Digital dilemma: How will US respond to Sony hack?

December 18 2014, byEric Tucker And Tami Abdollah

In this July 27, 2013 file photo, North Korea's leader Kim Jong Un waves to spectators and participants of a mass military parade celebrating the 60th anniversary of the Korean War armistice in Pyongyang, North Korea. If the U.S. government's claim that North Korea was involved in the unprecedented hack attack on Sony Pictures that scuttled Seth Rogen's latest comedy is correct, no one can say they weren't warned. The movie, "The Interview," pushed all of North Korea's buttons. (AP Photo/Wong Maye-E, File)

The detective work blaming North Korea for the Sony hacker break-in

appears so far to be largely circumstantial, The Associated Press has learned. The dramatic conclusion of a Korean role is based on subtle clues in the hacking tools left behind and the involvement of at least one computer in Bolivia previously traced to other attacks blamed on the North Koreans.

Experts cautioned that hackers notoriously employ disinformation to throw investigators off their tracks, using borrowed tools, tampering with logs and inserting false references to language or nationality.

The hackers are believed to have been conducting surveillance on the network at Sony Pictures Entertainment Inc. since at least the spring, based on computer forensic evidence and traffic analysis, a person with knowledge of the investigation told the AP.

If the hackers hadn't made their presence known by making demands and destroying files, they probably would still be inside because there was no indication their presence was about to be detected, the person said. This person, who described the evidence as circumstantial, spoke only on condition of anonymity because he was not authorized to talk openly about the case.

Still, the evidence has been considered conclusive enough that a U.S. official told the AP that federal investigators have now connected the Sony hacking to North Korea.

In public, White House spokesman Josh Earnest on Thursday declined to blame North Korea, saying he didn't want to get ahead of investigations by the Justice Department and the FBI. Earnest said evidence shows the hacking was carried out by a "sophisticated actor" with "malicious intent."

All this has led to a dilemma for the Obama administration: How and

whether to respond?

An earlier formal statement by the White House National Security Council also did not name North Korea but noted that "criminals and foreign countries regularly seek to gain access to government and private sector networks" and said "we are considering a range of options in weighing a potential response. " The U.S. official who cited North Korea spoke on condition of anonymity because that official was not authorized to openly discuss an ongoing criminal case.

U.S. options against North Korea are limited. The U.S. already has a trade embargo in place, and there is no appetite for military action. Even if investigators could identify and prosecute the individual hackers believed responsible, there's no guarantee that any who are overseas would ever see a U.S. courtroom. Hacking back at North Korean targets by U.S. government experts could encourage further attacks against American targets.

"We don't sell them anything, we don't buy anything from them and we don't have diplomatic relations," said William Reinsch, a former senior U.S. Commerce Department official who was responsible for enforcing international sanctions against North Korea and other countries. "There aren't a lot of public options left."

This photo provided by Columbia Pictures - Sony shows, Randall Park, center, as North Korean leader Kim Jong Un in Columbia Pictures' "The Interview." North Korea has been linked to the unprecedented act of cyberwarfare against Sony Pictures that exposed tens of thousands of sensitive documents and escalated to threats of terrorist attacks that ultimately drove the studio to cancel all release plans for "The Interview." (AP Photo/Columbia Pictures - Sony, Ed Araquel)

Sony abruptly canceled the Dec. 25 release of its comedy, "The Interview," which the hackers had demanded partly because it included a scene depicting the assassination of North Korea's leader. Sony cited the hackers' threats of violence at movie theaters that planned to show the movie, although the Homeland Security Department said there was no credible intelligence of active plots. The hackers had been releasing onto the Internet huge amounts of highly sensitive—and sometimes embarrassing—confidential files they stole from inside Sony's computer network.

North Korea has publicly denied it was involved, though it has described the hack as a "righteous deed."

The episode is sure to cost Sony many millions of dollars, though the eventual damage is still anyone's guess. In addition to lost box-office revenue from the movie, the studio faces lawsuits by former employees angry over leaked Social Security numbers and other personal information. And there could be damage beyond the one company.

Sony's decision to pull the film has raised concerns that capitulating to criminals will encourage more hacking.

"By effectively yielding to aggressive acts of cyberterrorism by North Korea, that decision sets a troubling precedent that will only empower and embolden bad actors to use cyber as an offensive weapon even more aggressively in the future," said Sen. John McCain, R-Ariz., who will soon become chairman of the Senate Armed Services Committee. He said the Obama administration has failed to control the use of cyber weapons by foreign governments.

Homeland Security Secretary Jeh Johnson said on MSNBC that the administration was "actively considering a range of options that we'll take in response to this attack."

The hacking attack could prompt fresh calls for North Korea to be declared a state sponsor of terrorism, said Evans Revere, a former State Department official and Northeast Asia specialist. North Korea was put on that American list of rogue states in 1988 but taken off in 2008 as the U.S. was involved in multination negotiations with the North on its nuclear weapons program.

Evidence pinning specific crimes on specific hackers is nearly always imprecise, and the Sony case is no exception.

A poster for the movie "The Interview" is taken down by a worker after being pulled from a display case at a Carmike Cinemas movie theater, Wednesday, Dec. 17, 2014, in Atlanta. Georgia-based Carmike Cinemas has decided to cancel its planned showings of "The Interview" in the wake of threats against theatergoers by the Sony hackers. (AP Photo/David Goldman)

Sony hired FireEye Inc.'s Mandiant forensics unit, which last year published a landmark report with evidence accusing a Chinese Army organization, Unit 61398, of hacking into more than 140 companies over the years. In the current investigation, security professionals examined blueprints for the hacking tools discovered in Sony's network, the Korean language setting and time zone, and then traced other computers around the world used to help coordinate the break-in, according to the person with knowledge about the investigation.

Those computers were located in Singapore and Thailand, but a third in Bolivia had previously been traced to other attacks blamed on North

Korea, the person told the AP. The tools in the Sony case included components to break into the company's network and subsequently erase all fingerprints by rendering the hard drive useless.

"The Internet's a complicated place," said Adam Meyers, vice president of intelligence at CrowdStrike Inc., a security company that has investigated past attacks linked to North Korea. "We're talking about organizations that understand how to hide themselves, how to appear as if they're coming from other places. To that end, they know that people are going to come looking for them. They throw things in the way to limit what you can do attribution on."

Another agreed. "If you have a thousand bad pieces of circumstantial evidence, that doesn't mean your case is strong," said Jeffrey Carr, chief executive of Taia Global Inc., which provides threat intelligence to companies and government agencies.

In this Wednesday, Dec. 17, 2014 file photo, a banner for "The Interview" is posted outside Arclight Cinemas in the Hollywood section of Los Angeles. Sony Corp.'s miseries with its television and smartphone businesses were bad enough. Now its American movie division, a trophy asset, is facing tens of millions of dollars in losses from leaks by hackers that attacked the company over the movie that spoofs an assassination of North Korean leader Kim Jong Un. Sony Pictures canceled all release plans for the film at the heart of the attack. (AP Photo/Damian Dovarganes, File)

An FBI "flash" bulletin sent to some companies with details of the hacking software described it as "destructive malware, a disk wiper with network beacon capabilities." The FBI bulletin included instructions for companies to listen for telltale network traffic that would suggest they had been infected.

Other movie studios aren't taken chances. Warner Bros. executives earlier this week ordered a company-wide password reset and sent a five-point security checklist to employees advising them to purge their computers of any unnecessary data, in an email seen by The Associated Press.

"Keep only what you need for business purposes," the message said.