Google and China Eight Weeks Later: Where Are We Now?

Jeffrey Barlow
Pacific University

Recommended Citation
Google and China Eight Weeks Later: Where Are We Now?

Posted on March 1, 2010 by Editor

Editorial by Jeffrey Barlow

In the February issue of Interface, my editorial was on “Google and China: Minor Incident or Cyberwar?” [1]. One month after that piece and two months after the incident was announced, I want to revisit the issues here, because it gives us some insight into the notion of “cyber war,” if it clarifies little else.

While it is not my intent here to defend my earlier judgments, arrived at during six weeks of working in China, I think it easy enough to do so. My first judgment was simply that nothing is certain.

We now know a bit more, but given the amount of time which has passed, surprisingly little. We do not know, for example, how serious an impact the event will in fact have, either on Google’s relationship with China, or China’s relationship with the U. S. Google now says that it will be meeting with the Chinese government after the New Year’s holidays end there [2].

Interestingly, Google’s focus has apparently become less the incidents themselves than its desire to provide unfiltered searches in China—this is the issue being negotiated. While it is true that Google frequently conflated these issues in the initial responses to the incident, it is somewhat surprising to see the issue boiled down to this. If the incidents are to be used as a bargaining chip with China, it makes sense to make the issue network filtering. I do, however, have a fair amount of experience bargaining with Chinese institutions and officials, and I am very glad that I am not on that Google bargaining team—it will be very hard to get fruitfully from the one issue —"you hacked our servers!" to “And…uh….so we want an end to filtering!”

One reason this bargaining process is surprising is that the change in emphasis amounts in part to an affirmation of the position taken by many Chinese sources who felt that the issue was more a commercial one than a defense of privacy on Google’s part. Unfiltered searching, for example,
will not provide any additional protection to the Chinese dissidents who were supposedly hacked in the incidents.

But an end to filtering would be very good for Google’s share of the search market in China because it would then be the only completely open search engine for Chinese users. Other engines, notably Baidu, which has about two-thirds of the Chinese market to Google’s less than one-third, will, as Chinese corporations, be obliged to follow Chinese laws.

We also know a bit more about the origins of the attacks. Google invited the National Security Agency into the investigation in early February [3]. Whether the additional information comes from NSA or not, it is now held that the direct source of the attack was two Chinese educational institutions. However, because of the inherent uncertainties involved in trying to trace artful cyber attacks, our understanding has not in fact been decisively furthered. To quote The New York Times statement at the discovery:

“Within the computer security industry and the Obama administration, analysts differ over how to interpret the finding that the intrusions appear to come from schools instead of Chinese military installations or government agencies. Some analysts have privately circulated a document asserting that the vocational school is being used as camouflage for government operations. But other computer industry executives and former government officials said it was possible that the schools were cover for a “false flag” intelligence operation being run by a third country. Some have also speculated that the hacking could be a giant example of criminal industrial espionage, aimed at stealing intellectual property from American technology firms” [4].

These are pretty much some of the possibilities I discussed in February, though the mention of two specific Chinese schools is certainly an important new wrinkle.

I remain suspicious of anybody’s ability to identify the source of an attack without being able to access the machine that was directly involved, or, at a minimum, generous assistance from the Internet Providers involved. It is my understanding that to trace the activities taking place on a “captured” computer, that is, one to which a hacker has gained control, it is not enough to merely trace the attacker back to a network. To do so is to leave open the possibility that the attack went to that network, to a specific machine, but from that machine (another captured one) hopped to yet another network and another captured machine, and perhaps another and another. As The New York Times put it in part of an article which otherwise tries to build the case against the two Chinese universities:

“Beijing has not announced an investigation, but Web security experts emphasize that the Chinese government would need to be involved to find the ultimate perpetrators of the attacks.”
“The U.S. would not be able to trace this” back to the source, said O. Sami Saydjari, the founder of the Cyber Defense Agency, a private Web security firm based in Wisconsin. “We cannot trace it beyond borders. We’d need the cooperation of the Chinese” [5].

In China, Internet Providers are both few in number and tightly controlled. If the Chinese government is in any way involved in the attacks—and if it is not, it is difficult to see the point of the issue, it just becomes another of hundreds of thousands of daily hacking events, possibly devoid of political or international significance at all—then it is difficult to imagine the Chinese government pitching in to, in effect, investigate itself.

We have now traced the series of attacks being generally described as the Google attack to two networks in China, but until we are able to actually access the machines directly involved we have stopped short of certainty—that is the hackers may have utilized that machine as a route into yet another undiscovered source. This is why the experts quoted above left open the three possibilities that they mentioned, each of which recognizes the possibility of yet another undetected hop out of the network.

There are also some real shortcomings in the research of the American authorities concerned, which quickly announced that one of the two schools, the Lanxian Vocational School in Shandong, was closely linked to the Chinese military. There is a great deal of controversy over this particular designation [6] —many feel it rather to be a down-at-the-heels junior college equivalent incapable of producing true elite hackers and we must again wait for additional information to accumulate [7].

The other university, Shanghai Jiaotong, is indeed an elite school, comparable to America’s M.I.T. in China. Evidence, however, is largely circumstantial beyond the bare fact that apparently the attack was related to its network at some point [8].

The uncertainties inherent in this incident have provided a feast for news organizations. China is so high on the American media radar at present that the story has been repeated endlessly. One recent exhaustive analysis of the news gathering process on this one story by Jonathan Stray of the Neiman Media Labs [9], made this point:

“We often talk about the new news ecosystem — the network of traditional outlets, new startups, nonprofits, and individuals who are creating and filtering the news. But how is the work of reporting divvied up among the members of that ecosystem?

To try to build a datapoint on that question, I chose a single big story and read every single version listed on Google News to see who was doing the work. Out of the 121 distinct versions of last week’s story about tracing Google’s recent attackers to two schools in China, 13 (11 percent) included at least some original reporting. And
just seven organizations (six percent) really got the full story independently."

That is, of the welter of commentary and reporting on the issue, only a few sources possess real authority [10]. The others are not only repeating secondary reports, but often adding additional commentary and opinion to those original stories. This has been particularly true for the cyber war boffins, both individuals and institutions, including American defense groups, which stand to gain by increased anxieties and the resultant hope of enhancing their budgets.

Shay has a very useful table of the 121 unique stories which he examined from which a number of conclusions can be drawn: The New York Times was at least the partial source for the great majority of the stories. A number did access Chinese English-language sources, notably Xinhua, but only 18 of the 121 accessed any Chinese sources at all.

What then, at the last, do we learn about cyber war? The lessons to me seem to boil down once again to a very few:

- There is always going to be an element of uncertainty involved where cyber attacks are concerned.
- This uncertainty magnifies the risk of bad judgments.
- Where Sino-American relations are involved, there are major commercial and political interests internal to the U.S. involved, which further complicates the issues.

We are certain that there will be additional issues over the Google events, and we look forward to following them here at Interface.

Endnotes

[1] See “Google and China: Minor Incident or Cyber war?”


[6] Chinese bloggers and students at Lanxiang have been having a great deal of fun with the NYT story; for English translations go to: http://www.zonaeuropa.com/201002c.brief.htm#002 See also the Stray story below which also mentions other Chinese sources’ judgment on the school’s
nature.

[7] For a supportive view, see By Nick Farrell, “Google was brought down by Chinese hairdressers” Curl up and dye westerners, The Inquirer, Mon Feb 22 2010.

[8] For the sort of evidence being brought forward against Jiaotong (Entirely circumstantial in my opinion, with the possible exception of the reports initially quoted in the NYT articles quoted here, which have yet to reveal the nature of their evidence.) See Jaikumar Vijayan, “Chinese school linked to Google attacks also linked to ‘01 attacks on White House site” A former U.S. Army officer linked ‘01 hacker to Shanghai Jiaotong University. February 19, 2010 07:06 AM ET Computer world.com at: http://www.computerworld.com/s/article/9159258/Chinese_school_linked_to_Google_attacks_also_linked_to_01_attacks_on_White_House_site


[10] According to Stray: — “Only seven stories (six percent) were primarily based on original reporting. These were produced by The New York Times, The Washington Post, the Wall Street Journal, The Guardian, Tech News World, Bloomberg, Xinhua (China), and the Global Times (China).”

This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=3741] .