US-China tensions flare over Snowden's revelations

John Chan
27 June 2013

The supposedly cooperative "new model of great power relations" proposed by Chinese President Xi Jinping during his informal summit with US President Barack Obama in California earlier this month has quickly broken apart following Edward Snowden's revelations about the extensive and intrusive US cyber operations directed against China.

The anger and concern in Beijing over the cyber warfare implications of the American hacking and surveillance has been compounded by the US accusations against China for allowing Snowden to leave Hong Kong last weekend.

The former National Security Agency (NSA) contractor has revealed to the world, the NSA's massive cyber hacking and electronic data collection in China, as well as the US and internationally. His revelations have dealt a blow to the Obama administration's propaganda offensive branding China as the main threat to global cyber security.

Hong Kong, a Chinese territory, not only defended its actions in allowing Snowden to leave as "lawful", despite a US request to detain him. Moreover, it requested an "explanation" from Washington about the NSA's hacking of the city's computers since 2009. According to Snowden, this cyber intervention included the Hong Kong Internet Exchange, which handles all the territory's Internet traffic.

Washington openly attacked Beijing for letting Snowden leave Hong Kong. White House spokesman Jay Carney dismissed the Hong Kong government's explanation and accused China of being behind the decision to allow Snowden to fly out. In what amounted to a threat, he warned: "That decision unquestionably has a negative impact on the US-China relationship."

Chinese foreign ministry spokeswoman Hua Chunying replied on Tuesday: "The accusation that the US side made against the central government of China fell short of proof. The Chinese side will absolutely not accept it." Hua added: "The US side's doubt about the lawful operation by the government of the Hong Kong Special Administrative Region is totally unreasonable."

China's state-owned media voiced stronger criticisms of Washington's rank hypocrisy. The Xinhua news agency declared in an editorial that the US, which "has long been trying to play innocent as a victim of cyber attacks, has turned out to be the biggest villain in our age."

A front-page commentary in the Chinese Communist Party's *People's Daily* on Tuesday praised Snowden for "tearing off Washington's sanctimonious mask." Wang Xinjung of the Academy of Military Science wrote: "Not only did the US authorities not give us an explanation and apology [over the exposed US hackings into Chinese networks], it instead expressed dissatisfaction at the Hong Kong special administrative region for handling things in accordance with law."

The US, Wang declared, "has gone from a 'model of human rights' to 'an eavesdropper on personal privacy', the 'manipulator' of the centralised power over the international Internet, and the mad 'invader' of other countries' networks."

There are real fears within China's academic and government circles over the implications of the US cyber operations against China. Jia Xiudong of the China Institute of International Studies told *China Daily* on Monday that the scale of the US hacking against China "is shocking, it is beyond expectations." He added: "Snowden's claims show that many such attacks may be backed by the US government."

In an interview with the English-language Hong Kong-based *South China Morning Post* on June 12,

Snowden revealed intensive US hacking into Hong Kong and mainland Chinese computer networks. (See: "Edward Snowden reveals US computer hacking aimed at China")

Just before Snowden's departure from Hong Kong, the *Post* published more details of US surveillance operations to collect the data of Chinese mobile phone companies and the NSA's hacking at Tsinghua University in Beijing and the Hong Kong headquarters of Pacnet, one of the largest undersea fiber optic cable operators in Asia.

In particular, Snowden disclosed the collection of vast mobile phone messaging data in China. He said: "The NSA does all kinds of things like hack Chinese cell phone companies to steal all your SMS data."

Text messaging is used widely in China, not only by ordinary people, but government officials. In 2012, Chinese users exchanged nearly 900 billion SMS messages. China Mobile is the world's largest mobile network carrier, with 735 million subscribers, followed by China Unicom's 258 million and China Telecom's 172 million.

Equally significant was Snowden's revelation of the NSA's hacking of the networks of Tsinghua University—one of the most prestigious educational institutes in China. In a single day in January alone, there were 63 intrusions. The university is home to one of China's six major backbone networks that manage the entire country's Internet traffic—the China Education and Research Network (CERNER). This means that the NSA could have mined the data of millions of users.

The NSA hacking into Pacnet also has immense implications. Pacnet is the hub for 46,000 kilometres of fiber-optic cables, connecting regional data centres across the Asia-Pacific, including China, Hong Kong, Taiwan, Japan, South Korea and Singapore.

Snowden's exposure of the extent of US cyber operations has raised concerns in the Chinese military and security establishment that the country is vulnerable not only to surveillance, but US cyberware aimed at disrupting or destroying Chinese infrastructure including electronic networks, phone systems and the power grid.

The Obama administration is already restructuring and boosting its military capacities in the region as part of its aggressive "pivot to Asia" aimed at containing China. The NSA revelations have made clear that the US is also building up its cyber warfare capacities along with military hardware and bases throughout the region.

The state-owned *Global Time s* interviewed five security experts last Friday. They agreed that "China's cyber security is already in grave danger" and called on Beijing to respond accordingly by establishing cyber warfare capabilities.

Qin An of the Cyber Space Strategic Institute warned that China faced threats "not only from the sea and air, but also the Internet." He stated: "Some Americans have already changed the 'Air/Sea Battle' for containing China to 'Air/Sea/Cyber Battle'. As a result, we must establish a comprehensive perspective of security and cyber defence."

"Air/Sea Battle" is a key military doctrine developed by the Pentagon, outlining preparations for a massive air and missile assault on Chinese military command and communications systems.

The debate within China's strategic circles underscores the fact that, Snowden's disclosures have intensified the tensions produced by the relentless US campaign to undermine China in every strategic arena.