SKorea misidentifies China as cyberattack origin

March 22 2013, by Sam Kim

A South Korean police officer from Digital Forensic Investigation walks inside the Cyber Terror Response Center at National Police Agency in Seoul, South Korea, Friday, March 22, 2013. South Korea said Friday it was preparing for the possibility of more cyberattacks as a new team of investigators tried to determine if North Korea was behind a synchronized shutdown of tens of thousands of computers at six South Korean banks and media companies.(AP Photo/Ahn Young-joon)

(AP)—In an embarrassing twist to a coordinated cyberattack on six

major South Korean companies this week, investigators said Friday they wrongly identified a Chinese Internet Protocol address as the source.

A joint team of government and private experts still maintains that hackers abroad were likely to blame, and many analysts suspect North Korea. But the error raises questions about investigators' ability to track down the source of an attack that shut down 32,000 computers Wednesday and exposed big Internet security holes in one of the world's most wired, tech-savvy countries.

South Korean investigators said Thursday that a malicious code that spread through the server of one of the hackers' targets, Nonghyup Bank, was traced to an IP address in China. Even then it was clear that the attack could have originated elsewhere because hackers can easily manipulate such data.

But the state-run Korea Communications Commission said Friday that the IP address actually belonged to a computer at the bank. The IP address was used only for the company's internal network and happened to be identical to a public Chinese address.

"We were careless in our efforts to double-check and triple-check," KCC official Lee Seung-won told reporters. He blamed the error on investigators' rush to give the public details on the search for a culprit.

Yonhap news agency, in an analysis Friday, called the blunder "ridiculous" and said the announcement is certain to undermine government credibility.

Yonhap criticized officials for failing to dispel public anxiety in a country where people's lives are closely interwoven with services provided by media and financial institutions.

A South Korean police officer from Digital Forensic Investigation comes out from the Cyber Terror Response Center at National Police Agency in Seoul, South Korea, Friday, March 22, 2013. South Korea said Friday it was preparing for the possibility of more cyberattacks as a new team of investigators tried to determine if North Korea was behind a synchronized shutdown of tens of thousands of computers at six South Korean banks and media companies.(AP Photo/Ahn Young-joon)

An initial assumption that the attack came from abroad may have made investigators jump to conclusions, said Lee Kyung-ho, a cybersecurity expert at Seoul's Korea University.

"They rushed," he said. "They should've investigated by checking the facts step by step."

The investigation will take weeks. Investigators have said the attacks

appeared to come from "a single organization" and suspect the hackers were from outside the country. Lee Seung-won, the KCC official, discounted the possibility that the attack could have come from within South Korea, but he didn't elaborate.

Lee Kyung-ho and many other South Korean experts suspect North Korea is behind the attack on broadcasters YTN, MBC and KBS, as well as Nonghyup and two other banks.

While there are many possible explanations, he said, including a homegrown hacker, the culprits are most likely to be North Koreans angry over ongoing U.S.-South Korean military drills. Lee said Pyongyang is well aware that an attack on financial institutions and media companies would create lots of publicity and turmoil in South Korea's vibrantly capitalistic society.

North Korea has issued many threats against the South and the U.S. in recent days, but by Friday it had yet to mention the South Korean computer crashes in state-run media.

South Korean officials say they have no proof of Pyongyang's involvement. The country is preparing to deal with more possible attacks, presidential spokesman Yoon Chang-jung told reporters earlier Friday. He didn't elaborate.

Determining who's behind a digital attack is often difficult, but North Korea is a leading suspect for several reasons.

It has unleashed a torrent of threats against Seoul and Washington since punishing U.N. sanctions were imposed for Pyongyang's Feb. 12 nuclear test. It calls ongoing routine U.S.-South Korean military drills a threat to its existence. Pyongyang also threatened revenge after blaming Seoul and Washington for a separate Internet shutdown that disrupted its own

network last week.

Seoul alleges six previous cyberattacks by North Korea on South Korean targets since 2009.

Wednesday's cyberattack did not affect South Korea's government, military or infrastructure, and there were no initial reports that customers' bank records were compromised. But it disabled cash machines and disrupted commerce.

All three of the banks that were hit were back online and operating regularly Friday. It could be next week before the broadcasters' systems have fully recovered, though they said their programming was never affected.