

Rallying For Democracy

<http://www.rallyingfordemocracy.org>

China In Focus 20- China vs Google: Risky-Business and Cyber-War

28/01/2010 18:12 by admin

Recent hacker attacks of Google's Gmail email systems have been described as a violation of human rights and international internet protocols. The attacks went far beyond monitoring the communications of dissidents in China. Also hit by the attacks were U.S. government sites, private corporations with industrial secrets in which China has an interest, large U.S. Defense contractors in which experts said the Chinese were seeking information on new weapons systems and IT firms where China was seeking to steal sophisticated software source codes, which would enable China to become even more proficient in internet spying and sabotage. In response to Google's protests, the official People's Daily published a commentary that called Google a "spoiled child" and noted that in its pursuit of profit the Internet giant would not act on its threat to pull out of the Chinese market.

Did Google simply misunderstand China's peaceful pursuit of internet expansion? In March, 2009, researchers in Toronto concluded a 10-month investigation that revealed a massive cyber espionage ring called Ghostnet, which penetrated more than 1,200 systems in 103 countries. The victims were foreign embassies, NGOs, news media institutions, foreign affairs ministries, and international organizations. Almost all Tibet-related organizations had been compromised, including the offices of the Dalai Lama. The attacks used Chinese malware and came from Beijing.

More than simply risky business, the attacks followed a continuation of Chinese military doctrine, which was implemented more than ten years ago under the direction of China's supreme leader, Jiang Zemin. This 21st Century version of Mao Tse Tung's "People's War" utilizes large China-based cyber strike force groups, with names such as the Red Hackers and Ghostnet, which have been recruited and mobilized under the tutelage of the Chinese military's information warfare department. In April, 2009, the Wall Street Journal reported that China was suspected of being behind a major theft of data from Lockheed Martin's F-35 fighter program, the most advanced airplane ever designed. Multiple infiltrations of the F-35 program apparently went on for years.

In 2004, Sandia National Laboratories traced the origins of a massive cyber espionage ring back to a team of government sponsored researchers in Guangdong Province, China. The hackers, code named by the FBI "Titan Rain," stole massive amounts of information from military labs, NASA, the World Bank, and others.

Significantly, the recent December 2009 attacks that shocked Google demonstrated an evolution of China's cyber-warfare capabilities. An IT security expert told the Washington Post on January 14, 2010, "They are using multiple types [of penetration] against multiple targets - but all in the same attack campaign. That's a marked leap in coordination."

AsiaSentinel.com reports on January 22, 2010: "Research and development in IT, including cyber-espionage and counter-espionage figure prominently in the 12th Five Year Plan (2011-2015) which is being drafted by both the central government and the People's Liberation Army (PLA). President and Commander-in-Chief, Hu Jintao, has put expansion of the PLA's cyber-warfare capacity as a top priority of the defense and security forces.

"Preferential policies are also being made available for civilian IT and telecommunications industries, which have since the 1980s been sharing resources and data with relevant units in the PLA, the paramilitary People's Armed Police and the Ministry of Public Security. The PLA General Staff Department is paying above-average salaries to attract "accomplished and patriotic hackers." A number of such hacker-turned-IT specialists are believed to have been placed as "moles" inside the China operations of high-tech multinationals. Moreover, Chinese missions in the United States and other countries have the past year taken advantage of the recession in the West to recruit hundreds of Chinese graduates from the best computer-science departments in Western universities."

Sensitive and public information about the Chinese military's use of IT as a cornerstone of its "Revolution in Military

Rallying For Democracy

<http://www.rallyingfordemocracy.org>

Affairs" has been readily ignored by many Western policymakers and corporations who see China as the principal market for economic gain. The April 25, 2002 Los Angeles Times contained a feature story describing a classified CIA report warning of a wave of potential attacks by Chinese students backed by authorities in Beijing to actively damage and disrupt US computer systems through the use of internet hacking and computer viruses. The LA Times quoted a US intelligence official as stating, "The Chinese government is actively and aggressively working on their cyber warfare capability. They have a lot of people and a lot of brainpower, and they are smart enough to appreciate that a significant aspect of any future conflict is going to be cyber in nature."

Following a 2000 incident that involved the Chinese Air Force downing of a U.S. military aircraft over the South China Sea, over 1,200 cyber attacks against US government and commercial web sites disrupted or defaced entire systems with graffiti and Chinese patriotic messages vowing revenge for the death of a Chinese pilot. The attacks were generated by student hackers in China, and US officials believed that tacit approval was given by the Chinese government.

Japan, India, Europe and Taiwan have been the targets of numerous hacker attacks and penetration from Chinese-based sources. Many of these attacks have directly followed foreign policy, security or trade disputes. Because Western companies and governments have ignored the human rights of the Chinese people to free expression and the flow of information, Beijing has been emboldened to impose its will internationally. Inside of China, web sites related to Tibetan freedom or the Falun Gong religious movement have been repeatedly targeted regardless of the country in which they are located. In China, with the assistance of Western companies such as Google and Yahoo, security officials have blocked information of sensitive subjects that threaten the power of the Communist Party. The January 14, 2010 Washington Post reports that the Chinese government has blocked or shut down thousands of web sites, and has blocked YouTube, Twitter and Facebook. In addition, some 136,000 unregistered websites have been closed down.

The advent of the dominance of cyber war capabilities in China's was advocated just one decade ago by visionary PLA 21st Century warfare strategists such as Maj. General Dai Quingmin, who was Chief of the PLA's Information Warfare Center in Wuhan. Supported by Communist Party and Central Military Commission leader Jiang Zemin, General Dai pioneered the long-term war-fighting doctrine of preemptive attacks on computer and information-based systems. The core objective of the doctrine is that "the weak can defeat the strong" by turning greater opponents' most powerful weapons and technologies against them.

The cyber-capabilities gap has been quickly reduced by utilizing technologies from American IT corporations, sending thousands of bright young students to the most advanced Western university IT programs and permitting them to work for leading hi-tech companies in Silicon Valley and elsewhere before returning home. Li Yanhong, aka Robin Li, worked in Silicon Valley before returning to China to set up what is now the world's largest censored internet search engine, known as Baidu. He started with \$26 million in Western venture capital, including a modest grant from Google. The January 14, 2010 Washington Post reports that, in the days following Google's protests of cyber attacks, Baidu's stocks on Nasdaq surged 21 percent, adding \$2.8 billion to the company's market value in only three days.

A classic book on 21st Century war fighting, titled "No Limits Warfare," published by the People's Liberation Army in 1999, incorporates dual-use high tech hacking, economic warfare and low-tech terror networks, such as Bin Laden's, under classical Chinese strategic doctrine. The book was a clarion call to the Chinese people to prepare with confidence for future conflict with the "more powerful" West. The authors call for breaking with all limits on civilian vs. military, and using "all means, including nonmilitary means, for striking at the enemy from all angles and at all levels, to meet our war aims. No limits warfare is very broad, including hackers, with such computer players following national political aims, being no longer hackers but rather internet supremacists."