South Korea’s intelligence agency purchased spyware from Hacking Team

Ben McGrath
16 July 2015

In revelations last week, South Korea was one of the countries listed as having bought spyware from the Italian company known as Hacking Team. With its history of military dictatorship, this is another clear sign that Seoul is once again erecting a police state.

Hacking Team’s files, which were leaked online July 5 and then posted by WikiLeaks, detailed the company’s sales and other communications. They showed that South Korea’s 5163 Army Division had purchased spyware known as the Remote Control System (RCS) in January 2012 and continued to deal with the company until this January. Hacking Team touted the RCS as a means for infecting smart phones and computers unbeknownst to the users and monitoring everything from phone calls to messaging apps.

The 5163 Army Division was reportedly acting as one of the fronts used by South Korea’s powerful National Intelligence Service (NIS) to hide its activities abroad.

The NIS quickly came under suspicion of using the eavesdropping technology, prompting an admission that the agency had in fact purchased the program. “It is true that the NIS bought the spyware, but it was for analyzing its technology and establishing strategy against North Korea,” a NIS official told *Hankyoreh* on July 12.

On Tuesday, NIS chief Lee Byeong-ho admitted that the agency had not only bought spyware from Hacking Team in January 2012, but also in July of the same year. He again claimed that the purchase was made to study the technology so that it could be directed against North Korea. The NIS claims that it never used the programs to spy on South Korea’s residents. “Spying on people can never occur. If the NIS ever did, I will accept any punishment,” said Lee.

South Korea regularly claims its anti-democratic measures are directed against North Korea, but leaked communications with Hacking Team reveal a different story. A Hacking Team e-mail from 24 March 2014 stated, “[The South Korean army] also asked about the progress of Kakao Talk, which they mentioned is very commonly used in their country.” This was a request for spyware that could hack into the Kakao Talk messaging service, an app widely used by people of all ages in South Korea. It is a clear indication that the NIS is targeting the South Korean population itself.

Other e-mails from Hacking Team provided by WikiLeaks revealed that the NIS first expressed interest in purchasing spyware in 2010 through a small company in Seoul known as Nanatech, and showed particular interest in spying on cell phone conversations. “Our customer wants to know that whether the solution [spyware] got the function of monitoring the voice conversation on the mobile phone. He means that he need the functions of monitoring the histories of targets calls and their voice dialogue on mobile phone, [sic]” a 10 September 2010 e-mail from Nanatech stated.

Furthermore, the so-called threat posed by North Korea can easily be turned against South Koreans. In January, a Korean-American woman, Shin Eun-mi, was deported for allegedly praising the regime in Pyongyang. Shin’s only “crime” was daring to question the red-scare atmosphere being whipped up by the South Korean government following the decision in December by the Constitutional Court to dissolve the opposition Unified Progressive Party (UPP).

The NIS targeted UPP for disbandment on the pretext of its alleged North Korean sympathies. This minor party, which was on the periphery of the main opposition New Politics Alliance for Democracy

(NPAD), was dissolved after the intelligence agency made phony claims that it had uncovered a pro-North Korean plot involving UPP members.

Revelations emerged in May that the NIS also sought to victimize teachers who belonged to the UPP's forerunner, the Democratic Labor Party, and to illegalize their union, the Korea Teachers and Education Workers Union.

The latest leaks involving Hacking Team reveal the anti-democratic character of the NIS and the South Korean state as a whole. Despite the façade of parliamentary democracy, the police state apparatus, erected by the United States following World War II to provide a foothold on the Korean peninsula, has never been torn down.

In 2012, the NIS used its powers to intervene in the 2012 presidential election between Park Geun-hye, who won the presidency, and Moon Jae-in, who is now the head of the NPAD. The NIS ran an online smear campaign using various aliases to slander Moon and other candidates as North Korean sympathizers. Moon lost by only 3.6 percentage points.

Daum Kakao, the company that owns Kakaotalk, revealed last October that it had received 147 warrants from South Korean intelligence agencies to monitor Kakao Talk conversations, as well as nearly 5,000 warrants to seize the records of past conversations. In September 2014, Park Geun-hye met with officials from telecommunication companies, including Daum Kakao, saying, "Indiscriminate muckraking online that sows public discord has crossed the line, and public insecurity is getting out of control."

The comments came a few months after the sinking of the Sewol ferry in April, in which 304 people died, mostly high school students. The government hoped to clamp down on the widespread anti-Park sentiment that emerged in the wake of the tragedy.

The NIS was founded in 1961 as the Korea Central Intelligence Agency (KCIA) following the May 16 coup that installed Park Chung-hee, the father of current president. Park utilized the KCIA for nearly two decades to maintain his vise-like grip on power before, ironically, being assassinated by KCIA head Kim Jae-gyu in 1979.

Under Park, kidnappings, torture, and phony claims of anti-government plots were the norm, as the KCIA went after political opponents deemed left-wing and pro-communist. Throughout its existence, the KCIA renamed as the NIS has maintained its "anti-communist" investigation functions. These powers were extended during the administration of the so-called democrat Kim Dae-jung, who, until 2002, utilized an illegal wiretapping department organization within NIS to spy on his political opponents.