Who pulled the plug on North Korea's Internet?

23 December 2014, by Jo Biddle

Workers remove a poster-banner for "The Interview" from a billboard in Hollywood, California on December 18, 2014 a day after Sony announced it was cancelling the movie's Christmas release due to a terrorist threat

North Korea's Internet was on the fritz for a second day Tuesday. But the US is staying silent on whether it launched a cyber attack as payback for the hacking of Sony Pictures.

And in the murky world of cyber security, experts say there are several plausible scenarios for why North Korea suddenly went dark, stressing it's impossible to know exactly what happened.

Did the US launch a cyber attack on North Korea?

While some have been quick to make the link between Pyongyang's connectivity woes and a pledge by US President Barack Obama to retaliate for last month's Sony hack, many analysts aren't convinced.

"It's unlikely, if only because we can't make decisions that fast," said cyber expert James Lewis, a senior fellow with the Center for Strategic and International Studies (CSIS).

Washington has asked for help from Pyongyang's ally Beijing to rein the North's cyber activities, so "monkeying" around with Internet services linked to China would not make much sense, he told AFP.

It was also a pretty unsophisticated attack, if it was an attack, said Doug Madory, director of Internet Analysis with Dyn Research, the US monitoring company which broke the story of Pyongyang's Internet problems.

"We don't have direct evidence of some kind of cyber attack, but it would be consistent with that," he told AFP. Given the low-level of sophistication "the cast of characters that could have pulled this off is immense."

"If a nation state such as the US wanted to take North Korea off, I'm not sure it would have taken them 12 hours."

For its part, the Obama administration is dodging questions and refusing to publicly outline any measures it takes against Pyongyang.

So is China the main suspect?

It's certainly near the top of the list. North Korea only has connections to four Internet networks and they all run through China, operated by a single provider, China Unicom.

This undated file picture released from North Korea's official Korean Central News Agency on April 27, 2014 shows North Korean leader Kim Jong-Un (C) looking at a computer

"That's a fragile state of affairs," said Jim Cowie, chief scientist with Dyn Research.

China has been increasingly frustrated by the erratic behavior of North Korea's new young leader, Kim Jong-Un.

Simply pulling the plug on its Internet would send a strong signal of its displeasure, while at the same time shoring up ties with the United States which has indicted five Chinese military officers for hacking into US companies to steal trade secrets.

On the other hand, simply pulling a plug would not have caused the "hours and hours" of instability in the networks, which first alerted Dyn Research to the problem.

Could the outage be an internal North Korean issue?

CSIS analyst Lewis believes the top scenario is the North Koreans are either "inadvertently doing this, or more likely combing through their networks" to figure out how the US traced them to the Sony attack.

"The pattern of up-and-down connectivity, followed by a total outage, is consistent with a fragile network under external attack," said Cowie.

"But it's also consistent with more common causes, such as power problems," he argued, pointing to such things as breaks in fiberoptic cables.

What about hacktivist groups such as Anonymous?

"It's entirely possible that there is a joker out there," said Madory, adding that what appears to have happened was that the North Korean networks came under some kind of "duress", began struggling to stay up and then eventually just caved in.

The historic water tower at Sony Pictures Studios in Culver City, California is seen on December 16, 2014

Supporting this theory is the fact that North Korea has been targeted by Anonymous in the past.

Have nations carried out other cyber attacks against countries?

Yes. North Korea is believed to have carried out five cyber attacks on South Korea, according to Lewis.

The Stuxnet malware program, widely thought to have been developed by the US and Israel around 2009, was a computer worm reportedly designed to sabotage Iran's efforts to make a nuclear bomb.

At least seven countries are believed to have carried out cyber attacks: Britain, China, Israel, Iran, North Korea, Russia and the United States, Lewis said. About another dozen countries are reportedly trying to develop cyberattack capabilities.

Where does international law stand?

An international legal framework on cyber warfare is currently being negotiated through the UN First Committee, which deals with disarmament and threats to international peace.

"There's an agreement that international law applies, but there's recognition that there are gray areas," said Lewis. The use of force is prohibited for example, "but how about the erasure of data?"

Ironically, the Sony affair could help the negotiators by providing data to guide the discussions.

Madory argued, however, that if the United States is not involved it should come out and say so, and similarly China Unicom could share its data in a bid to solve the mystery.

APA citation: Who pulled the plug on North Korea's Internet? (2014, December 23) retrieved 23 June 2021 from https://phys.org/news/2014-12-north-korea-internet.html