IN FOCUS

24 JAN 2014

CHINA TARGETS TIBETAN SITES: PREEMPTIVE OR DEFENSIVE?

Simrat Virk
Research Associate, CAPS

China resorting to extreme measures to fulfill its goals isn't a new phenomenon. Keeping in mind that most of the media in China is state-controlled and the information that comes in and goes out undergoes strict government scrutiny- cyber hacking is the latest trend employed by China in Tibet. This is yet another attempt by China to restrain the voice of the exiled Tibetan community living in India.

Cyber hacking has been a criminal offence in China since 1997; however the implementation of any law prohibiting it is missing. Action is taken only if the attackers target state secrets and assets. The first public trial in a hacking case was carried out in 1998 on two people who hacked a state-owned bank in Jiangsu, stealing several thousand dollars; one of them was later executed.[i] Not only the locals, even foreign journalists and others working in China have been vulnerable targets for hackers. For example, David Barboza, a journalist working with *The New York Times,* found that his account had been hacked by a group of hackers in early 2013. This was soon after he alleged that the activities of relatives of Premier Wen Jiabao were suspect. [ii] The foreign press has predictably been at the receiving end of most of the activities of hackers. A report given in by a leading cyber security firm, Mandiant, states that cyber-crimes on journalists have been rampant since 2008. [iii]

Trends seem to suggest that most cyber-hacking cases are state sponsored. Data also shows that hackers target some of the most critical sectors; victims mainly include organisations dealing with information technology, think tanks working on China, aerospace industries, agencies involved with scientific research, and international organisations like the

Olympic Agency and the World Anti-Doping Agency (the latter two particularly after the 2008 Beijing Olympics). Reports have suggested that sites run by Tibetan activists have also been regularly attacked by hackers. Even the United States has not been spared. The Annual Report to Congress last year for the first time officially accused China of launching cyber-attacks against the US Department of Defence.[iv] Experts believe that since none of the agencies targeted have any commercial value therefore cyber-attacks such as these are perhaps politically motivated.

As mentioned previously, dissidents, particularly within the Tibetan community are primary targets for the hackers. Reuters reported in August last year that the Chinese language website of the Central Tibetan Administration, CTA (formerly known as the Tibetan Government in Exile) had been targeted.[v] The aim, experts claim was an attempt to target sites of the human rights activists, who perhaps are the frequent visitors of the site. (However, the website was restored the next day.) Kaspersky, the lab that led the report also reported that it was indeed the same hackers who had targeted the site in 2011. It is believed that the site has nearly 700 visitors every day; therefore the consequences of such cybercrimes are immense.[vi]

ARTICLES BY SAME AUTHOR

CHINA'S RESPONSE TO THE SYRIAN CRISIS
CHINA CONTINUES WITH MINING WORK IN TAR AMIDST PROTESTS

Dharamsala, which is home to several thousand Tibetan refugees, is known to witness the maximum number of cybercrimes in the world.[vii] Chinese hackers now not only target the sites of the CTA or the Dalai Lama, but also those believed to be close to the Dalai Lama. Even local Tibetans living in India find themselves being targeted frequently. Communication lines between Tibetans living in exile and those in Tibet have improved tremendously, but have in the bargain become soft targets for such illegal activities. Realising this, Gyatso Sither, coordinator at the Tibet Action Institute, a New York based nonprofit institute that trains volunteers on how to use safe lines of communication states, "if we don't use secure lines of communication, Tibetans in Tibet could be prosecuted"; for exchanging sensitive information with their counterparts in India. [viii] He like many others train students on the dangers of unsafe mediums of communication that include opening unexpected attachments and sharing email passwords.

Experts believe that one of the primary reasons for Chinese hackers targeting Tibetan organisations and individuals is to keep a check on the activities of the protestors. One form of protest that the Tibetans now resort to is that of self-immolation. There has been a spurt in the number of cases reported; since 2009 there have been 120 fresh cases that have been reported. China in an attempt to preempt such incidents of self-immolation, hacks the accounts of protesters and campaigners so it can gather information on any possible incident of self-immolation. Another reason for the hacking is to quell the voice of the Dalai Lama and his supporters; and to prevent his message from getting across to the thousands of supporters. In this context, Chen Quanguo, Tibet's Communist party chief is believed to have written in the party journal Quishi, "Work hard to ensure that the voice and image of the enemy forces and the Dalai clique are neither seen nor heard." One of the steps includes an increase in the monitoring of online content.[ix] What is perhaps the primary reason for an increase in cybercrimes is to disallow the voice of the Tibetan agitators from getting across to the rest of the world, thus gathering support for their cause and more importantly preventing news of human rights violations from trickling out.

ARTICLES BY SAME AUTHOR

CHINA'S RESPONSE TO THE SYRIAN CRISIS
CHINA CONTINUES WITH MINING WORK IN TAR AMIDST PROTESTS

Tibet now faces the added threat of cyber hacking which will be an impediment to its endeavour for freedom. It will therefore have to ensure that China does not use too hardline an approach towards Tibet's freedom struggle. Hence, only following guidelines for cyber security is not enough, strict anti-hacking measures are the need of the hour.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies CAPS)

----------***XXX***----------

[i] *Cyber Hacking; of the cyber – universe,* The Economist , April 6, 2013, at http://www.economist.com/news/special-report/*21574636*-chinas-state-sponsored-hackers-are-ubiquitousand-totally-unabashed-masters (accessed on January 16, 2014)

[ii] Adam Clark Estes, *China hacked The New York Times for four months straight,* The Wire, January 30,2103, at http://www.thewire.com/business/2013/01/china-hacked-new-york-times-four-months-straight/61620/ (accessed on January 16, 2014)

[iii] *Ibid*

[iv] *Annual Report to Congress; Military & Security Developments Involving The People's Republic of China,* May 6, 2013 at http://www.cfr.org/china/annual-report-congress-military-security-developments-involving-peoples-republic-china/p28408 (accessed on January, 20, 2014)

[v] Jim Finkle, *Dalai Lama's site hacked, infects others-expert,* Reuters, August 13,2013, at http://uk.reuters.com/article/2013/08/12/uk-tibet-cyberattack-idUKBRE97B0R020130812 (accessed on January 16, 2014)

[vi] *Hacked*, First Post, August 13, 2013, at http://tech.firstpost.com/news-analysis/website-of-tibets-government-in-exile-hacked-214775.html (accessed on January 15, 2014)

[vii] Jonathan Kaiman, *Hack Tibet,* Foreign Policy ,2013, at http://www.foreignpolicy.com/articles/2013/12/04/hack_tibet_china_cyberwar (accessed on January 15, 2013)

[viii] *Ibid*

[ix] *China Targets Dalai Lama for Spreading Propaganda*, Global Voices Advocacy Defending Free Speech Online, November 13, 2013, at http://advocacy.globalvoicesonline.org/2013/11/06/netizen-report-china-targets-dalai-lama-for-spreading-propaganda/ (accessed on January 16, 2014)