Experts suspect North behind SKorea computer crash (Update 2)

March 20 2013, by Hyung-Jin Kim

A customer stands in front of automated teller machines at a branch of Shinhan Bank after the bank's computer networks was paralyzed in Seoul, South Korea, Wednesday, March 20, 2013. Police and South Korean officials were investigating the simultaneous shutdown Wednesday of computer networks at several major broadcasters and banks. While the cause wasn't immediately clear, speculation centered on a possible North Korean cyberattack. (AP Photo/Ahn Young-joon)

A cyberattack caused computer networks at major South Korean banks

and top TV broadcasters to crash simultaneously Wednesday, paralyzing bank machines across the country and prompting speculation of North Korean involvement.

Screens went blank at 2 p.m. (0500 GMT), the state-run Korea Information Security Agency said, and more than seven hours later some systems were still down.

Police and South Korean officials couldn't immediately determine responsibility and North Korea's state media made no immediate comments on the shutdown. But some experts suspected a cyberattack orchestrated by Pyongyang. The rivals have exchanged threats amid joint U.S.-South Korean military drills and in the wake of U.N. sanctions meant to punish North Korea over its nuclear test last month.

The network paralysis took place just days after North Korea accused South Korea and the U.S. of staging a cyberattack that shut down its websites for two days last week. Loxley Pacific, the Thailand-based Internet service provider, confirmed the North Korean outage but did not say what caused it.

The South Korean shutdown did not affect government agencies or potential targets such as power plants or transportation systems, and there were no immediate reports that bank customers' records were compromised, but the disruption froze part of the country's commerce.

Some customers were unable to use the debit or credit cards that many rely on more than cash. At one Starbucks in downtown Seoul, customers were asked to pay for their coffee in cash, and lines formed outside disabled bank machines.

Shinhan Bank, a major South Korean lender, reported a two-hour system shutdown, including online banking and automated teller machines. It

said networks later came back online and that banking was back to normal. Shinhan said no customer records or accounts were compromised.

Another big bank, Nonghyup, said its system eventually came back online. Officials didn't answer a call seeking details on the safety of customer records. Jeju Bank said some of its branches also reported network shutdowns.

Broadcasters KBS and MBC said their computers went down at 2 p.m., but that the shutdown did not affect TV broadcasts. Computers were still down about seven hours after the shutdown began, according to the state-run Korea Communications Commission, South Korea's telecom regulator.

The YTN cable news channel also said the company's internal computer network was paralyzed. Footage showed workers staring at blank computer screens.

KBS employees said they watched helplessly as files stored on their computers began disappearing.

Last year, North Korea threatened to attack several news companies, including KBC and MBC, over their reports critical of children's' festivals in the North.

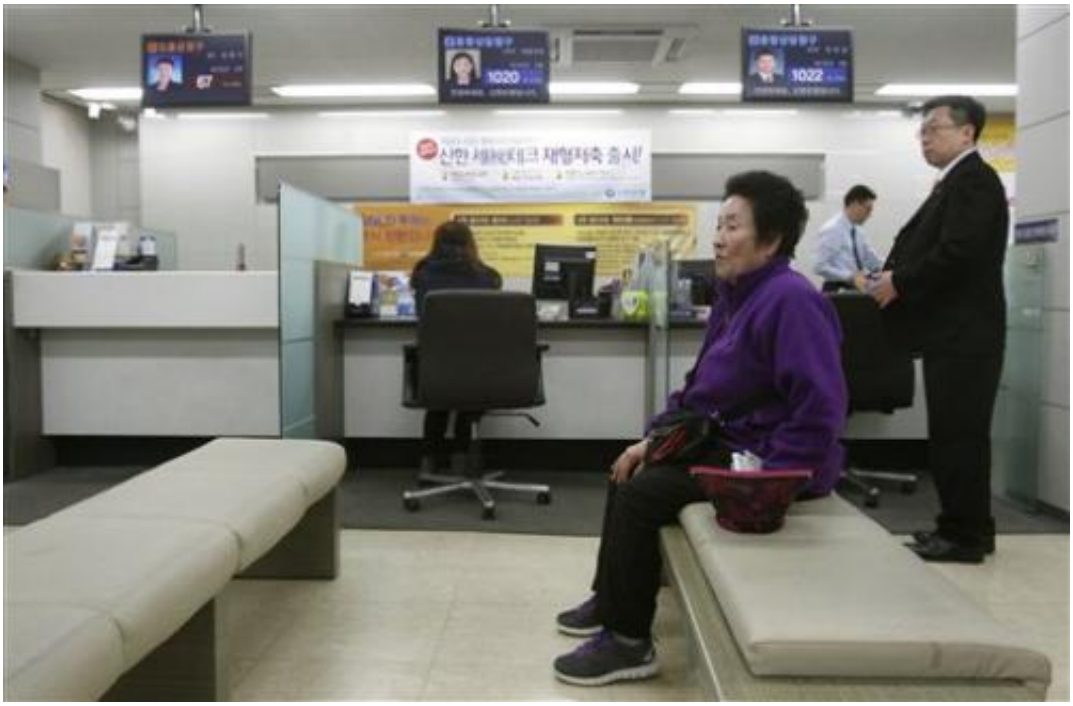
"It's got to be a hacking attack," said Lim Jong-in, dean of Korea University's Graduate School of Information Security. "Such simultaneous shutdowns cannot be caused by technical glitches."

The Korea Information Security Agency had reported that an image of skulls and a hacking claim had popped up on some of the computers that shut down, but later said those who reported the skulls did not work for

the five companies whose computers suffered massive outages. KISA was investigating the skull images as well.

"If it plays out that this was a state-sponsored attack, that's pretty bald faced and definitely an escalation in the tensions between the two countries," said James Barnett, former chief of public safety and homeland security for the U.S. Federal Communications Commission.

An ominous question is what other businesses, in South Korea or elsewhere, may also be in the sights of the attacker, said Barnett, who heads the cybersecurity practice at Washington law firm Venable.



A customer sits in a branch of Shinhan Bank in Seoul, South Korea, while the bank's computer networks are paralyzed Wednesday, March 20, 2013. Police and South Korean officials were investigating the simultaneous shutdown Wednesday of computer networks at several major broadcasters and banks. While the cause wasn't immediately clear, speculation centered on a possible North Korean cyberattack. (AP Photo/Ahn Young-joon)

"This needs to be a wake-up call," he said. "This can happen anywhere."

An official at the Korea Communications Commission said investigators speculate that malicious code was spread from company servers that send automatic updates of security software and virus patches.

LG Uplus Corp., which provides network services for the companies that suffered outages, saw no signs of a cyberattack on its networks, company spokesman Lee Jung-hwan said.

The South Korean military raised its cyberattack readiness level but saw no signs of cyberattacks on its networks, the Defense Ministry said.

No government computers were affected, officials said. President Park Geun-hye called for quick efforts to get systems back online, according to her spokeswoman, Kim Haing.

The shutdown raised worries about the overall vulnerability to attacks in South Korea, a world leader in broadband and mobile Internet access. Previous hacking attacks at private companies compromised millions of people's personal data. Past malware attacks also disabled access to government agency websites and destroyed files in personal computers.

Seoul believes North Korea runs an Internet warfare unit aimed at hacking U.S. and South Korean government and military networks to gather information and disrupt service.

Seoul blames North Korean hackers for several cyberattacks in recent years. Pyongyang has either denied or ignored those charges. Hackers operating from IP addresses in China have also been blamed.

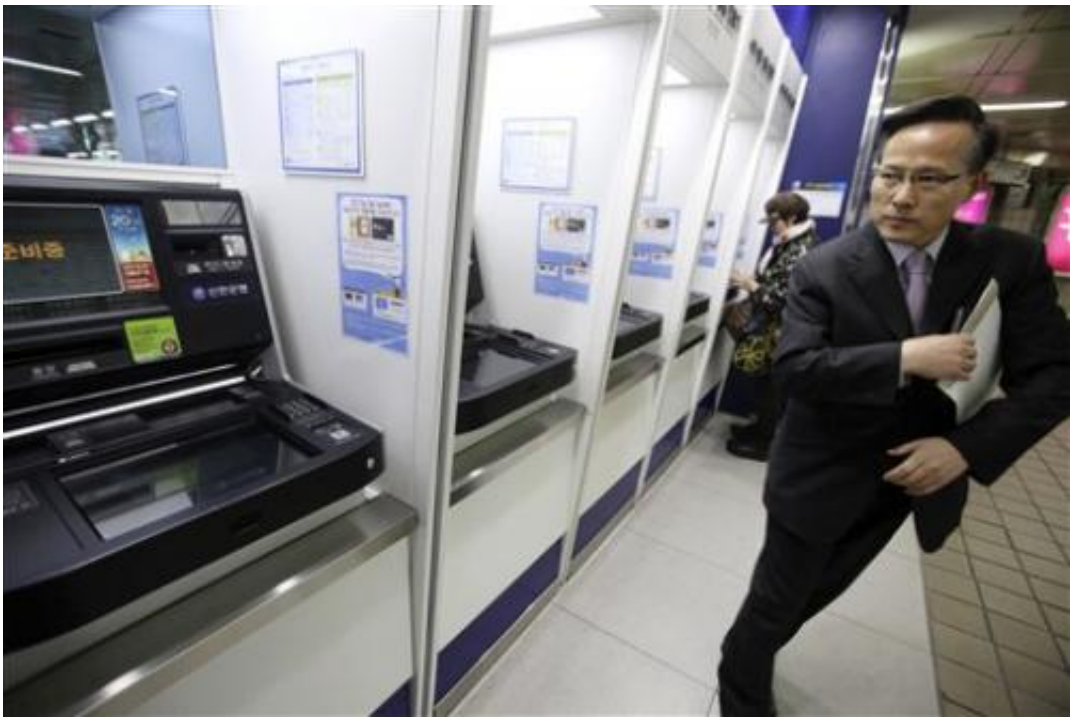
In 2011, computer security software maker McAfee Inc. said North Korea or its sympathizers likely were responsible for a cyberattack against South Korean government and banking websites earlier that year. The analysis also said North Korea appeared to be linked to a 2009 massive computer-based attack that brought down U.S. government Internet sites. Pyongyang denied involvement.

"North Korea has almost certainly done similar attacks before," said Tim Junio, a cybersecurity fellow at Stanford University's Center for International Security and Cooperation. "Part of why this wasn't more consequential is probably because South Korea took the first major incident seriously and deployed a bunch of organizational and technical innovations to reduce response time during future North Korea attacks."

South Korea has created a National Cybersecurity Center, a national monitoring sector and a Cyber Command modeled after the U.S. Cyber Command.

"These companies have security monitoring centers getting fed info from all over Korea to help detect incidents quickly and push technical solutions," he said. "They also have formal relationships with the government and sectors within their companies dedicated to national security work, including North Korean malware."

The shutdown comes amid rising rhetoric and threats of attack from Pyongyang over the U.N. sanctions. Washington also expanded sanctions against North Korea this month in a bid to cripple the government's ability to develop its nuclear program.



A depositor leaves after checking his account through an automated teller machine at a subway station as the bank's computer networks was paralyzed in Seoul, South Korea, Wednesday, March 20, 2013. Police and South Korean officials were investigating the simultaneous shutdown Wednesday of computer networks at several major broadcasters and banks. While the cause wasn't immediately clear, speculation centered on a possible North Korean cyberattack. (AP Photo/Ahn Young-joon)

North Korea has threatened revenge for the sanctions and for ongoing U.S.-South Korean military drills, which the allies describe as routine but which Pyongyang says are rehearsals for invasion.

On Wednesday, North Korean leader Kim Jong Un inspected military drills in which drone planes hit targets and rockets shot down mock enemy cruise missiles. Kim told officers the North should "destroy the enemies without mercy so that not a single man can survive to sign a document of surrender when a battle starts," according to the official

Korean Central News Agency.

Last week, North Korea's Committee for the Peaceful Reunification of Korea warned South Korea's "reptile media" that the North was prepared to conduct a "sophisticated strike" on Seoul.

North Korea also has claimed cyberattacks by the U.S. and South Korea. The North's official Korean Central News Agency accused the countries of expanding an aggressive stance against Pyongyang into cyberspace with "intensive and persistent virus attacks."

South Korea denied the allegation and the U.S. military declined to comment.

Lim said he believes hackers in China were likely culprits in the outage in Pyongyang, but that North Korea was probably responsible for Wednesday's attack.

"Hackers attack media companies usually because of a political desire to cause confusion in society," he said. "Political attacks on South Korea come from North Koreans."

Orchestrating the mass shutdown of the networks of major companies would have taken at least one to six months of planning and coordination, said Kwon Seok-chul, chief executive officer of Seoul-based cybersecurity firm Cuvepia Inc.

Kwon, who analyzed personal computers at one of the three broadcasters shut down Wednesday, said he hasn't yet seen signs that the malware was distributed by North Korea.

"But hackers left indications in computer files that mean this could be the first of many attacks," he said.

Lim said tracking the source of the outage would take months.