From: (b)(6)
To: Vanee M Vines; ""NSAPAO@NSA.GOV" (NSAPAO@NSA.GOV)"
Subject: NY Times piece on Sony
Date: Tuesday, January 20, 2015 2:39:54 PM
Attachments: image001.jpg

Vanee,
Justin Fishel has left the Pentagon and moved to ABC. He hit up RADM Kirby and COL Warren on the NY Times piece. Did he reach out to NSA? Are you commenting on the story?

Thanks,
r/ (b)(6)

From: Justin Fishel [mailto:justin.fishel@gmail.com]
Sent: Monday, January 19, 2015 02:47 AM Coordinated Universal Time
To: Kirby, John F RADM USN OSD PA (US); Warren, Steven H COL USARMY OSD PA (US)
Subject: You guys got anything on this?

N.S.A. Tapped Into North Korean Networks Before Sony Attack, Officials Say

http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?smid=tw-bna

WASHINGTON — The trail that led American officials to blame North Korea <http://topics.nytimes.com/top/news/international/countriesandterritories/northkorea/index.html?inline=nyt-geo> for the destructive cyberattack on Sony Pictures Entertainment in November winds back to 2010, when the National Security Agency <http://topics.nytimes.com/top/reference/timestopics/organizations/n/national_security_agency/index.html?inline=nyt-org> scrambled to break into the computer systems of a country considered one of the most impenetrable targets on earth.

Spurred by growing concern about North Korea's maturing capabilities, the American spy agency drilled into the Chinese networks that connect North Korea to the outside world, picked through connections in Malaysia favored by North Korean hackers and penetrated directly into the North with the help of South Korea and other American allies, according to former United States and foreign officials, computer experts later briefed on the operations and a newly disclosed N.S.A. document <http://www.spiegel.de/media/media-35679.pdf> .

A classified security agency program expanded into an ambitious effort, officials said, to place malware that could track the internal workings of many of the computers and networks used by the North's hackers, a force that South Korea's military recently said numbers roughly 6,000 people. Most are commanded by the country's main intelligence service, called the Reconnaissance General Bureau, and Bureau 121, its secretive hacking unit, with a large outpost in China.

The evidence gathered by the "early warning radar" of software painstakingly hidden to monitor North Korea's activities proved critical in persuading President Obama <http://topics.nytimes.com/top/reference/timestopics/people/o/barack_obama/index.html?inline=nyt-per> to accuse

the government of Kim Jong-un <http://topics.nytimes.com/top/reference/timestopics/people/k/kim_jongun/index.html?inline=nyt-per> of ordering the Sony attack, according to the officials and experts, who spoke on the condition of anonymity about the classified N.S.A. operation.

Mr. Obama's decision to accuse North Korea of ordering the largest destructive attack against an American target — and to promise retaliation, which has begun in the form of new economic sanctions — was highly unusual: The United States had never explicitly charged another government with mounting a cyberattack on American targets.

Mr. Obama is cautious in drawing stark conclusions from intelligence, aides say. But in this case "he had no doubt," according to one senior American military official.

"Attributing where attacks come from is incredibly difficult and slow," said James A. Lewis, a cyberwarfare <http://topics.nytimes.com/top/reference/timestopics/subjects/c/cyberwarfare/index.html?inline=nyt-classifier> expert at the Center for Strategic and International Studies in Washington. "The speed and certainty with which the United States made its determinations about North Korea told you that something was different here — that they had some kind of inside view."

For about a decade, the United States has implanted "beacons," which can map a computer network, along with surveillance software and occasionally even destructive malware in the computer systems of foreign adversaries. The government spends billions of dollars on the technology, which was crucial to the American and Israeli attacks on Iran's nuclear program <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all> , and documents previously disclosed by Edward J. Snowden, the former security agency contractor, demonstrated how widely they have been deployed against China <http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0> .

But fearing the exposure of its methods in a country that remains a black hole for intelligence gathering, American officials have declined to talk publicly about the role the technology played in Washington's assessment that the North Korean government had ordered the attack on Sony.

The extensive American penetration of the North Korean system also raises questions about why the United States was not able to alert Sony as the attacks took shape last fall, even though the North had warned, as early as June, that the release of the movie "The Interview," a crude comedy about a C.I.A. plot to assassinate the North's leader, would be "an act of war."

Dinner in Pyongyang

The N.S.A.'s success in getting into North Korea's systems in recent years should have allowed the agency to see the first "spear phishing" attacks on Sony — the use of emails that put malicious code into a computer system if an unknowing user clicks on a link — when the attacks began in early September, according to two American officials.

But those attacks did not look unusual. Only in retrospect did investigators determine that the North had stolen the "credentials" of a Sony systems administrator, which allowed the hackers to roam freely inside Sony's systems.

In recent weeks, investigators have concluded that the hackers spent more than two months, from mid-September to mid-November, mapping Sony's computer systems, identifying critical files and planning how to destroy computers and servers.

"They were incredibly careful, and patient," said one person briefed on the investigation. But he added that even with their view into the North's activities, American intelligence agencies "couldn't really understand the severity" of the destruction that was coming when the attacks began Nov. 24. <x-apple-data-detectors://1>

In fact, when, Gen. James R. Clapper Jr. <http://topics.nytimes.com/top/reference/timestopics/people/c/james_r_clapper_jr/index.html?inline=nyt-per> , the director of national intelligence, had an impromptu dinner in early November with his North Korean counterpart during a secret mission to Pyongyang <http://www.nytimes.com/2014/11/09/world/kenneth-bae-matthew-todd-miller-released-by-north-korea.html> to secure the release of two imprisoned Americans, he made no mention of

Sony or the North's growing hacking campaigns, officials say.

In a recent speech at Fordham University in New York, Mr. Clapper acknowledged that the commander of the Reconnaissance General Bureau, Kim Yong-chol, with whom he traded barbs over the 12-course dinner, was "later responsible for overseeing the attack against Sony." (General Clapper praised the food; his hosts later presented him with a bill for his share of the meal.)

Asked about General Clapper's knowledge of the Sony attacks from the North when he attended the dinner, Brian P. Hale, a spokesman for the director of national intelligence, said that the director did not know he would meet his intelligence counterpart and that the purpose of his trip to North Korea "was solely to secure the release of the two detained U.S. citizens."

"Because of the sensitivities surrounding the effort" to win the Americans' release, Mr. Hale said, "the D.N.I. was focused on the task and did not want to derail any progress by discussing other matters." But he said General Clapper was acutely aware of the North's growing capabilities.

Jang Sae-yul, a former North Korean army programmer who defected in 2007, speaking in an interview in Seoul, said: "They have built up formidable hacking skills. They have spent almost 30 years getting ready, learning how to do this and this alone, how to target specific countries."

Still, the sophistication of the Sony hack was such that many experts say they are skeptical that North Korea was the culprit, or the lone culprit. They have suggested it was an insider, a disgruntled Sony ex-employee or an outside group cleverly mimicking North Korean hackers. Many remain unconvinced by the efforts of the F.B.I. director, James B. Comey, to answer critics by disclosing some of the American evidence.

Mr. Comey told the same Fordham conference that the North Koreans got "sloppy" in hiding their tracks, and that hackers periodically "connected directly and we could see them."

"And we could see that the I.P. addresses that were being used to post and to send the emails were coming from I.P.s that were exclusively used by the North Koreans," he said. Some of those addresses appear to be in China, experts say.

The skeptics say, however, that it would not be that difficult for hackers who wanted to appear to be North Korean to fake their whereabouts. Mr. Comey said there was other evidence he could not discuss. So did Adm. Michael S. Rogers, the N.S.A. director, who told the Fordham conference that after reviewing the classified data he had "high confidence" the North had ordered the action.

A Growing Capability

North Korea built its first computer with vacuum tubes in 1965, with engineers trained in France. For a brief time, it appeared ahead of South Korea and of China, which not only caught up but also came to build major elements of their economic success on their hardware and software.

Defectors say that the Internet was first viewed by North Korea's leadership as a threat, something that could taint its citizens with outside ideas.

But Kim Heung-kwang, a defector who said in an interview that he helped train many of the North's first cyberspies, recalled that in the early 1990s a group of North Korean computer experts came back from China with a "very strange new idea": Use the Internet to steal secrets and attack the government's enemies. "The Chinese are already doing it," he quoted one of the experts as saying.

Defectors report that the North Korean military was interested. So was the ruling Workers' Party, which in 1994 sent 15 North Koreans to a military academy in Beijing to learn about hacking. When they returned, they formed the core of the External Information Intelligence Office, which hacked into websites, penetrated fire walls and stole information abroad. Because the North had so few connections to the outside world, the hackers did much of their work in China and Japan.

According to Mr. Kim, the military began training computer "warriors" in earnest in 1996 and two years later opened Bureau 121, now the primary cyberattack unit. Members were dispatched for two years of training in China and Russia. Mr. Jang said they were envied, in part because of their freedom to travel.

"They used to come back with exotic foreign clothes and expensive electronics like rice cookers and cameras," he said. His friends told him that Bureau 121 was divided into different groups, each targeting a specific country or region, especially the United States, South Korea and the North's one ally, China.

"They spend those two years not attacking, but just learning about their target country's Internet," said Mr. Jang, 46, who was a first lieutenant in a different army unit that wrote software for war game simulations.

Mr. Jang said that as time went on, the North began diverting high school students with the best math skills into a handful of top universities, including a military school specializing in computer-based warfare called Mirim University, which he attended as a young army officer.

Others were deployed to an "attack base" in the northeastern Chinese city of Shenyang, where there are many North Korean-run hotels and restaurants. Unlike the North's nuclear and ballistic missile programs, the cyberforces can be used to harass South Korea and the United States without risking a devastating response.

"Cyberwarfare is simply the modern chapter in North Korea's long history of asymmetrical warfare," said a security research report in August by Hewlett-Packard.

An Attack in Seoul

When the Americans first gained access to the North Korean networks and computers in 2010, their surveillance focused on the North's nuclear program <http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html?inline=nyt-classifier> and its leadership, as well as efforts to detect attacks aimed at United States military forces in South Korea, said one former American official. (The German magazine Der Spiegel published an N.S.A. document on Saturday that provides some details of South Korea's help in spying on the North.) Then a highly destructive attack in 2013 on South Korean banks and media companies suggested that North Korea was becoming a greater threat, and the focus shifted.

"The big target was the hackers," the official said.

That attack knocked out almost 50,000 computers and servers in South Korea for several days at five banks and television broadcasters.

The hackers were patient, spending nine months probing the South Korean systems. But they also made the mistake seen in the Sony hack, at one point revealing what South Korean analysts believe to have been their true I.P. addresses. Lim Jong-in, dean of the Graduate School of Information Security at Korea University, said those addresses were traced back to Shenyang, and fell within a spectrum of I.P. addresses linked to North Korean companies.

The attack was studied by American intelligence agencies. But after the North issued its warnings about Sony's movie last June, American officials appear to have made no reference to the risk in their discussions with Sony executives. Even when the spear-phishing attacks began in September — against Sony and other targets — "it didn't set off alarm bells," according to one person involved in the investigation.

The result is that American officials began to focus on North Korea only after the destructive attacks began in November, when pictures of skulls and gruesome images of Sony executives appeared on the screens of company employees. (That propaganda move by the hackers may have worked to Sony's benefit: Some employees unplugged their computers immediately, saving some data from destruction.)

It did not take long for American officials to conclude that the source of the attack was North Korea, officials say. "Figuring out how to respond was a lot harder," one White House official said.

cid:5C705FC7-55AD-488A-9CBC-16AF67015EA0

Joshua Hoyos

Assignment Editor | ABC News

47 West 66th Street, 5th Floor, New York, NY <x-apple-data-detectors://0/1>

w: 212.456.2700 | m: 917.728.2634 | @JoshuaHoyos

Sent from my iPhone