The Heritage Foundation

ISSUE BRIEF

No. 4367 | MARCH 20, 2015

The U.S. Needs to Respond to North Korea's Latest Cyber Attack

Bruce Klingner

On March 17, Seoul accused Pyongyang of conducting a series of cyber attacks against South Korean nuclear facilities in December 2014.[1] South Korean prosecutors assert that North Korean hackers were responsible for repeated disclosures of information, including blueprints of South Korean nuclear reactors gleaned from cyber attacks, as well as threats to extort money and destroy the nuclear facilities. The hackers demanded that Seoul shut down three reactors or they would carry out another attack. They warned people living nearby to "stay away" from the area[2] since it would "be a Fukushima" nuclear disaster.[3]

The targeted Korea Hydro and Nuclear Power Company controls South Korea's 23 nuclear power plants, accounting for 30 percent of the country's power. The company reported in December that its computer systems were breached but not the reactor control systems. However, South Korean President Park Geun-hye ordered a comprehensive review of the country's nuclear infrastructure against what she called "cyber terrorism" since nuclear power plants "directly impact the safety of the people."[4]

North Korea's Cyber Warfare Capabilities

The North Korean cyber attack against South Korea's nuclear sector is similar to the late 2014 North Korean attack on Sony Pictures. Both attacks were against civilian targets and accompanied by public declarations and demands by affiliated hacker groups, and both sought to extort money and threatened violence. North Korea previously conducted several cyber attacks against U.S. and South Korean government agencies, as well as South Korean banks, businesses, and media organizations, but the two recent attacks were the first accompanied by threats.

Contrary to perceptions of North Korea as a technically backward nation, the regime has a very robust and active cyber warfare capability. The Reconnaissance General Bureau, North Korea's intelligence agency, oversees Unit 121 with 3,000 "cyber-warriors" dedicated to attacking Pyongyang's enemies.[5] North Korean leader Kim Jong-un declared cyber warfare was "a magic weapon" that empowered Pyongyang to launch "ruthless strikes" against South Korea.[6] A South Korean cyber expert assessed that North Korea's electronic warfare capabilities were surpassed only by the United States and Russia.[7]

A Weak Response

In response to the North Korean cyber attack on Sony, President Barack Obama issued Executive Order 13687, which, though expansive in legal breadth, was only weakly implemented. The Administration targeted 13 North Korean entities, three organizations already on the U.S. sanctions list, and 10 individuals not involved in cyber warfare.

Now that Seoul has accused North Korea of being responsible for December's "cyber terrorism," it must articulate its policy response. South Korea should consider rescinding its involvement in the joint North-South Korean economic venture at Kaesong.

This paper, in its entirety, can be found at **http://report.heritage.org/ib4367**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

The 10-year-old economic experiment—the flagship of Seoul's efforts at unconditional engagement with Pyongyang—is not economically viable, having failed to garner sufficient South Korean and international business interest. North Korea has repeatedly unilaterally altered business contracts and linked the business zone to political demands.

More important, the venture failed in its primary objective to induce North Korean economic and political reform and moderate the regime's belligerent and threatening behavior. Seoul cancelled all inter-Korean economic engagement—except Kaesong—after Pyongyang sank a South Korean naval ship in South Korean waters in 2010, killing 46 sailors. Maintaining a "business as usual" policy is unseemly after Pyongyang attacked South Korea's nuclear sector.

White House officials described January's executive order as "a first step...this is certainly not the end,"[8] but the Administration has yet to follow up with any additional measures. During a YouTube interview, President Obama claimed North Korea "is the most isolated,[9] the most sanctioned, the most cut-off nation on Earth." That is simply not true. The U.S., the European Union, and the U.N. have imposed far more pervasive and compelling measures against Iran. Washington has targeted fewer North Korean entities than those of the Balkans, Burma, Cuba, Iran, and Zimbabwe. The U.S. has sanctioned more than twice as many Zimbabwean entities than North Korean.

Nor has Washington designated North Korea as a primary money-laundering concern as it did Iran and Burma. The U.S. has targeted Zimbabwe, Congo, and Burma for human rights violations, but it has yet to take any action against North Korea more than a year after the U.N. Commission of Inquiry accused Pyongyang of human rights violations so egregious as to qualify as crimes against humanity.

Conclusion

The Obama Administration should move beyond its timid sanctions policy and take action to better defend U.S. cyberspace, punish North Korea, and deter further aggression by other malicious nations. Congress and the Administration should:

- **Direct** the Director of National Intelligence to prepare classified and unclassified National Intelligence Estimates on North Korea's cyber capabilities and past attacks.
- **Return** North Korea to the state sponsors of terrorism list. Given the threat of violence against companies and individuals in the U.S., North Korea should be returned to the list.
- **Fully implement** existing U.S. laws against North Korea's illicit activities.

1. Grace Oh, "N. Korea Behind Nuke Power Plant Data Leakage: Investigators," Yonhap News Agency, March 17, 2015, http://english.yonhapnews.co.kr/national/2015/03/17/15/0302000000AEN20150317005551315F.html (accessed March 19, 2015).
2. Victoria Richard, "South Korea to Hold Nuclear Drills after Hack Threat," *The Times*, December 22, 2014, http://www.thetimes.co.uk/tto/news/world/asia/article4304722.ece (accessed March 19, 2015).
3. Jung Kyo-sik, Ser Myo-ja, "North Suspected in Nuke Hacking," Joongang Ilbo, December 26, 2014, http://koreajoongangdaily.joins.com/news/article/Article.aspx?aid=2998926 (accessed March 19, 2015).
4. Justin McCurry, "South Korean Nuclear Operator Hacked Amid Cyber-Attack Fears," *The Guardian*, December 22, 2014, http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack (accessed March 19, 2015).
5. Sangwon Yoon, "North Korea Recruits Hackers at School," Al-Jazeera, June 20, 2011, http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html (accessed March 19, 2015).
6. "N. Korea Boosting Cyber Warfare Capabilities," *The Chosun Ilbo*, November 5, 2013, http://english.chosun.com/site/data/html_dir/2013/11/05/2013110501790.html (accessed March 19, 2015).
7. Choi He-suk, "N.K. Third for Cyber War Capabilities," *The Korea Herald*, June 7, 2012, http://www.koreaherald.com/view.php?ud=20120607001276 (accessed March 19, 2015).
8. "U.S. Sanctions North Korea Over Sony Hacking," *Dallas Morning News*, January 2, 2015, http://www.dallasnews.com/news/local-news/20150102-u.s.-sanctions-north-korea-over-sony-hacking.ece (accessed March 19, 2015).
9. "Best of Obama's Interviews with YouTube Stars," YouTube, January 23, 2015, https://www.youtube.com/watch?v=wgJU7ou4zeQ (accessed March 19, 2015).

- Congress should **assess** additional measures against North Korea, including those contained in the proposed North Korea Sanctions Enforcement Act.

- **Review** existing legislation and executive orders on cyber crime. Assess whether a new executive order should be created for cyber attacks similar to those for terrorism and proliferation of WMD.

In issuing the latest executive order on North Korea, the Obama Administration cited the regime's "provocative, destabilizing, and repressive actions and policies," including its "destructive, coercive cyber-related actions," repeated violations of U.N. Security Council resolutions, and serious human rights abuses. As such, North Korea's actions "constitute a continuing threat to the national security, foreign policy, and economy of the United States."[10]

To date, the U.S. response has not matched the rhetoric. Failure to adequately respond to North Korea's repeated violations of U.S. and international law and U.N. resolutions will only encourage Kim Jong-un to continue, in the words of Director of National Intelligence James Clapper, to "challenge the international community with provocative and threatening behavior in pursuit of his goals."[11]

*—**Bruce Klingner** is Senior Research Fellow for Northeast Asia in the Asian Studies Center, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

10. News release, "Executive Order—Imposing Additional Sanctions with Respect to North Korea," The White House, January 2, 2015, https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea (accessed March 19, 2015).
11. James R. Clapper, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Armed Services Committee, U.S. Senate, February 26, 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (accessed March 19, 2015).