# A look at North Korea's cyberwar capabilities

December 18 2014, byYoukyung Lee


In this July 16, 2013 file photo, a woman walks by a sign at Cyber Terror Response Center of National Police Agency in Seoul, South Korea. Most North Koreans have never even seen the Internet. But the country Washington suspects is behind a devastating hack on Sony Pictures Entertainment has managed to orchestrate a string of crippling cyber infiltrations of South Korean computer systems in recent years, officials in Seoul believe, despite North Korea protesting innocence. (AP Photo/Ahn Young-joon, File)

Most North Koreans have never seen the Internet.

But the country Washington suspects is behind a devastating hack on Sony Pictures Entertainment has managed to orchestrate a string of crippling cyber infiltrations of South Korean computer systems in recent years, officials in Seoul believe, despite North Korea protesting innocence.

Experts say the Sony Pictures hack may be the costliest cyberattack ever inflicted on an American business. The fallout from the hack that exposed a trove of sensitive documents, and this week escalated to threats of terrorism, forced Sony to cancel release of the North Korean spoof movie "The Interview." The studio's reputation is in tatters as embarrassing revelations spill from tens of thousands of leaked emails and other company materials.

Despite widespread poverty, malnutrition and decades of crippling U.S.-led economic sanctions, Pyongyang has poured resources into training thousands of hackers who regularly target bitter rival Seoul.

A look at the country's suspected capabilities and where experts believe the authoritarian nation is heading with its cyber program:

—NORTH KOREA'S CYBERARMY

South Korea's former spy chief and a North Korean defector put the number of professional hackers at between 1,000 and 3,000. These numbers from Seoul's intelligence agency in 2010 and a leaked North Korean government document from 2009, which contained an order from late leader Kim Jong Il, may be outdated. But they agree that North Korea trains hackers at top schools to launch attacks on cyberspace mostly targeted at South Korea.

Defector Kim Heung Kwang said he trained student hackers at a university in the industrial North Korean city of Hamhung for two

decades before defecting in 2003. Hackers also are sent to study abroad in China and Russia.

In 2009, then-leader Kim Jong Il ordered Pyongyang's "cyber command" expanded to 3,000 hackers, Kim said, citing a North Korean government document that he obtained that year. The veracity of the document could not be independently confirmed.

Kim, who has lived in Seoul since 2004, believes that more have been recruited since then, and said some are based in China to infiltrate networks abroad.

Simon Choi, a senior security researcher at Seoul-based anti-virus company Hauri Inc., said North Korean hackers have honed their skills from various attacks in South Korea. Choi, who analyzes malicious codes from North Korea, said the country's skills have improved and it is able to disguise malware as harmless computer code.

The perception of growing cyber security threats from North Korea has prompted South Korea's defense ministry to beef up its cyber warfare capabilities.

In this May 5, 2012 file photo, South Korean cyber activists listen to North Korean defector Lee Mi-yeon, back to camera, during her lecture on national cyber security at Ministry of Patriots and Veterans Affairs in Suwon, South Korea. Most North Koreans have never even seen the Internet. But the country Washington suspects is behind a devastating hack on Sony Pictures Entertainment has managed to orchestrate a string of crippling cyber infiltrations of South Korean computer systems in recent years, officials in Seoul believe, despite North Korea protesting innocence. (AP Photo/Ahn Young-joon, File)

## —PAST CYBERATTACKS

South Korea blames North Korea for carrying out at least six high-profile cyberattacks since 2007 with many more unsuccessful attempts at infiltrating computer systems of businesses and government agencies. In the six cases, hackers destroyed hard drive disks, paralyzed banking systems or disrupted access to websites. Some of these attacks were so crippling that in one case a South Korean bank was unable to resume

online banking services for more than two weeks.

The first suspected cyberassault by North Korea took place on July 7, 2009 in the form of "denial of service" attacks on dozens of websites of South Korean and U.S. government agencies. Hackers triggered intense traffic from tens of thousands of "zombie" PCs that are crippled by malware. Initially, South Korea's spy agency pointed the finger at North Korea. Some experts later said that there were no conclusive evidence that Pyongyang was behind it, but South Korea came to see the attack as a prelude to a growing cyber threat from the North.

A similar infiltration was carried out on March 4, 2011. Hackers attacked about 40 South Korean government and private websites, prompting officials to warn of a substantial threat to the country's computers. The targets included websites belonging to South Korea's presidential office, the foreign ministry, the national intelligence service, US Forces Korea and major financial institutions.

One month later, South Korean bank Nonghyup was the victim of a damaging cyberattack on the country's financial industry. It took the bank more than two weeks to recover and resume online banking and ATM services. South Korean authorities concluded that North Korea was responsible for the April 12, 2011 attack.

A smaller scale breach linked to North Korea was on South Korean daily newspaper JoongAng Ilbo on June 6, 2012. Hackers changed the home page of its website and destroyed data in its editorial system.

One of the most damaging attacks took place in 2013. The March 20 cyberattack struck 48,000 computers and servers, hampering banks for 2-5 days. Officials said that no bank records or personal data were compromised but staffers at three TV broadcasters were unable to log on to news systems for several days, although programming continued.

Three months later on the anniversary of the outbreak of the Korean War, dozens of government and media companies were hit by malicious code and denial of service attacks.

—WHAT NEXT FOR NORTH KOREA'S CYBERWAR

Experts believe that for impoverished North Korea, expanding its warfare into cyberspace is an attractive choice because it is cheaper and faster to develop malicious computer codes than to build nuclear bombs or other weapons of mass destruction. Online attacks can be performed anonymously, another upside for the infiltrators.

It is also a battle in which North Korea has little to lose. Unlike South Korea where commerce and many aspects of daily life are dependent on the Internet, only a fraction of North Koreans can go online. In South Korea, a crippled website or a disruption of online banking poses great inconvenience.

"North Korea has very few Internet-connected PCs so they have little in the way of being attacked. But South Korea has a huge IT infrastructure that can come under attack," said Choi, the security expert. That provides ample targets for North Korean hackers, he said.

Choi believes the North's hackers are highly skilled and organized with the capacity to "freely hack into other computer systems without any limits."

Experts have warned of the possibility that North Korea could mobilize its hackers to attack key infrastructure such as power plants.

—CAVEATS

What the world knows about North Korea's cyberwarfare capabilities

comes mostly from intelligence agencies and North Korean defectors who left the country before 2007 when the first major cyberattack linked to North Korea occurred in South Korea.

North Korea's nuclear capabilities have been a point of pride for the isolated nation, but it has never openly admitted the existence of a state-trained cyberarmy.

The North has denied Seoul's accusations it is responsible for cyberattacks in South Korea. In the Sony Pictures case, North Korea said it might have been the work of sympathizers.