US-China tensions continue over Google

John Chan
8 February 2010

The US-China tensions have continued over Google's criticism of alleged Chinese hacking and censorship. The Obama administration has used the issue as part of its intensifying pressure on Beijing since the beginning of the year, including a $US6.4 billion arms sale to Taiwan, a planned meeting with Tibet's Dalai Lama and punitive US tariffs against Chinese goods.

US Secretary of State Hillary Clinton late last month called on China to conduct a transparent investigation into the hacking of Google and other US Internet companies since December. "Countries or individuals that engage in cyber attacks should face consequences and international condemnation," she said.

Clinton's speech signalled support for Google's accusations that the Chinese government was involved in the sophisticated hacking of human rights activists' email accounts. More broadly, she lectured the Chinese Communist Party (CCP) over Internet censorship and the need for "freedom of expression".

After subsequently meeting with Chinese Foreign Minister Yan Jiechi in London on the sideline of the Afghanistan conference, Clinton played down the tensions, saying: "Obviously, they feel strongly that they are much more open than perhaps they're getting credit for." But she reiterated that everyone should make sure "that no one uses the Internet for purposes of censorship or repression".

It is clear that the Obama administration is pressing harder on the so-called human rights issue as part of a more aggressive stance against China. Last April, when Clinton visited Beijing in the midst of the global economic turmoil, the US was seeking Chinese assistance. She publicly declared that human right issues "should not" interfere with Washington-Beijing cooperation over the financial crisis.

US expressions of concern about democratic rights in China are completely cynical. Washington is well aware that the profits of American investors in China depend on a police-state regime that suppresses any opposition, particularly by the working class. The Tiananmen Square massacre in June 1989 evoked public criticism in Washington, but was soon followed by a flood of investment to take advantage of China's regimented cheap labour.

James McGregor, head of the American Chamber of Commerce's government relations committee in China, told the *New York Times* on January 27 that "most Western companies also need China more than ever". Moreover, the newspaper noted, more and more Western political leaders are studying the "advantages" of Beijing's autocratic regime that produced fast economic growth, "even if that means a stiff measure of domestic repression".

The White House is also using the Google allegations to tighten Internet monitoring in the US. The *Washington Post* reported last week that Google was finalising a partnership with the National Security Agency to investigate the alleged Chinese hacking. The agreement has been delayed by public concern that this so-called "information sharing" would allow the US intelligence agency to monitor private online communications. Google had previously refused to participate in the NSA's so-called Terrorist Surveillance Program that includes the warrantless interception of phone calls and emails in the name of "fighting terrorism".

Google's own stance over the hacking allegations is driven more by profit than concerns over democratic rights. After initially threatening to withdraw from China, the corporation toned down its rhetoric. Google CEO Eric Schmidt's told the *Financial Times* on January 21 that the company was not pulling out of China. "We have a good business in China. This is about the censorship rules, not

anything else," he said.

At stake is a share in the world's largest Internet market, estimated at 384 million users. After setting up in 2006, Google now accounts for 33.2 percent of Chinese search engine market—half its local rival of Baidu (66.1 percent). For the past four years, it has obediently implemented China's censorship regime, along with Yahoo and other search engines.

Schmidt told the *Financial Times* Google would soon stop implementing the censorship restrictions, but gave no concrete timetable. Google did allow access to search results on sensitive issues such as the Dalai Lama, the banned Falun Gong religious movement and 1989 Tiananmen Square massacre—but only for a day or so.

Google users in China are mainly from the more educated urban middle-classes. Many are attracted by Google's relatively wider online search power, compared to Baidu. By hinting at providing freer access to information, Google is hoping to boost its position against Baidu.

However, the *Financial Times* pointed out that China's Internet users have particular characteristics—tending "to roam the web like a huge playground, whereas Europeans and Americans are more likely to use it as a gigantic library". According to the China Internet Network Information Centre, 61.5 percent of local users are below the age of 29 and only 12.1 percent have a university degree. Some 42.5 percent have a monthly income of just $146 or less.

Watch David North's remarks commemorating 25 years of the *World Socialist Web Site* and donate today.

Deeply concerned about rising social tensions, Beijing encourages the use of the Internet as "a playground". While vigorously policing the Internet to block sensitive political content and discussion, it turns a blind eye to the enforcement of intellectual property rights, allowing users access to free music, films and games. It is a situation, the *Financial Times* commented, "that helps keep the minds of many off topics that could prove inconvenient to their rulers".

Behind US criticisms of the hacking of Google, there are also concerns about China's ability to wage cyber warfare—that is, to disable enemy computer networks and communications, conduct espionage and disrupt vital utilities such as power supplies. According to a 2008 study by British/Israeli counter-surveillance corporation Spy-Ops, China's cyber force had more than 10,000 personnel, with an offensive capability rating as 4.2 (1 is low and 5 is significant)—second only to the US.

The Western media generally inflates the threat of Chinese cyber attacks, highlighting previous hacking incidents, allegedly originating from China, on Western governments and arms contractors. US cyber threats against China are scarcely mentioned. Zhou Yonglin, the deputy chief of China's National Computer Network Emergency Response Technical Team, declared last month that China was the world's largest target for hackers, with more than 260,000 Internet addresses under assault last year. A large proportion, one in six, originated in the US.

Hacking and espionage go beyond the military and state agencies. In the US, China and other countries, the intelligence services have shady connections with various hackers' organisations. A cyber security study published by US Center for Strategic and International Studies (CSIS) and commissioned by technology security firm McAfee acknowledged that the main source of cyber attacks internationally was the US.

The US military has definite cyber warfare plans. The *Washington Post* reported last month that the Pentagon is planning to establish a Cyber Command, not only to defend US military computer networks, "but to establish the Pentagon's cyber strategy as the United States enters an era in which any major conflict will almost certainly involve an element of cyber warfare".

As well as using Google's hacking allegations to intensify political pressure on China, the US will undoubtedly use the accusations to justify this expansion of cyber warfare capacities.