Further revelations in South Korean hacking scandal

Ben McGrath
25 July 2015

The scandal in South Korea surrounding the National Intelligence Service (NIS) has deepened as additional details have emerged over the agency's use of various eavesdropping technologies. The issues were compounded last weekend following the apparent suicide of an NIS agent involved with operating the hacking programs.

Every revelation points to the pursuit of police-state capacities by the NIS, which was first established as the Korean Central Intelligence Agency (KCIA) in 1961, under the military dictatorship headed by President Park Geun-hye's father, Park Chung-hee.

Last week, NIS chief Lee Byeong-ho downplayed the agency's purchase of the Remote Control System (RCS) from Hacking Team—an Italian company—in 2012, the same year as South Korea's general and presidential elections. Lee claimed that RCS was only used for studying the technology so that it could be used against North Korea, and not to spy on South Korean residents or interfere in the elections.

The NIS purchased ten RCS lines in January and ten more temporary lines in July 2012. However, email records between Hacking Team and Nanatech, the company that acted as an intermediary for the NIS, showed that the intelligence agency purchased 35 additional lines on December 6 that year, shortly before the presidential election on December 19.

Each line corresponded to the number of smart phones, computers or other devices the NIS could hack into and monitor, meaning the NIS could eavesdrop on dozens of people simultaneously. The lines could also be shifted to new targets after the monitoring of others was completed. To infect a device, the user must access a particular URL that has been compromised with a malware code.

Other emails from Hacking Team revealed that the NIS conducted a trial run of the Tactical Network Injection (TNI) program in April 2014, prior to the June regional elections, although the NIS did not purchase it in the end. The TNI system is able to infect a broader range of devices.

Given the intelligence agency's propensity for obtaining spyware prior to elections, the official story that the NIS did not use the programs to interfere in the contests has been called into question. The fact that the NIS also launched an Internet smear campaign against candidates running against President Park Geun-hye in 2012 has only heightened those suspicions.

The scandal took another turn when an NIS agent, identified only by his surname Im (also spelled Lim), was found dead in his car in the city of Yongin, just south of Seoul on July 18. The cause of death was reportedly suicide from a charcoal briquette, which releases carbon monoxide when burned. Im was in charge of operating the spyware.

Im supposedly left behind a suicide note in which he stated that the NIS never engaged in any spying on the South Korean public. "There was no surveillance on citizens or election affairs," it reputedly said.

However, Im also erased computer files on the hacking programs. Im reportedly wrote in his note: "Deciding that the prestige of the NIS was more important than the impact on the outside, I deleted material that could cause misunderstandings about operations against terrorists and against North Korea. This was a mistake caused by my faulty judgment."

Im's death raised numerous questions, not least of all why he ended his life if he and the NIS were not engaged in spying on the South Korean public. Questions are also being asked about what the deleted files contained. The NIS claims that the files are recoverable and that they will be made available to

members of the National Assembly Intelligence Committee.

None of this can be taken at face value. According to Nanatech CEO Heo Son-gu, in an interview with the *Hankyoreh* newspaper on Tuesday, the NIS targeted at least one "South Korean living in China," although Heo did not give further details.

Information leaked from Hacking Team also showed that the NIS attempted last month to spread the RCS malware through the URLs of popular restaurants, a cherry blossom tourism page and English-language sites about MERS (Middle East Respiratory Syndrome), among others.

The official opposition New Politics Alliance for Democracy (NPAD) has called into question NIS claims that all the files can or will be recovered. Representative Sin Gyeong-min, a member of the Intelligence Committee, stated: "We just don't understand the deletion of the files. Then, how can we understand the complete restoration?"

The NPAD has launched its own so-called inquiry into the affair and proposed a parliamentary investigation, which the ruling Saenuri Party has opposed. The opposition party also accused President Park Geun-hye of concealing the revelations. "Now is the time for the president to either cover up the scandal or clear the allegations," NPAD assembly floor leader Lee Jong-geol said.

However, the spying and eavesdropping are not the result of a few bad apples in the government or the NIS itself. The NPAD hopes to channel public opposition to the NIS into support for the party, but the NPAD essentially operated no differently from the conservatives when in power.

During the administrations of so-called progressives Kim Dae-jung and No Moo-hyun, the NIS was also utilized to spy on South Korean residents. During a 2005 investigation, Kim's use of the spy agency to illegally monitor political opponents was made public. No, who was president at the time, used the investigation to dispel fears of government spying. However, "legal" wiretaps by the NIS increased during No's administration. Between 2005 and 2006 for example, the number of phones being traced officially rose from 8,082 to 8,440, while wiretaps by the police and military investigators supposedly fell.

The South Korean ruling class increasingly views the entire population with suspicion and apprehension. The role of the NIS, since its inception in 1961 as the KCIA, has been to enable the ruling elites to maintain their grip on power. Regardless of whatever investigation takes place, both establishment parties will be intent on ensuring that the agency's operations are intensified, not hindered in any way.