Google and China: Minor Incident or Cyberwar?

Jeffrey Barlow

Pacific University

Recommended Citation

Google and China: Minor Incident or Cyberwar?

Rights
Terms of use for work posted in CommonKnowledge.

This editorial is available at CommonKnowledge: https://commons.pacificu.edu/inter10/7
Google and China: Minor Incident or Cyberwar?

Posted on February 1, 2010 by Editor

Editorial by Jeffrey Barlow

- Introduction
- What is Certain?
- Who was Responsible?
- The need for caution in a period of rising tension
- Cyberwar and democracy

Introduction

I was in China from December 17, 2009 to January 22, 2010, teaching and lecturing at three Chinese universities. In addition, I spent five days in Hong Kong, much of it with very knowledgeable members of the international business community. This was the period when the recent Google incident began — by which I mean Google’s charges that attempts had been made to hack the accounts of Chinese dissidents in Gmail, causing Google to state that it would no longer censor its Chinese search results, and would, if necessary, leave China.

I had ample opportunity following these events to discuss the issues with Chinese people. The audiences at my presentations collectively numbered several hundreds, and we had a total of well over three hours of discussions together following my presentations, not counting numerous smaller lunches and dinners. My interlocutors included Chinese undergraduates at a medical school in Wenzhou, a seminar of Chinese graduate students of law in Nanjing, and a graduate and undergraduate group including ethnic minorities, such as Zhuang, Yao, Dong, and Miao in Nanning [1].

I have also, of course, been writing on issues relating to China and the Internet for several years now, as well as on cyberwar. [2]. Given this recent experience in China, and my continued interest in related topics, it may seem probable, then, that I have something profound to say upon the subject of Google and Cyberwarfare. However, perhaps the most profound thing I can
say is that in this matter I consider very little is proven, nothing is certain, and not even a deliberately paced move to judgment is warranted.

This uncertainty is inherent to most cyberwarfare incidents. We often will not even be certain that such incidents have occurred; we will rarely know who is responsible, or what their motives were. Part of the cost of the Internet is relative anonymity for the perpetrators of such incidents.

This inherent uncertainty creates a very volatile, even potentially dangerous, situation when such incidents involve the interests of nation states, particularly ones as powerful, and as necessary to a peaceful international order, as are the United States and the People’s Republic.

What is Certain?

A brief answer here: almost nothing is certain. There was an incident, or a series of incidents, and these became linked in the media to many other similar but unrelated incidents in an attempt to establish meaning, and to draw audiences. From there everything gets rather murky.

Even Google’s motives in raising the issue now are disputed. Particularly in China, Netizens seem mostly to believe that the issue is simply about Google’s frustration at its local market share. It is prepared to leave because it was not a winner; it has only about one third of the market for search engines as its closest Chinese competitor, Baidu. This is a very interesting shift in attitudes between Chinese and American people.

After many decades of doing outrageous things for the flimsiest of idealistic or ideological reasons, Chinese now see economic explanations as dominant ones. Americans, after decades of criticizing this Chinese behavior, now believe that Google acted not out of self-interest but out of altruism. And after the event, Google’s statement that it was prepared to withdraw from China caused its stock prices to increase markedly, demonstrating, if nothing else, that Americans are prepared to support enthusiastically acts in opposition to Chinese policies.

So, accepting Google’s explanations, what do we know about the possible perpetrators? Again, nothing is certain. This, of course, does not prevent the media from not only speculating, but of presenting speculations as certainties.

Media criticisms of China often show some common characteristics which Chinese people, including very thoughtful and learned ones, interpret as due to prejudice. One of these is that while early reports are often carefully nuanced, subsequent pieces accept the earlier tentative ones as rock-hard evidence and a cascade toward certainty ensues. It is also common now that headlines or article headers seem to proclaim certainties while the content is often considerably more tentative.

An important piece by John Markoff in The New York Times is almost a classroom example for this sort of process. The article title fairly screams: “Evidence Found for Chinese Attack on Google” [3]. Most readers would, like myself I think, immediately assume a smoking gun. This is
the only part of the piece that everybody will read; most readers are not going to go much further. Thus we have it, case solved, the Chinese government did it!

This article deserves some close analysis, if only because the stakes are proving to be very high. Secretary of State Hillary Clinton quickly became involved, the Chinese government took a very obdurate position, and soon we have had a major international incident, followed by Chinese anger over U.S. intentions to soon sell major weapons systems to Taiwan, and the Dali Lama waits in the wings should Sino-American relations somehow survive the first two disruptions. Thos relations have gone in less than a month from quite warm, to very distant, with various important meetings and reciprocal visits being cancelled.

The argument that the Chinese government was responsible is, as best I can tell, based largely upon the evidence cited in Markoff's article [4]. However, the article itself tells us only that the perpetrators are likely Chinese speakers because the malicious code was in the Chinese language and copied from a source that appeared, it is said, only in a Chinese technical journal. Does this in fact prove that the Chinese government did it?

The expert interviewed by Markoff used numerous qualifiers and finally concluded: “Occam’s Razor suggests that the simplest explanation is probably the best one.” I will suggest below that there are several even simpler explanations, and that, in any event, the simplest explanation may not be the best one. The instant appeal of Occam’s Razor here is probably that, as one analyst has said, it is a “mirror of prejudice” [5]. That is, to us, the simplest explanation is that the Chinese government did it, because in our opinion, that is the sort of thing they would do. In China there are more than a few who believe, on pretty much the same grounds, that the C.I.A. is responsible.

**Who was Responsible?**

If not the Chinese government, then who? Markoff’s expert wound up appealing to a medieval argument for good reason; that is about the best that we can do. There are so many ways to loop Internet attacks through the web itself that certainty is finally impossible without something other than electronic evidence. There are also many ways to “spoof” identities.

This attack began, it seems, most directly from a computer based in Taiwan, and then it has been followed back to mainland computers. This is an awfully simple route. Hackers and spammers in the private black-hat sector routinely use many more hops than that. Given purported Chinese control of some critical American sites, it would not have been impossible to pass the attack through Pentagon computers, for example. For most analysts, a loop ending at a Chinese Internet Protocol address was as far as it was necessary to go; beyond that, lacking an ability to open up those machines, it was probably as far as they could go.

One argument for it not being the Chinese government is simply that the attacks could have been much more sophisticated and eminently deniable. As Google stated, the attacks were unsuccessful, and all the evidence suggests that the authors simply exploited known
weaknesses in a number of computing programs.

If solid evidence that it was the Chinese government is lacking, for many, such evidence is not necessary. Who else had motive and ability? But this argument fails; there are many possible perpetrators with both motive and ability.

One possible perpetrator is any one of a number of young Chinese nationalists popularly known as “Angry Youth,” or, if referring specifically to hacker nationalists, as Hong Ke (Red Guests) [6]. These folks think that the government is just not doing enough to stand up to the bad guys, in this case, the former Western imperialists. These people see themselves as a sort of vigilante volunteer force ever ready to respond to slights against China by hacking web pages or computers. I return to them in my conclusion below.

Do any of the Angry Youth have the ability for hacks of the sorts which occurred? Unquestionably. Among their numbers are distributed groups of well-trained and well-equipped I.T. specialists. They can write code and read even highly technical articles, like the one discussed above with the smoking code in it. And, as suggested, these attempts do not in any event seem to have been particularly sophisticated.

Are there other possible suspects? What if we ask the question qui bono — who benefits? Then the list quickly lengthens. Many of the firms targeted in these events, in addition to Google, were large Western corporations. What, then, about commercial rivals? And while we are speculating about commercial rivals, let us remember that the United States itself allegedly once turned electronic espionage techniques upon European corporate rivals, using the National Security Agency’s Echelon operation [7].

All corporations, of course, have strong motives for cracking into their competitors’ internal documents. What of Google’s competitor in China, Baidu? True it has 60% of the search engine market already, but perhaps it aspires to total monopoly?

If we posit the actions as deliberately misleading and intended to stir up trouble between the Chinese government and Google, or even between the Chinese and American governments, many other possible suspects enter the list: The anti-governmental hacker mirror image of Angry Youth, Chinese dissident youth; or Fa Lun Gang, the Buddhist sect which once took over Chinese Central Television for most of a day, operating, apparently, from a former American air base and listening post in Taiwan. Even Taiwan itself, which will benefit greatly from these events as the U.S. Congress discusses arms sales to it.

These latter potential suspects must strike any reasonable person as distant possibilities indeed, but again, nothing is certain in these events. This leads, I think, to the necessary conclusion that great caution is required here.

The need for caution in a period of rising tension
What began as an incident between a single corporation and unknown hackers, who, after all, failed in their goals to open up Gmail accounts, has escalated to the point where the events are often now described as cyberwar [8]. China has responded in turn, by accusing the U.S. of online warfare in the case of the Iranian election, and attacking U.S. motives in opposing censorship as ultimately political ones [9].

This is a very dangerous time in Sino-American relations and for the Internet as well. Tensions between the U.S. and China are, in my opinion, higher than they have been since 2001 when China forced down an American plane, which supposedly intruded into their air space around Hainan Island in the South China Sea.

One important question is, given that such incidents as these have happened regularly for some time, and that the Chinese have often been accused of committing them, why has the issue rather suddenly become so salient? Many of us think that most nations as well as many non-state groups have engaged in such activities on a regular basis for a very long time. There are millions of hacking attempts every year.

There are no easy explanations, of course, for sudden changes in either media coverage or public opinion. But I think that the international context has changed dramatically since the onset of the recent banking crises about this time last year. As a result of the crises, the Chinese are much less prepared to defer to Western, and particularly, American models, whether they are economic or political ones. Consequently they are, as Martin Jacques has argued in his recent work, *When China Rules the World* prepared to be much more active in redressing what they feel to be long-standing injustices in the global political and economic order.

I found this to be true among the Chinese audiences to which I spoke. There is a very strong feeling of triumphalism among what I would estimate to be about ten percent of Chinese youth, based on my personal experience. These feel that China has long been oppressed, and now has the power to resist additional wrongs, and even to redress outstanding grievances.

The U.S., for its part, has not made any adjustments in either policy or attitudes to the “rise of China”. Many Americans think of China’s progress as a trick or due to cheating, possibly illusory, or simply a result of the Chinese adopting our system. Included in this mélange of attitudes is a great deal of negativity toward China, and as the Google incident shows, an uncritical readiness to accept the worst possible interpretation of every event. A recent comment I saw in an on-line copy of *Business Week* rather sums it up for many Americans: “China can kiss my @zz !!!!!!” [10].

China is correct that for many Americans the Internet is a tool, which it is hoped, will bring about regime change there. The U.S., in turn, discusses being even more aggressive in utilizing electronic means to influence Chinese internal affairs. Some have suggested funding servers in the U.S. configured to facilitate Chinese Netizens’ evasions of their country’s firewalls [11].
To do so amounts to a formal policy commitment to regime change and formal encouragement to Chinese secessionists or revolutionaries. How then, would we respond if China were to create equivalent servers for use by Pakistani supporters of Al Qaeda, which include, apparently the Pakistani military intelligence? Pakistan is, after, all, an ally of China in some important regards.

In addition, Americans are locked in a seemingly insoluble internal political conflict, unable to agree on fundamental issues at a national level, despite the crisis which we all agree is upon us. Teabags and pitchforks have been substituted for coherent national discussions. This is an unfortunate time to have rational debate over cyberwarfare, China policy, or anything else substantive. For Clinton or Obama to raise doubts or cautions at this time would be taken as a lack of resolve, of toughness, even of patriotism.

This conflict is unfortunate in a number of ways, but especially for Chinese democracy. Many Chinese think that the Internet is in fact already steadily encouraging democracy in China (See review of Marina Yue Zhang’s work, China 2.0 in this issue.) This encouragement, however, is done in a manner which permits China both stability and political reform, even if not at the dramatic pace which might satisfy many Americans [12].

The hardening of both American and Chinese positions and the policy brawls in the U.S. make compromise in this incident unlikely. Google has told China it will not censor search data; China believes that the U.S. spreads disinformation in an attempt to force “regime change” abroad.

The implications for the worldwide Internet are not good. It may shortly be broken — de facto, if not formally — into national segments and many users will be unable to search outside those national boundaries.

**Cyberwar and democracy**

The implication of this recent event, and one possible outcome of current developments, is that cyberwarfare will become more or less a constant factor, not so much a specific event as an ongoing reality. It may indeed have been the case that in fact this happened sometime ago — many point to 2005 as the time at which attacks seemingly emanating from China increased markedly. But we are, at present, on the verge of making such mutual electronic warfare part of our national policy.

To do so will raise some serious issues for governance. Civilian control of the military has been a critical issue in American democracy. Douglas McArthur, when commander of U.N. forces in Korea, tried to put the U.S. and China in a position where an American invasion of China was a likelihood, and nuclear war a possibility. President Truman, at considerable political risk, yanked McArthur from command. If cyberwar with China becomes a national policy, given that it is necessarily covert, how are we to assure civilian control of such activities?

And how to be sure that it remains a state function, and not a rapidly accelerating chaotic series of events involving non-state groups such as Angry Youth in China and American cyber-vigilantes
hacking away at each other and at the Internet? That genie will be very hard to get back into the bottle.

Endnotes

[1] For my blog maintained through this entire period, see: http://chinatripper.wordpress.com/ These entries were largely spontaneous and emphatically do not represent the perspectives of the Berglund Center for Internet Studies, nor of Pacific University. I have also rethought some of my positions on the basis of additional evidence.

[2] I more often used the term netwar. See: http://bcis.pacificu.edu/journal/results.php?cx=006538533868481694997%3Am_imeb1yh-g&cof=FORID%3A9&ie=UTF-8&q=netwar+Barlow&sa=Search&siteurl=bcis.pacificu.edu%252Fjournal%252F#1269


[4] Google has not, insofar as I am aware, ever stated that in fact the Chinese government was responsible, though that too has entered the discourse as a certainty.


here that I believe that this is already being done.

[12] See the review of Marina Yue Zhang, China 2.0 for examples of just this argument.

This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=3725].

6 THOUGHTS ON “GOOGLE AND CHINA: MINOR INCIDENT OR CYBERWAR?”

Cherise Schmider
on January 30, 2014 at 5:18 PM said:

Nice weblog right here! Additionally your web site rather a lot up very fast! What web host are you using? Can I am getting your associate link in your host? I want my website loaded up as quickly as yours lol

Alesha Grothoff
on January 30, 2014 at 6:14 PM said:

Thanks a bunch for sharing this with all of us you really recognize what you’re speaking about! Bookmarked. Please additionally seek advice from my site =). We can have a hyperlink trade agreement between us!

Omer
on February 4, 2014 at 11:25 PM said:

Losing weight is not dependent on diet on your own, however. As an example, pasta, various potato recipes, various sugars, i.

If you’re trying to prevent hunger and consume less, protein is the approach to take due to the fact healthy proteins satisfy craving for food much more than fats as well as carbs.

http://mydrawbridge.com/profile/ritalindst
Wedding rings of the hcg weight loss diet has our throw choose akin to dieter those a lot Health calorie-restricted diet regime. The recipes for these dishes are widely available due to websites and books dedicated to HCG diet plans. Visit the Hcg Supercharged website now and like the brand new offers for special packs.

spybubble

com The merchandise isn’t sold via another outlets, during the event you could probably comes across other websites which link straight towards fee processor page. -Call Tracking - See all the numbers the phone has called and see every one of the numbers which have phoned them. While there’s plenty of specifics of the product, the particular people behind the service remain a mystery.

Ny lottery results

My advice to someone considering training racehorses as a career is to go to school and have a background. A good rental location is one that does not have a lot of other rentals. The Powerball lottery game has been very popular and thus a technology that helps maximize the winning chances has been created.