GOOGLE, CHINA AND A WAKE-UP CALL TO PROTECT THE NET

Posted on January 19, 2010 by Keghart

THE GLOBE AND MAIL

Category: Opinions



By Ron Deibert and Rafal Rohozinski, The Globe & Mail, Toronto, 16 January 2010

Ron Deibert is associate professor of political science and director of the Citizen Lab at the University of Toronto's Munk Centre for International Studies. Rafal Rohozinski is CEO of the Ottawa-based SecDev Group. They are co-authors of the GhostNet study detailing alleged Chinese cyberespionage.

Google's announcement that it had been hit by cyberattacks from China and that it's reconsidering its services in that country has smacked the world like a thunderclap: Why the drastic move? How will China respond? Will other companies with interests in China, such as Microsoft and Yahoo, follow suit? What does it mean for the future of cyberspace?

By Ron Deibert and Rafal Rohozinski, The Globe & Mail, Toronto, 16 January 2010

Ron Deibert is associate professor of political science and director of the Citizen Lab at the University of Toronto's Munk Centre for International Studies. Rafal Rohozinski is CEO of the Ottawa-based SecDev Group. They are co-authors of the GhostNet study detailing alleged Chinese cyberespionage.

Google's announcement that it had been hit by cyberattacks from China and that it's reconsidering its services in that country has smacked the world like a thunderclap: Why the drastic move? How will China respond? Will other companies with interests in China, such as Microsoft and Yahoo, follow suit? What does it mean for the future of cyberspace?

Some may be puzzled. How does Google's decision to end censored search services in China relate to the attacks on its infrastructure, the theft of intellectual property and access to private e-mail accounts? Well, there are connections. Censorship, surveillance and information warfare are part of an emerging storm in cyberspace in which countries, corporations and individuals are vying for control.
China sees cyberspace as a strategic domain to further its ambitions as a superpower, and as an environment to be controlled in order to preserve domestic stability. It has invested heavily in a variety of tools and strategies to achieve this end – from the Great Firewall of China to stifling regulations that prohibit free speech online, and to tolerating and even encouraging attacks on foreign sources of information emanating from its sovereign jurisdiction.

Beijing has shown a willingness to take drastic measures. For the past six months, for example, the inhabitants of the Xinjiang region have been cut off from the Internet as part of China's attempt to stifle civic unrest.

China has also been bold in projecting cyberpower. For years, cyberespionage activities that target groups and countries of strategic interest to Beijing, such as the GhostNet network we uncovered, have been tracked back to mainland China. The fact that these activities have not been proved to have been carried out by the Chinese government speaks to the success of strategies that rely on

privateering and outsourcing to criminal hacker groups, thereby shielding authorities from any direct blame. Similar strategies are said to be carried out in Russia, Iran and elsewhere.

Google has faced the brunt of China's aggressive cyberpolicy – and, apparently, has had enough. But Google's response needs to be seen from a broader perspective.

The tectonic plates of cyberspace are shifting. The debate around cybersecurity, and calls for greater content controls globally, have dire consequences that go well beyond the curtailment of freedom of expression and access to information. Google's mission may well be to make all the world's information "universally accessible and useful," but its business model depends on an open global Internet.

How China responds to Google will have far-reaching implications for the future of cyberspace. It could enter into talks with Google that would lead to a gradual opening of Chinese cyberspace. Or it could call Google's bluff and shut down Google.cn, thus depriving the company of its 30-per-cent market share on the mainland. Or it could block Google from indexing Chinese domain or IP space altogether, shutting Chinese information space off to users of Google. Should that happen, the once unified global Internet space will begin a process of disintegration as countries define their own sovereign clouds.

Whatever path China takes will have immense repercussions for the future of cyberspace – and for the advances in access to knowledge, democratization, basic freedoms and human rights that cyberspace has helped to generate over the past 20 years.

So what's the next step for Google? Will it lead a global coalition of governments, corporations and citizens to protect cyberspace as an open, global space? Will it shake the remainder of the IT industry from their obsession on the bottom line into realizing that the very future of their industry depends on the position they take in defending the global information commons?

How our leaders respond is equally important. While Washington and other capitals realize the importance of cyberspace for the projection of military and intelligence power, they've been slow to recognize its importance to the advance of democratic values worldwide and as a global asset to be protected in its own right. Action is needed at the global level to ensure that cyberspace doesn't slip into a new dark age, torn by territorial divisions and segmented into privatized spaces.

Google's principled policy may be a wake-up call for those concerned with Internet business and security – but it should be a call to the barricades for the rest of us.

Ron Deibert is associate professor of political science and director of the Citizen Lab at the University of Toronto's Munk Centre for International Studies. Rafal Rohozinski is CEO of the Ottawa-based SecDev Group. They are co-authors of the GhostNet study detailing alleged Chinese cyberespionage.