The Heritage Foundation

ISSUE BRIEF

No. 4325 | DECEMBER 22, 2014

Washington Must Respond to North Korean Cyber Bullying and Threats of Terror

David Inserra and Bruce Klingner

Over the past week, the hack of Sony Pictures has gone from an embarrassing cybersecurity incident to successful international terrorism and extortion by North Korea. Several yet-to-be-released films were stolen from Sony Pictures and circulated on the Internet. The hackers, who call themselves the "Guardians of Peace," released private e-mails and the health records and salaries of Sony employees to pressure Sony not to release the movie *The Interview*, a comedy about a fictional plot to assassinate North Korean leader Kim Jong-un. To up the ante, the hackers also threatened a 9/11-type attack on theaters showing the film.[1]

Sony and theater chains quickly withdrew the film for financial and liability reasons. Cancelling the film's release will cost Sony an estimated $100 million in lost revenue.[2] The cancellation of *The Interview*, along with the cancellation of another planned satiric film on North Korea,[3] comes amidst the FBI's determination that the North Korean government was responsible for the hack.[4] Although the attack is on a private company, there are steps that the U.S. government should take in response to this cyber attack by North Korea. The U.S. must signal to the world that dictators and terrorist groups cannot squelch free speech via extortion or a threat of violence.

This paper, in its entirety, can be found at
http://report.heritage.org/ib4325

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

North Korea Cyber Capabilities

Contrary to the perception that North Korea is a technically backward nation, the regime has an active cyber warfare capability. The Reconnaissance General Bureau has 3,000 "cyber-warriors" dedicated to attacking Pyongyang's enemies.[5] Seoul concluded that North Korea was behind cyber attacks against South Korean government agencies, businesses, banks, and media organizations in 2009, 2011, 2012, and 2013. A South Korean cyber expert assessed that North Korea's electronic warfare capabilities were surpassed only by the United States and Russia.[6]

Telegraphing Weakness and Defeat

While North Korea is a serious threat to peace and U.S. interests, this incident requires policymakers to think beyond the Hermit Kingdom. Such an act of extortion will likely inspire other enemies and challengers of the U.S. around the world. ISIS, al-Qaeda, Iran, Russia, China, and others now know they can force a company operating in the U.S. to fold by threatening terrorism. If the U.S. government does not respond, the U.S. will send the message to bad actors around the globe that U.S. citizens and companies can be coerced with impunity. President Obama denounced the attack in his press conference and said that the U.S. will "respond proportionally" in a way and time of the U.S.'s choosing.[7] While this is a good first step, words and symbolic gestures are not enough. In light of other foreign policy retreats and mistakes, such as the recent announcement of normalization of relations with Cuba in return for nothing or the New Strategic Arms Reduction Treaty that was supposed to appease Russia, bad actors

around the world are getting a clear message that the U.S. can be easily duped or coerced.[8] A similar mistake should not be made in this case.

North Korea's role in this cyber attack and its threats against Sony violate multiple laws. Before a criminal indictment can be sought by the Justice Department, though, the government will have to gather all the relevant and material facts. Those facts are not yet available, at least not to the public. Once the government finds out the facts, then they can, and should, find out what statutes the hackers violated and indict the individuals for participating in this egregious terrorist act. Indictments alone, however, are not the solution.

Deterring Aggression

The U.S. government should take action to better defend U.S. cyberspace, punish North Korea, and deter further aggression by other malicious nations. Congress and the Administration should:

1. **Direct the Director of National Intelligence to prepare classified and unclassified National Intelligence Estimates on North Korea's cyber capabilities and past attacks.**
2. **Enable cybersecurity information sharing.** The U.S. government cannot protect every computer from all attacks. Instead, the U.S. should harness the power of the private sector through information sharing. While no guarantee against hacking, information sharing is an easy way to boost security of the private sector and the government by making all who participate more informed and better prepared to avoid and respond to cyber attacks.[9]
3. **Return North Korea to the state sponsors of terrorism list.** The Bush Administration had removed Pyongyang from the list in 2008 as part of the Six-Party Talks nuclear negotiations. Given the threat of violence against companies and individuals in the U.S., North Korea should be returned to the state sponsors of terrorism list.
4. **Fully implement existing U.S. laws against North Korea's illicit activities.** Contrary to media depictions of North Korea as the most heavily sanctioned country in the world, the U.S. has imposed stronger punitive measures against the Balkans, Burma, Cuba, Iran, and Zimbabwe.

1. Brent Lang, "Sony Hackers Threaten 9/11 Attack on Movie Theaters that Screen 'The Interview,'" *Variety*, December 16, 2014, https://variety.com/2014/film/news/sony-hackers-threaten-911-attack-on-movie-theaters-that-screen-the-interview-1201380712/ (accessed December 19, 2014).
2. Nate Silver, "Killing 'The Interview' Could Cost Sony $100 Million," Five Thirty Eight, December 17, 2014, http://fivethirtyeight.com/datalab/killing-the-interview-could-cost-sony-100-million/ (accessed December 19, 2014).
3. Esther Zuckerman, "Steve Carell North Korea-Set Movie Dropped," *Entertainment Weekly*, December 17, 2014, http://insidemovies.ew.com/2014/12/17/steve-carell-north-korea-set-movie-dropped/ (accessed December 19, 2014).
4. News Release, "Update on Sony Investigation," Federal Bureau of Investigation, December 19, 2014, http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (accessed December 19, 2014).
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 December 19, 2014).
6. "N.K. Third for Cyber War Capabilities," *The Korea Herald*, June 7, 2012, http://www.koreaherald.com/view.php?ud=20120607001276 (accessed December 19, 2014).
7. "Obama Pledges Proportional Response to Sony Hack," Associated Press, December 19, 2014, http://abcnews.go.com/Politics/wireStory/obama-pledges-proportional-response-sony-hack-27721995 (accessed December 19, 2014).
8. James Jay Carafano, "More Reasons Not to Trust Russia on New START," Daily Signal, December 15, 2010, http://dailysignal.com/2010/12/15/more-reasons-not-to-trust-russia-on-new-start/; Ana Quintana, "Q&A on Obama's Policy Changes Toward Cuba," Daily Signal, December 18, 2014, http://dailysignal.com/2014/12/18/q-presidents-recent-policy-changes-toward-cuba/; and Kim R. Holmes and James Jay Carafano, "Defining the Obama Doctrine, Its Pitfalls, and How to Avoid Them," Heritage Foundation *Backgrounder* No. 2457, September 1, 2010, http://www.heritage.org/research/reports/2010/08/defining-the-obama-doctrine-its-pitfalls-and-how-to-avoid-them.
9. David Inserra and Paul Rosenzweig, "Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2899, April 1, 2014, http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

Washington should impose the same measures on Pyongyang as it has already done for other countries for far less egregious violations of U.S. law.[10]

5. **Congress should assess additional measures against North Korea**, including those contained in the House of Representatives–approved North Korea Sanctions Enforcement Act.[11]

6. **Review existing legislation and executive orders on cyber crime.** Assess whether a new executive order should be created for cyber attacks similar to those existing for terrorism and proliferation of WMD.[12]

7. **Set clear guidelines for cyber self-defense.** Current law, most notably the Computer Fraud and Abuse Act, makes it illegal for U.S. companies and individuals to engage in any acts of self-defense.[13] While it is not in the U.S.'s interests to make cyberspace a free-fire zone, allowing approved private-sector organizations to engage in clearly defined, non-malicious forms of tracking and tracing cyber aggressors is the bare minimum that Congress should allow companies to do to better protect themselves and assist in the identification of hackers.[14]

8. **Respond with covert cyber attacks against North Korean government targets.** The serious threat of violence against the U.S. and the message U.S. non-action sends to other actors must be confronted. With firm proof of North Korea's responsibility in hand and announced to the world, covert cyber attacks against the North Korean targets would maintain U.S. deniability while also ensuring that North Korea and other actors understand that terrorism against the U.S. will be punished, deterring future extortion.

Standing for American Values and Interests

North Korea poses a growing national security threat to the United States and its allies. Pyongyang continues to augment and refine its nuclear and missile arsenals. In recent years, the regime has conducted cyber attacks against government and private targets. Without a firm response from the U.S. to North Korea's hack of Sony and subsequent threat of terrorism, such attacks and threats against the U.S. and her interests will only grow more common.

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

10. Bruce Klingner, "Time to Get North Korean Sanctions Right," Heritage Foundation *Backgrounder* No. 2850, November 4, 2013, http://www.heritage.org/research/reports/2013/11/time-to-get-north-korean-sanctions-right.
11. North Korea Sanctions Enforcement Act of 2014, H.R. 1771, 113th Congress, http://docs.house.gov/billsthisweek/20140728/BILLS-113hr1771-SUS.pdf (accessed December 19, 2014).
12. Executive Order 13224, September 23, 2001, http://www.state.gov/j/ct/rls/other/des/122570.htm (accessed December 19, 2014).
13. 18 U.S. Code § 1030, http://www.law.cornell.edu/uscode/text/18/1030 (accessed December 19, 2014).
14. Steven P. Bucci, Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2785, April 1, 2013, http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.