U.S.-China Economic and Security Review Commission
Staff Report

January 14, 2015

China's Position on the Sony Attack: Implications for the U.S. Response

by

Jordan Wilson
Research Fellow, Security and Foreign Affairs

The author thanks Richard Bejtlich and Jon Lindsay for their review of early drafts. These experts do not necessarily agree with or endorse the staff report's assessments and statements contained herein, and any errors should be attributed to the author.

Background

In late November 2014, Sony Pictures Entertainment confirmed it was the victim of a cyber attack that crippled its networks and stole large quantities of personal and commercial data.[1] On December 19, the U.S. Federal Bureau of Investigation (FBI) publicly identified North Korea as responsible for these crimes, describing the attack as "destructive" and "coercive" in nature.[2] President Obama pledged the United States would respond "proportionately" and "in a place and time and manner that we choose."[3] On January 2, 2015, the United States imposed financial sanctions on North Korea's arms industry as a "first step in retaliation."[4,*] Analysts and news media have suggested further steps could include listing North Korea as a state sponsor of terrorism, bringing down its propaganda websites, and targeting its computer hardware,[5] with a kinetic response termed "the remotest of possibilities."[6]

U.S. officials reached out to China's government following this attribution in an effort to "share information," "express our concerns," and "ask for their cooperation," as stated by one representative.[7] The United States reportedly asked specifically for assistance in a "blocking action" to eliminate North Korea's ability to carry out future attacks,[8] as Chinese state-owned enterprise China Unicom is a crucial conduit for nearly all of the regime's telecommunications.[9] Beijing has yet to publicly respond to the U.S. overture or officially acknowledge North Korean involvement, stating only that China "is against all forms of cyber attacks," including those launched by a state "using facilities beyond its own national borders against a third country."[10]

As China has received attention as a potential factor in this attack, is in a unique position to influence North Korea, and is a key player in the development of international norms in cyberspace, its reactions to U.S. decisions on these matters are of particular interest.

Was China Involved in the Attack against Sony?

President Obama said on December 20 the U.S. had found "no indication that North Korea was acting in conjunction with another country."[11] Some analysts have suggested, however, that China could have played a role in the attack, but the Administration has avoided public accusations for diplomatic reasons. Arguments for China's involvement have largely drawn on its physical proximity to North Korea's cyber infrastructure as well as political ties to its leadership; one U.S. senator made the case that carrying out an operation of this size required China "being involved or at least knowing about it,"[12] a statement swiftly criticized by China's government.[13] Other sources suggest the Sony attack could have been routed through Chinese servers[14] or that a network of as many as 1,000 North Korean hackers operating in China could have played a role,[15] particularly the "Bureau 121" group reportedly working out of North Korean-owned locations in Shenyang.[16]

None of these assertions has been accompanied by substantive evidence of knowledge or assistance on the part of China's government, however.[†] Proximity is insufficient to prove complicity, as reports show the

[*] North Korea experienced recurring Internet failures over several days beginning December 22, 2014. Some have speculated the outages were the result of a U.S. cyber attack, but to date there has been no evidence to support this claim. Former director of operations at U.S. Cyber Command Maj. Gen. Brett Williams, USAF (Retd.) has stated it is "unlikely this was the result of U.S. actions," as it was not a "proportionate response" as promised, and the United States would likely use a more sophisticated and targeted approach to impact the North Korean leadership directly. Interview with Lawrence O'Donnell, *MSNBC*, Television, December 22, 2014. *http://www.msnbc.com/the-last-word/watch/what-s-behind-north-korean-internet-outage--376176707647*.

[†] According to Richard Bejtlich, Chief Security Strategist at FireEye, Inc., the presence of these units in China could constitute "state-ignored" responsibility if China's government knowingly allowed North Korean hackers to operate

Sony attack was routed through servers in Bolivia, Italy, the United States, and five other countries as well.[17] Furthermore, evidence indicates North Korea is capable of having conducted the operation on its own;[*] its cyber forces have benefited from a surge in investment and training in recent years,[18] and previously developed a similar but more rudimentary malware called DarkSeoul, used to attack South Korea in 2013.[19] FBI Director James Comey referred to "clear links" to this malware, as well as numerous other lines of evidence indicating North Korea's responsibility, in detailed remarks given on January 7.[20]

Will China Assist the U.S. Response?

It is unlikely China will cooperate with U.S. government actions against North Korea, based on three factors:

- First, U.S.-China cyber cooperation is currently at a low point, marked by China's suspension of the "U.S.-China Cyber Working Group" in May 2014 in response to the FBI's indictment of five People's Liberation Army officers for cyber espionage.[21] Recent efforts to restart dialogue on the subject have proven unsuccessful.[22] China considers the United States' current stance to be hypocritical and threatening to its interests, and has used information on U.S. cyber activities from recent intelligence leaks to justify avoiding collaboration and to build traction with other like-minded nations.[23] Given this atmosphere, China is extremely unlikely to assist the United States with a defining response in the cyber domain, particularly in such a politically-charged matter.

- Second, China to date has withheld judgment on whether North Korea was involved in the attack at all,[24] and implied the FBI's statement offers insufficient evidence to substantiate the U.S. claim.[25] This is consistent with China's refusal to assign blame for North Korea's provocative actions in the past, including the sinking of a South Korean naval vessel and bombardment of a South Korean island in 2010,[26] indicating it probably will take the same course in this case.

- Finally, China has actively censored reports on the cyber attack domestically,[27] limiting its citizens' access to the flood of media output detailing North Korea's crimes. This would be an unlikely course of action to take if China were preparing to condemn or act against North Korea.

How Would China React to a U.S. Cyber Operation against North Korea?

In the case of a clear, attributable counterattack in cyberspace by the United States against North Korea, China most likely would respond with strong condemnation through official channels. Two considerations support this assumption:

- First, in the current contentious atmosphere of bilateral cyber relations, China is better able to defend its stance by condemning a unilateral move by the U.S. to define boundaries in this domain than by acquiescing to or supporting it. Affirming the "redline" drawn by U.S. retaliation would do harm to China's position, as it would have had no input into the process of the line's establishment and has found little common ground with the United States on setting such boundaries in the past.[28]

---

in Shenyang and carried their network traffic. The U.S. Government has made no statements regarding whether China had such knowledge. Richard Bejtlich, Chief Security Strategist, FireEye, Inc., interview with Commission staff, January 9, 2015.

[*] This refers to North Korea's use of either internal units or third party criminal groups to carry out the attack. The public FBI statement refers to the North Korean government's "responsibility" and does not distinguish between these types of forces. For practical purposes such as identifying North Korea's intent and capability to launch such an operation, there is no difference.

Condemning the U.S. operation, on the other hand, would be a costless move, as it is not likely to undermine the dialogue further while the two sides have yet to even begin identifying areas of agreement.

- Second, while a "second strike" such as this would be unprecedented, China's past responses to other U.S. actions in the cyber domain are informative. Chinese official statements and domestic scholarly and media articles have excoriated U.S. cyber deterrence policies,[29] stating in one article the United States is "playing a dangerous game with cyber deterrence" and "militarizing cyberspace."[30] Responding to U.S. cyber attribution efforts, some have called these cases "typically fictitious" and accused the United States of being too quick to attribute "improper individual behaviors" to state actors.[31] Revelations of U.S. acts of cyber espionage led to descriptions of the United States as "the biggest cyber villain in our age."[32] This theme suggests a similar response from Beijing in the case of an unmistakable U.S. cyber attack for deterrence purposes.

Could a Response Deter Future Chinese Cyber Operations against the U.S.?

Responsive action against North Korea in any form takes the United States into uncharted territory in the worldwide cyber domain. The Sony cyber attack is a new type of event, as conducting a cyber operation against a company for coercive purposes goes beyond traditionally subtle cyber espionage, yet falls short of an "act of war" that causes equivalent to a traditional military attack.[33,*] As stated by a former White House cybersecurity advisor, the United States' decision will "indelibly serve to influence future nation-state behavior."[34] The costs imposed will help determine whether actions in this gray zone between computer network exploitation and computer network attack, creating "harms between the concepts of war and peace" as termed by one analyst,[35] are deterred in the future, not only from North Korea but from state and non-state actors worldwide.

Past U.S. responses such as the FBI indictment or official denunciations have in no way discouraged Chinese state-sponsored intrusions into government and industry networks thus far. This case provides a new opening, however, for the United States to solidify its declaratory policy, define what is acceptable, and potentially change the calculus of actors in this domain in regards to this new type of attack.[36] It can take this action without incurring the costs of disrupting an already weakened cyber dialogue with China, in which finding common ground on such redlines has been highly challenging.[37] Although typical cyber espionage activities would remain unaffected, should Chinese entities ever in the future contemplate similar "gray zone" cyber operations against U.S. industry networks for coercive purposes, the precedent set by the U.S. response to North Korea likely will influence their calculations.

Conclusion

China's likely position on the Sony attack and the developing U.S. response is that of a nonaligned and disapproving third party. A forceful and unmistakable retaliation offers the United States the opportunity to define redlines and enhance its security in this challenging domain, while incurring few costs due to the current stalled state of U.S.-China dialogue on cyber issues.

---

[1] U.S. Federal Bureau of Investigation, *Update on Sony Investigation*, December 19, 2014. *http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation*; Associated Press, "Sony Saga Blends

---

[*] This is the most current, albeit ambiguous, definition given by U.S. officials for an "act of war" in cyberspace. See Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War: Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force," *Wall Street Journal*, May 31, 2011. *http://www.wsj.com/articles/SB10001424052702304563104576355623135782718*.

Foreign Intrigue, Star Wattage," *New York Times,* December 20, 2014. *http://www.nytimes.com/aponline/2014/12/20/us/politics/ap-us-sony-hack.html*; and Lori Grisham, "Timeline: North Korea and the Sony Pictures Hack," *USA Today,* January 5, 2015. *http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.*

[2] U.S. Federal Bureau of Investigation, *Update on Sony Investigation,* December 19, 2014. *http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.*

[3] Associated Press, "Obama Says North Korea Hacked Sony, Vows Response," *New York Times,* December 19, 2014. *http://www.nytimes.com/aponline/2014/12/19/arts/ap-us-sony-hack.html.*

[4] Carol E. Lee and Jay Solomon, "U.S. Targets North Korea in Retaliation for Sony Hack: New Sanctions Target Individuals Working for Arms Industry," *Wall Street Journal,* January 3, 2015. *http://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942*.

[5] David Rothkopf, "Obama Is Wrong: The Sony Hack Is Not 'Cybervandalism': Why the United States Needs a Broad, New Strategy to Prepare for – and Defend against – the Next Generation of Online Warfare," *Foreign Policy,* December 22, 2014. *http://foreignpolicy.com/2014/12/22/cyber-attack-sony-hack-north-korea-obama-response/?wp_login_redirect=0*; David E. Sanger, Nicole Perlroth, and Eric Schmitt, "U.S. Asks China to Help Rein in Korean Hackers," *New York Times,* December 20, 2014. *http://www.nytimes.com/2014/12/21/world/asia/us-asks-china-to-help-rein-in-korean-hackers.html*; Jonathan Cheng and Jeyup S. Kwaak, "North Korea: How Can the U.S. Respond to Sony Hack Attack?: Experts Say Possible Responses Range from Financial Sanctions to Targeting North Korea's Cyber Capabilities," *Wall Street Journal,* December 20, 2014. *http://www.wsj.com/articles/north-korea-how-can-the-u-s-respond-to-sony-hack-attack-1419063801*; Anna Yukhananov and James Pearson, "Washington Is Limited in its Response to North Korea over Sony Hack," Reuters, December 19, 2014. *http://www.reuters.com/article/2014/12/19/us-sony-cybersecurity-sanctions-idUSKBN0JX1UW20141219?feedType=RSS&feedName=topNews&utm_source=twitter*; and Joseph Marks, "What Does a Cyber Counterattack Look Like?" *Politico,* December 19, 2014. *http://www.politico.com/story/2014/12/what-does-a-cyber-counterattack-look-like-113715.html.*

[6] Jonathan Cheng and Jeyup S. Kwaak, "North Korea: How Can the U.S. Respond to Sony Hack Attack?: Experts Say Possible Responses Range from Financial Sanctions to Targeting North Korea's Cyber Capabilities," *Wall Street Journal,* December 20, 2014. *http://www.wsj.com/articles/north-korea-how-can-the-u-s-respond-to-sony-hack-attack-1419063801.*

[7] Ralph Ellis, Holly Yan, and Kyung Lah, "U.S. Seeks China's Help against North Korean Cyberattacks," CNN, December 20, 2014. *http://www.cnn.com/2014/12/20/world/asia/north-korea-sony-response/.*

[8] David E. Sanger, Nicole Perlroth, and Eric Schmitt, "U.S. Asks China to Help Rein in Korean Hackers," *New York Times,* December 20, 2014. *http://www.nytimes.com/2014/12/21/world/asia/us-asks-china-to-help-rein-in-korean-hackers.html*.

[9] Nicole Perlroth and David E. Sanger, "North Korea Loses its Link to the Internet," *New York Times,* December 22, 2014. *http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html*; David E. Sanger, Nicole Perlroth, and Eric Schmitt, "U.S. Asks China to Help Rein in Korean Hackers," *New York Times,* December 20, 2014. *http://www.nytimes.com/2014/12/21/world/asia/us-asks-china-to-help-rein-in-korean-hackers.html*; and Carol E. Lee, "U.S. Approaches China in Effort to Respond to North Korean Hacking Communications with Chinese Officials Seek Beijing's Intervention," *Wall Street Journal,* December 20, 2014. *http://www.wsj.com/articles/u-s-approaches-china-in-effort-to-respond-to-north-korean-hacking-1419122637?mod=WSJ_hpp_LEFTTopStories*.

[10] Ministry of Foreign Affairs of the People's Republic of China, *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on December 22, 2014*, December 22, 2014; Xinhua (English edition), "China against All Forms of Cyber Attacks, Cyber Terrorism," December 22, 2014. *http://news.xinhuanet.com/english/china/2014-12/22/c_133870914.htm*; and Zhang Yunbi and Chen Weihua, "Awaiting Word from China on Sony Hack," *China Daily,* December 23, 2014. *http://usa.chinadaily.com.cn/world/2014-12/23/content_19143627.htm*.

[11] Ralph Ellis, Holly Yan, and Kyung Lah, "U.S. Seeks China's Help against North Korean Cyberattacks," CNN, December 20, 2014. *http://www.cnn.com/2014/12/20/world/asia/north-korea-sony-response/.*

[12] Jeremy Diamond, "Graham Suspects China Involved in Sony Attack," CNN, December 29, 2014. *http://www.cnn.com/2014/12/28/politics/lindsey-graham-north-korea-guantanamo/.*

[13] Ministry of Foreign Affairs of the People's Republic of China, *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on December 29, 2014*, December 29, 2014. *http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1224045.shtml*.

[14] Simon Denyer, "China Reluctant to Join U.S. in Punishing North Korea over Cyberattacks," CNN, December 23, 2014. *http://www.washingtonpost.com/world/asia_pacific/china-reluctant-to-join-us-in-punishing-north-korea-over-*

cyberattacks/2014/12/23/911c5418-1bac-4307-9119-32adac212568_story.html; Gordon G. Chang, "Did China Help North Korea Hack Sony?" *Forbes,* December 21, 2014. *http://www.forbes.com/sites/gordonchang/2014/12/21/did-china-help-north-korea-hack-sony/*.

[15] Nicole Perlroth and David E. Sanger, "North Korea Loses its Link to the Internet," *New York Times,* December 22, 2014. *http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html*; *Huanqiu* (China), "South Korea Says North Korea Has Built a Network of About 1000 People in China," December 22, 2014. *http://www.wokeji.com/military/jsyw/201412/t20141222_904313.shtml*. [Staff translation]; and Gordon G. Chang, "Did China Help North Korea Hack Sony?" *Forbes,* December 21, 2014. *http://www.forbes.com/sites/gordonchang/2014/12/21/did-china-help-north-korea-hack-sony/*.

[16] Will Ripley, "North Korean Defector: 'Bureau 121' Hackers Operating in China," CNN, January 7, 2015. *http://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/*; HP Security Research, *HP Security Briefing Episode 16, August 2014: Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*, August 2014, 22. *http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf*.

[17] Jose Pagliery, "What Caused Sony Hack: What We Know Now," CNN Money, December 29, 2014. *http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/*; Nicole Perlroth and David E. Sanger, "North Korea Loses its Link to the Internet," *New York Times,* December 22, 2014. *http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html*; and Drew Harwell and Ellen Nakashima, "Hackers' Threats Prompt Sony Pictures to Shelve Christmas Release of 'The Interview,'" *Washington Post,* December 17, 2014. *http://www.washingtonpost.com/business/economy/top-movie-theater-chains-cancel-premiere-showings-of-the-interview/2014/12/17/dd1bdb2a-8608-11e4-9534-f79a23c40e6c_story.html*.

[18] *Yonhap* (ROK), "DPRK Cyber War Capabilities Surge under Kim Jong Un," December 20, 2014. Open Source Center Transcription ID: KPO2014122044582812; Ju-Min Park and James Pearson, "In North Korea, Hackers Are a Handpicked, Pampered Elite," Reuters, December 5, 2014. *http://www.reuters.com/article/2014/12/05/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205*; HP Security Research, *HP Security Briefing Episode 16, August 2014: Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*, August 2014, 60. *http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf*.

[19] Mike Levine, Pierre Thomas, and Jack Cloherty, "Sony Hacking: FBI Blames North Korea," ABC News, December 19, 2014. *http://abcnews.go.com/International/interview-fbi-links-north-korea-sony-hacking/story?id=27694178*; *Chosun Ilbo* (ROK), "Evidence in Hacker Attack Points to North Korea," April 11, 2013. *http://english.chosun.com/site/data/html_dir/2013/04/11/2013041100648.html*; and U.S. Federal Bureau of Investigation, *Update on Sony Investigation*, December 19, 2014. *http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation*.

[20] Robert Hackett, "FBI Director: Sony Hackers 'Got Sloppy'", *Fortune,* January 7, 2015, *http://fortune.com/2015/01/07/fbi-director-sony/*.

[21] Mu Xueyuan, "China Suspends Cyber Working Group Activities with U.S. to Protest Cyber Theft Indictment," Xinhua (English edition), May 20, 2014. *http://news.xinhuanet.com/english/china/2014-05/20/c_126520553.htm*; Doug Drinkwater, "China Denies New FBI Hacking Claims," *SC Magazine,* October 20, 2014. *http://www.scmagazineuk.com/china-denies-new-fbi-hacking-claims/article/378095/*.

[22] Zhang Yunbi and Chen Weihua, "Awaiting Word from China on Sony Hack," *China Daily*, December 23, 2014. *http://usa.chinadaily.com.cn/world/2014-12/23/content_19143627.htm*; Cory Bennett, "US, China See Little Progress on Cybersecurity," *The Hill,* November 12, 2014. *http://thehill.com/policy/cybersecurity/223865-us-china-see-little-progress-on-cybersecurity*; Adam Segal, "Axiom and the Deepening Divide in U.S.-China Cyber Relations," Council on Foreign Relations *Net Politics Blog*, October 29, 2014. *http://blogs.cfr.org/cyber/2014/10/29/axiom-and-the-deepening-divide-in-u-s-china-cyber-relations/*; and Benjamin Kang Lim, "China Says It's Hard to Resume Security Talks with U.S.," Reuters, October 19, 2014. *http://www.reuters.com/article/2014/10/19/us-china-usa-cybersecurity-idUSKCN0I80GU20141019*.

[23] Amy Chang, *Warring State: China's Cybersecurity Strategy* (Center for a New American Security, December 2014), 30. *http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang.pdf*.

[24] Zhang Yunbi and Chen Weihua, "Awaiting Word from China on Sony Hack," *China Daily*, December 23, 2014. *http://usa.chinadaily.com.cn/world/2014-12/23/content_19143627.htm.*

[25] Will Ripley, "North Korean Defector: 'Bureau 121' Hackers Operating in China," CNN, January 7, 2015. *http://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/*.

[26] Victor Cha, "China's Choice," *Chosun Ilbo* (ROK), May 25, 2010. *http://english.chosun.com/site/data/html_dir/2010/05/25/2010052501422.html*; University of Southern California US-China Institute, *Hong Lei, China's Response to the Yeonpyeong Island Incident, November 25, 2010*, November 25, 2010. *http://china.usc.edu/(S(mb5cldyotnlbux55ol3cruu0)A(BAFo5-g9zQEkAAAAMDhhMGYzZDgtNzc0My00OGIxLWI4MGYtYWU3NjA3ZTg4MDVl7HxHeG9AZ48yTd4qediIP7XNSx81))/ShowArticle.aspx?articleID=2316&AspxAutoDetectCookieSupport=1*.

[27] Will Ripley, "North Korean Defector: 'Bureau 121' Hackers Operating in China," CNN, January 7, 2015. *http://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/*.

[28] Blake Sobczak, "China and U.S. Grapple over Red Lines for Cyberattacks," *Environment & Energy Publishing*, December 22, 2014. *http://www.eenews.net/stories/1060010888*; Cory Bennett, "US, China See Little Progress on Cybersecurity," *The Hill*, November 12, 2014. *http://thehill.com/policy/cybersecurity/223865-us-china-see-little-progress-on-cybersecurity*.

[29] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, September 20, 2013, pp. 7-8. *http://carnegieendowment.org/files/CLM42MS.pdf*.

[30] Yu Xiaoqu, "US Playing Dangerous Game with 'Cyber Deterrence,'" *People's Daily* (China), July 26, 2011, *http://english.people.com.cn/90001/90780/91343/7452284.html*.

[31] Ellen Nakashima, "Researchers Identify Sophisticated Chinese Cyberespionage Group," *Washington Post*, October 28, 2014. *http://www.washingtonpost.com/world/national-security/researchers-identify-sophisticated-chinese-cyberespionage-group/2014/10/27/de30bc9a-5e00-11e4-8b9e-2ccdac31a031_story.html?tid=pm_world_pop*; Yu Xiaoqu, "US Playing Dangerous Game with 'Cyber Deterrence'," *People's Daily* (China), July 26, 2011. *http://english.people.com.cn/90001/90780/91343/7452284.html*.

[32] BBC News, "China's Xinhua News Agency Condemns US 'Cyber-Attacks,'" June 23, 2013. *http://www.bbc.com/news/world-asia-23018938*.

[33] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War: Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force," *Wall Street Journal*, May 31, 2011. *http://www.wsj.com/articles/SB10001424052702304563104576355623135782718*; James A. Lewis, *The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict* (Center for Strategic and International Studies, October 2009). *http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf*.

[34] "Sony Saga Blends Foreign Intrigue, Star Wattage," *New York Times*, December 20, 2014. *http://www.nytimes.com/aponline/2014/12/20/us/politics/ap-us-sony-hack.html*.

[35] Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39(2) (Fall 2014), p. 181.

[36] Rob Lever, "US Eyes Cyber 'Deterrence' to Stop Hackers," Agence France-Presse, October 28, 2014. *http://news.yahoo.com/us-eyes-cyber-deterrence-stop-hackers-202710016.html*; National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), p. 57. *http://www.nap.edu/openbook.php?record_id=12997&page=57*; Maj. Gen. Brett Williams, USAF (Retd.), *MSNBC*, Television, December 22, 2014. *http://www.msnbc.com/the-last-word/watch/what-s-behind-north-korean-internet-outage--376176707647*.

[37] Blake Sobczak, "China and U.S. Grapple over Red Lines for Cyberattacks," *Environment & Energy Publishing*, December 22, 2014. *http://www.eenews.net/stories/1060010888*.