Sony saga blends foreign intrigue, star wattage

December 21 2014, byTami Abdollah And Eric Tucker

An exterior view of the Sony Pictures Studios building is seen in Culver City, Calif., Friday, Dec. 19, 2014. President Barack Obama declared Friday that Sony "made a mistake" in shelving the satirical film, "The Interview," about a plot to assassinate North Korea's leader. He pledged the U.S. would respond "in a place and manner and time that we choose" to the hacking attack on Sony that led to the withdrawal. The FBI blamed the hack on the communist government. (AP Photo/Damian Dovarganes)

The hackers who hit Sony Pictures Entertainment days before Thanksgiving crippled the network, stole gigabytes of data and spilled into public view unreleased films and reams of private and sometimes embarrassing executive emails.

One month later, the Obama administration confirmed what many had suspected: The North Korean government was behind the punishing breach. U.S. officials are promising a response, unspecified so far.

It was an extraordinarily public reaction from the highest levels of American government, considering that far more vital domestic interests have taken hits from foreign hackers in recent years—including the military, major banks and makers of nuclear and solar power whose trade secrets were siphoned off in a matter of mouse clicks.

Yet even in a digital era with an endless cycle of cyberattacks, none has drawn the public's attention like the Sony breach and its convergence of sensational plotlines:

—an isolated dictator half a world away.

—damaging Hollywood gossip from the executive suite.

—threats of terrorism against Christmas Day moviegoers.

—the American president chastising a corporate decision to shelve a satirical film.

—normally reticent law enforcement agencies laying bare their case against the suspected culprits.

"I can't remember the U.S. talking about a proportional response to Chinese espionage or infiltration of critical infrastructure for that

matter, as a policy issue in the same way that we're talking about this today," said Jacob Olcott, a cyberpolicy and legal issues expert at Good Harbor Security Risk Management and a former adviser to Congress.

The Sony Pictures Entertainment studio building is seen on Madison in Culver City, Calif., Friday, Dec. 19, 2014. President Barack Obama declared Friday that Sony "made a mistake" in shelving the satirical film, "The Interview," about a plot to assassinate North Korea's leader, and he pledged the U.S. would respond "in a place and manner and time that we choose" to the hacking attack on Sony that led to the withdrawal. The FBI blamed the hack on the communist government. (AP Photo/Damian Dovarganes)

President Barack Obama said Friday the U.S. would respond to the cyberattack, though he did not say how, after the FBI publicly blamed North Korea. He also criticized Sony's decision to cancel the release of

"The Interview," a comedy about a plot to assassinate North Korea's leader.

"This is uncharted territory," said Chris Finan, a former White House cybersecurity adviser. "The things we do in response to this event will indelibly serve to influence future nation state behavior."

North Korea has denied hacking the studio, and on Saturday proposed a joint investigation with the U.S., warning of "serious" consequences if Washington said no. The White House sidestepped the idea, said it was confident that North Korea was responsible and urged North Korean government officials to "admit their culpability and compensate Sony for the damages this attack caused."

At the same time, the U.S. was reaching out to China, North Korea's key ally, to ask for its cooperation as the U.S. weighs its response, said a senior Obama administration official, who wasn't authorized to comment by name and requested anonymity. Although China holds considerable leverage over the North and its technological infrastructure, involving Beijing could pose complications because Obama has pointedly accused China of engaging in its own acts of cybertheft.

Friday's announcement was a critical moment in an investigation that united the government and cybersecurity professionals who conducted painstaking technical analysis.

The breach was discovered days before Thanksgiving when Sony employees logged onto their computers to find a screen message saying they had been hacked by a group calling itself Guardians of Peace. Experts scoured months of system logs, determining through spikes in network traffic and other anomalies that the attackers had conducted surveillance on the network since spring.

The first goal was to determine the extent of the damage to the network, so crippled that investigators or any other visitors needed handwritten credentials to gain entry.

As they examined the malware, they detected that it was similar to DarkSeoul, used in attacks on South Korea banking and media institutions and connected to North Koreans.

Investigators determined the Internet protocol addresses used, and found that one in Bolivia was the same as one in the DarkSeoul hack. They also found time zone and language settings in Korean, and that the malware itself had source code believed to be held by North Korea.

The FBI statement said clues included similarities to other tools developed by North Korea in specific lines of computer code, encryption algorithms and data deletion methods. More significantly, the FBI discovered that computer Internet addresses known to be operated by North Korea were communicating directly with other computers used to deploy and control the hacking tools and collect the stolen Sony files.

That analysis, along with a North Korean official's declaration that "The Interview" was an "act of war," served to bolster the case for a North Korean motive.

In general, it's exceedingly difficult to pin down responsibility for a cyberattack because hackers typically try to throw investigators off their trail. North Korea's Internet infrastructure is air-gapped, or not directly connected to the outside world, except by proxies through other countries, so it's even more difficult to attribute the hack.

Even when investigators do zero in on suspected culprits, there's often a political calculation about when and whether to publicly name them. The Justice Department took the unusual step in May of announcing

indictments against five Chinese military officials accused of cyberespionage, but in many other instances, the public never learns the nationalities of the hackers, much less their identities.

In Sony's case, the FBI had been cautious about assigning blame to North Korea despite the evidence. Just a week before the public announcement, FBI Director James Comey had told reporters, "Before we attribute a particular action to a particular actor, we like to sort the evidence in a very careful way to arrive at a level of confidence that we think justifies saying 'Joe did it' or 'Sally did it,' and we're not at that point yet."

Beyond the FBI's announcement Friday, there were no details on remedies for Sony, no statement holding North Korea responsible for the already-known criminal acts of leaking copyright material, and no demand that North Korea return the stolen data.

"It seems highly unusual for the U.S. government to make an announcement like the FBI made today without a corresponding plan of action, which is exactly what was missing from the statements," Olcott said. "It was a press release to encourage more companies to work with the FBI in the future, but we actually don't really know why."