US penetrated N. Korea computer systems in 2010: report

January 19 2015

The United States secretly penetrated North Korea's computer systems four years ago—a breach that allowed Washington to insist Pyongyang was to blame for the recent cyberattack on Sony Pictures, the *New York Times* reported Monday.

Citing former US officials and a newly released National Security Agency (NSA) document, the Times detailed how the US spy agency in 2010 "penetrated directly" into the North's systems via Chinese networks and connections in Malaysia favored by North Korean hackers.

Primarily aimed at gathering information on the reclusive nation's nuclear program, the NSA's clandestine operation switched focus to the growing threat posed by North Korea's hacking capabilities following a destructive cyberattack on South Korean banks in 2013.

Hidden US software provided an "early warning radar" for North Korean activities, and provided the evidence that persuaded President Barack Obama that Pyongyang was behind the Sony hack, the Times said, citing an anonymous official familiar with the NSA mission.

US investigators concluded that North Korean hackers spent two months mapping Sony's computer systems in preparation for what became the biggest cyberattack in US corporate history.

North Korea denies any involvement, although it had publicly threatened Sony if it released the comedy film "The Interview" about a CIA plot to

assassinate leader Kim Jong-Un.

Given that threat and the reported level of US penetration, the Times report raised the question of why the NSA was unable to warn Sony in advance.

According to one US official cited by the newspaper, the intelligence agencies "couldn't really understand the severity" of the attack that was coming.

While North Korea's conventional military hardware is largely outdated and unsophisticated, its cyberwarfare capabilities have long been considered a significant threat.

South Korean intelligence believes North Korea runs an elite cyberwarfare unit with at least 6,000 personnel, trained in secret government and military programs.

A number of experts suggest the North's cybercapacity is heavily reliant on China, in terms of both training and the necessary software and hardware.

They say telecommunications giant China Unicom provides and maintains all Internet links with the North, and some estimate that thousands of North Korean hackers operate on Chinese soil.

According to South Korea's National Intelligence Service, more than 75,000 hacking attempts were made against South Korean government agencies between 2010 and September 2014—many of them believed to be from Pyongyang.

The Times interviewed a former North Korean army programmer who said the North began training computer "warriors" in earnest in 1996,

despatching many to undergo two years' training in China and Russia.

© 2015 AFP