Edward Snowden reveals US computer hacking aimed at China

John Chan
14 June 2013

Former US National Security Agency (NSA) contractor Edward Snowden revealed to Hong Kong's English-language newspaper, the *South China Morning Post*, on Wednesday that Washington has hacked into hundreds of civilian targets in Hong Kong and mainland China.

Snowden's revelations are a major blow to the claims made by the Obama administration that China is the greatest threat to global cyber security. This claim has been used to intensify US pressure on China and justify developing US cyber warfare capabilities to attack targets around the world.

For months, the Obama administration and US press outlets like *New York Times* have created a public scare—alleging, without any concrete evidence, that Chinese military cyber warfare units were hacking into US government, military and corporate networks. Obama himself has repeatedly raised the issue with Chinese President Xi Jinping, including at their first summit in California just last weekend.

Snowden has confirmed that the US National Security Agency (NSA) has been hacking computers in Hong Kong and mainland China at least since 2009.

According to documents shown to the *South China Morning Post*, the hundreds of targets of US hacking in Hong Kong include public officials, a university, businesses and students. They contain specific dates and IP addresses of computers in Hong Kong and mainland China hacked by the NSA in the past four years. They also include indications whether an attack was ongoing or had been completed, and other additional operational information. The documents reveal that the success rate of hacking against Hong Kong computers was more than 75 percent.

All attacks were aimed at civilian computers with no reference to Chinese military systems, Snowden said. He said it demonstrates "the hypocrisy of the US government when it claims that it does not target civilian infrastructure, unlike its adversaries."

Snowden explained he did not know what specific information they were looking for on these computers, "only that using technical exploits to gain unauthorised access to civilian machines is a violation of law."

Snowden said that the basic method of the NSA hackings is to attack network backbones, which are "like huge internet routers, basically, that give us access to the communications of hundreds of thousands of computers without having to hack every single one." One of the targets, the Chinese University of Hong Kong, fits into this category. It houses the Hong Kong Internet Exchange—a central hub of servers through which all web traffic in the city passes.

Snowden declared, "The primary issue of public importance to Hong Kong and mainland China should be that the NSA is illegally seizing the communications of tens of millions of individuals without any individualised suspicion of wrongdoing. They simply steal everything so they can search for any topics of interest."

Snowden's interviews expose the criminal policies of the United States government, which has always claimed to be the champion of defending "human rights" in China.

Washington's blatant and illegal hacking of computers in Chinese territory also lays bare the hypocrisy of Obama's "pivot to Asia"—aiming to contain China with a network of pro-US alliances. It is justified with claims that Washington is supposedly uniting with "democracies" such as Japan and Australia to militarily contain and encircle the "authoritarian" China. In fact, Washington is engaged in massive spying on targets in China, as well as in the United

States itself.

What Snowden revealed, as a low-ranking NSA employee, is only a small part of the cyber war the US is preparing as part of its general military preparations against China.

Even before Snowden's revelation of US cyber-attacks on China, Matthew Aid, a US intelligence expert, revealed in *Foreign Policy* on June 10 the existence of an NSA unit centrally involved in hacking Chinese computer and telecommunications networks during the past 15 years.

According to Aid, the highly secretive Maryland-based Office of Tailored Access Operations (TAO) has been "generating some of the best and most reliable intelligence information about what is going on inside the People's Republic of China."

Aid explained that given the large scale of TAO operations, it could no longer hide itself and is known to the Chinese government. This apparently became an issue during the US-China summit last weekend. Initially, Obama provocatively inserted the item of cyber security into the agenda at his meeting with Chinese President Xi—without even bothering to first inform Beijing.

China's top Internet official, Huang Chengqing, implicitly threatened to release "mountains of data" of US cyber hacking to steal Chinese government secrets.

Aid said that even though no one in the US media bothers to ask the White House whether the Chinese charges are true, "it turns out that the Chinese government's allegations are essentially correct."

"According to former NSA officials interviewed for this article," Aid wrote, TAO was now the largest and most important component of NSA's Signal Intelligence Directorate, with 1,000 military and civilian hackers, analysts and engineers.

Aid wrote that TAO's mission is to collect intelligence on foreign targets by cracking passwords, compromising computer security systems, stealing data stored on their hard drives, and then copying all messages and data traffic passing through targeted email and text-messaging. The technical term for this operation is known as CNE, or computer network exploitation.

TAO, Aid explained, "is also responsible for developing the information that would allow the United States to destroy or damage foreign computers and telecommunications systems with a cyber-attack if so directed by the president." This will be carried out by the US Cyber Command established by Obama.

The Chinese government has not directly commented on Snowden's case so far, but the official *China Daily* admitted that the case will "test developing Sino-US ties." At the recent summit, the two presidents agreed to put aside the row over cyber security for now, after Obama extracted concessions from Xi to put pressure on North Korea to return to talks over its nuclear programs.

But Snowden's flight to Hong Kong, which is indirectly under Chinese jurisdiction, has placed fresh pressure on Beijing. Not only is Xi seeking to improve relations with Washington, but there are fears that revelations of US cyber-hacking could trigger a broader backlash against China's own vast programs of online and physical spying on Chinese citizens.

There are now 700 million Internet users in China, largely among the youth. The Chinese government has been using its notorious "Great Firewall" to block them from any web sites with oppositional political ideas.

There has been support in China for Snowden as someone standing up to totalitarian power. CNN reported that China's Internet users "were typically supportive of the 29-year-old." An internet user "Xiaogong" hailed him "a real fighter for human rights. Now he is in China, we should protect him."

The *Wall Street Journal* also wrote that China's internet users welcomed him as a "hero." "This is the definition of heroism," one microblogger wrote. "Doing this proves he genuinely cares about his country and about his country's citizens. All countries need someone like him!"