, or reasons, for the sudden announcement of cyber attacks on the United States by China, what is abundantly clear is that both sides of the conflict have dirty hands: the United States

surveilling the world in the name of peace, and China hacking the world to steal its secrets. While the timing is questionable, the shared hypocrisy is staggering.

A graduate of Cornell University and a former investment advisor, Bob is a regular contributor to The New American *magazine and blogs frequently at www.LightFromTheRight.com, primarily on economics and politics. He can be reached at badelmann@thenewamerican.com.*