SONY'S NIGHTMARE BEFORE CHRISTMAS

The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace

National Security Report

Antonio DeSimone | Nicholas Horton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

SONY'S NIGHTMARE BEFORE CHRISTMAS

The 2014 North Korean Cyber Attack on Sony and
Lessons for US Government Actions in Cyberspace

Antonio DeSimone

Nicholas Horton

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

NSAD-R-17-045

Contents

Figures

Tables

Summary

The cyber attack on Sony Pictures Entertainment in late 2014 began as a public embarrassment for an American company and ultimately led to the unprecedented action by the US president to formally attribute a cyber attack to a nation-state (North Korea). The incident played out at the nexus of the private cyber-security industry and US government communities including the White House, the Federal Bureau of Investigation, and the National Security Agency.

The attack was triggered by Sony's plan to release *The Interview*, a comedy in which an American talk show host and his producer are recruited by the Central Intelligence Agency to travel to North Korea and assassinate North Korea's supreme leader, Kim Jong-un. The cyber attack was discussed everywhere: from supermarket tabloids, delighting in gossip-rich leaked emails, to official statements by leaders in the US government, including President Obama.

When laid out in a timeline, the events surrounding the cyber attack—which include the attribution to North Korea and subsequent responses by both the government and private-sector cyber-security experts—provide a case study of the actions and interactions of the players in a major cyber attack.

The events surrounding the attack and the attribution provide insight into three areas: the effects of government and private-sector actions on the perception of a cyber event among the public, the effect of attribution on the behavior of the attackers, and possible motives for North Korea's high-profile cyber actions. The incident also illuminates the role of multi-domain deterrence to respond to attacks in the cyber domain.

Cyber attacks have increased in number, scale, and variety in recent years,[1] threatening US economic interests and national security. In the eyes of some, the cyber threat from sophisticated actors capable of "full spectrum" actions "has potential consequences similar in some ways to the nuclear threat of the Cold War."[2] High-consequence cyber attacks call for a whole-of-government response to detect, deny, and deter bad actors and, when appropriate, retaliate. Proper and proportional retaliation in the face of a cyber attack is a particularly difficult problem. An attacker may not have appropriate cyber targets, calling for a retaliatory capability in a different domain. The policy issues associated with employing different levers of power under different authorities (multi-domain deterrence) should be informed by an understanding of the actions and interactions among the players in a cyber attack.

This report provides a case study of the 2014 cyber attack on Sony Pictures Entertainment (NOTE: in this paper, "Sony" will refer to Sony Pictures Entertainment, while "Sony Corp." will refer to the parent, Japan-based Sony Corporation). By following the course of a single incident, we hope to gain insight into how players across governments and the private sectors behave and respond when an attack occurs. The Sony attack achieved wide public notoriety, driven perhaps less by a broad interest in national security than by leaked emails that disclosed interesting ways celebrities misbehave. Looking past the fascination with the culture of celebrity and the backroom dealings in the entertainment industry, we find that the events in that short period, which included an unprecedented public attribution by the president, provide a window into nation-state actions in cyberspace and an interesting case study of US government activities at the intersection of law enforcement and national security.

The wide variety of actions and actors in this case study make it particularly interesting as a source of insights into the multi-domain deterrence problem: a private US company became the target of a cyber attack by a foreign nation-state with minimal cyber infrastructure and a nonexistent private industry. The United States cannot deter an attack like this by threatening retribution in kind. The United States is not likely to embrace a declaratory cyber-deterrence policy that includes attacks on private companies, and even if it did, this attacker does not have such assets to hold at risk. Multi-domain deterrence policies could have an impact on adversaries considering a cyber attack on a US asset; this case study can help shape such policies.

The general outline of the events is well known. Sony planned to release *The Interview*, a Seth Rogan comedy portraying the assassination of Kim Jong-un, the supreme leader of North Korea, or, officially, the Democratic People's Republic of Korea. The North Korean government objected to the movie, including a vehement protest to the secretary-general of the United Nations (UN), but Sony pushed ahead with its plan to show the film. One month before *The Interview*'s scheduled Christmas release, a cyber attack on Sony released a trove of sensitive data and caused extensive damage to Sony computers. Later, as leaks continued and anonymous threats to Sony increased, the US government reacted to this attack on a private company in an unprecedented public manner, attributing the attack to North Korea. This triggered strong public statements by North Korea in state-controlled media, as well as an overt response to the attack by the United States in the economic and diplomatic domains and, possibly, covert response in the cyber domain. Throughout the ordeal, public commentary and reactions by private cyber-security companies helped uncover the myriad of actions by governments, private industry, and shadowy groups.

[1] Symantec, *2016 Internet Security Threat Report,* 21, https://www.symantec.com/content/dam/symantec/docs/security-center/archives/istr-16-april-volume-21-en.pdf.

[2] DoD Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, January 2013, http://www.dtic.mil/docs/citations/ADA569975.

While the cyber attack itself played out over a few weeks in November and December 2014, the activities during those weeks are connected to actions by both the United States and North Korea that extend back at least a decade. This report lays out the timeline of events by the United States, North Korea, actors in cyberspace, and interested private sector parties.

The following section presents the overall timeline, and subsequent sections describe the details of the buildup and initial phases of the attack, the actions of the private cyber-security industry, the decision by the US government to attribute the attack to North Korea, and North Korea's reaction. The paper concludes with a discussion of the aftermath of the attack and possible broader implications of the events in this case study.

Timeline of Events

The 2014 Sony cyber attack includes actions by the United States and foreign governments, the US private sector, and shadowy cyber groups. A timeline of events during the most eventful weeks of the attack is displayed in Figure 1. This timeline provides a reference for the discussions in the rest of the report. Each event will be further described in the following sections.

Sony, *The Interview*, and the Attack

> and this isn't flunky it's the chairman of the entire sony corporation who I am dealing with.
>
> *– Email from Amy Pascal to Seth Rogen, on Kazuo Hirai's concern over* The Interview

The Interview was conceived in 2010 as a farcical movie, in the tradition of Borat,[3] that satirized the perceived idiosyncrasies of a distant nation from a Western perspective. Originally, the target of ridicule was Kim Jong-il, but between conception and screenplay, Kim Jong-il died and was succeeded by his son, Kim Jong-un, an equal—perhaps superior—subject for an irreverent American movie.

As Sony geared up its publicity machine in advance of a scheduled October release,[4] the first "teaser" trailer for the movie was posted to YouTube on June 11, 2014, promoting an October release of the movie. The trailer portrayed the film as satire in which a Hollywood talk show host and his producer are hired by the Central Intelligence Agency (CIA) to travel to North Korea and assassinate Kim Jong-un. The trailer parodies the American celebrity news culture but also mocks the mythology surrounding North Korean leadership.

Soon after the first trailer was released, North Korea responded quickly and vehemently in the international community. On June 27, a letter from North Korea's UN ambassador, Ja Song-nam, to Secretary-General Ban Ki-moon said, "Absolutely intolerable is the distribution of such a film in the United States, as it is the most undisguised terrorism and an act of war to deprive the service personnel and people of [North Korea] of their mental mainstay and bring down its social system."[5]

Both Sony and Sony Corp. expressed discomfort with the controversial film. Kazuo Hirai, chief executive officer of Sony Corp., screened the movie soon after the trailer was released. As later disclosed in emails leaked as part of the ensuing cyber attack, Hirai called Michael Lynton, the chief executive officer of

[3] Mark Seal, "An Exclusive Look at Sony's Hacking Saga," *Vanity Fair* (March 2015), https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

[4] Jason Hughes, "James Franco and Seth Rogen Are Going to Take Out Kim Jong-Un in 'The Interview' Trailer (Video)," *Wrap* (June 11, 2014), https://www.thewrap.com/seth-rogen-and-james-franco-are-going-to-take-out-kim-jong-un-in-the-interview-trailer-video/.

[5] United Nations, General Assembly Security Council. Letter dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations addressed to the Secretary-General. A/68/934–S/2014/451, June 27, 2014.

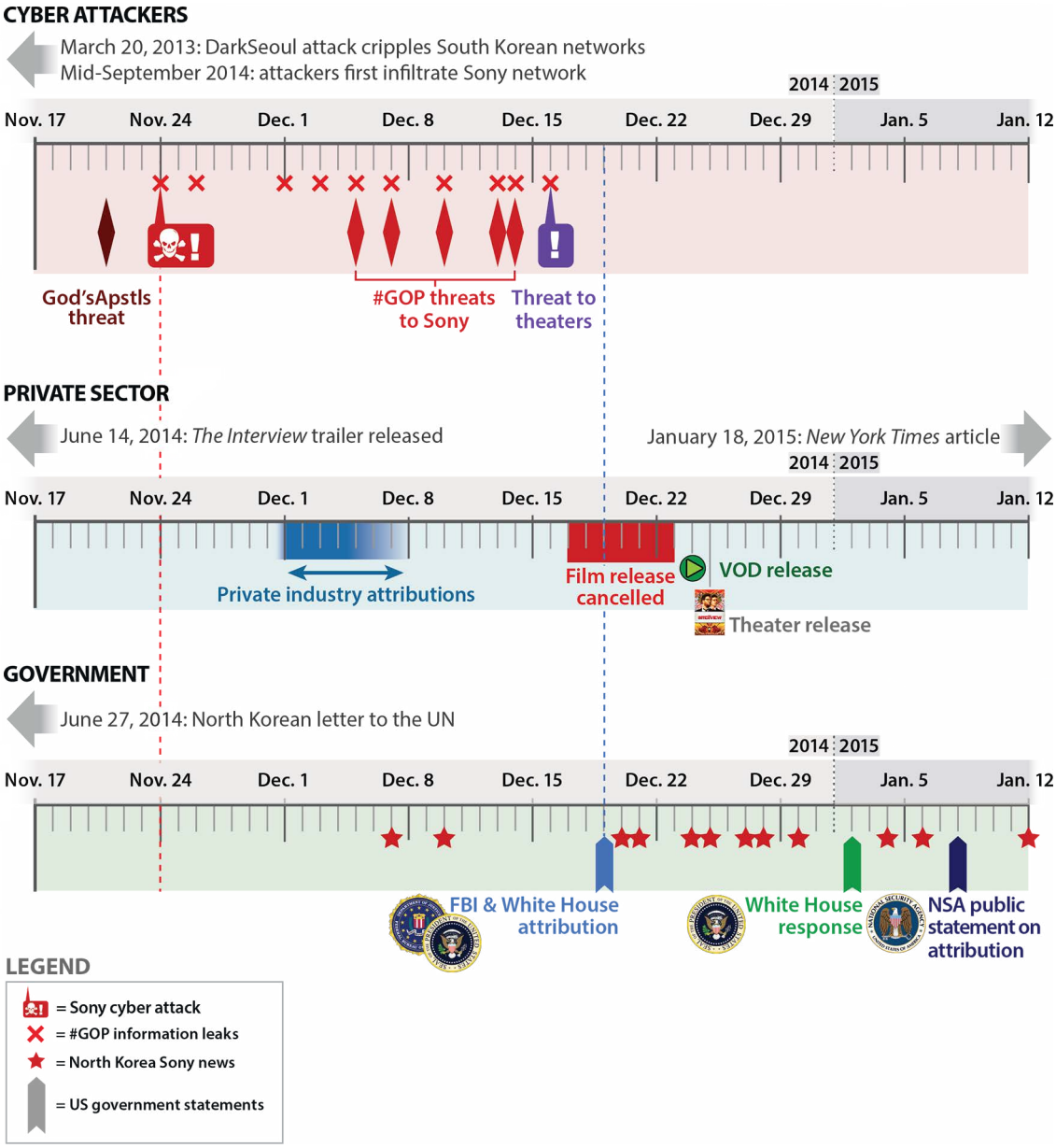


Figure 1. Timeline of Events Surrounding 2014 Sony Cyber Attack

Sony, and expressed his concerns for the film.[6] *Vanity Fair* reported that Hirai "believed the movie could enrage Japan's volatile enemy and neighbor."[7]

Despite the controversy, Sony decided to move ahead with the film. Hirai suggested multiple changes to the film, including a softening of Kim Jong-un's death

[6] Peter Elkind, "Inside the Hack of the Century. Part 2: The storm builds," *Fortune* (June 26, 2015), http://fortune.com/sony-hack-part-two/.

[7] Mark Seal, "An Exclusive Look at Sony's Hacking Saga," *Vanity Fair* (March 2015), https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

scene.[8] The edits pushed back the release date to December 25, 2014.[9]

> We've obtained all your internal data.
>
> *– #GOP*

Sony employees showed up for work the Monday before the Thanksgiving holiday, perhaps expecting a quiet week. Instead, they were greeted by an image on their computer monitors,[10] depicted in Figure 2, containing disturbing graphics, somewhat incoherent threats, and multiple suspicious URLs. For some of the Sony executives, this may not have been a complete surprise; on the Friday before the attack,[11] a group identifying themselves as "God'sApstls" sent an email to Sony executives, stating "We've got great damage by Sony Pictures… Pay the damage, or Sony Pictures will be bombarded as a whole."[12] However, the threats were vague, and the source had no credibility. Even with the benefit of hindsight, Sony's disregard of this anonymous threat is understandable.

The attack was the work of a group called the "Guardians of Peace" (#GOP). The disturbing screen image greeting Sony employees was reminiscent of website defacements characteristic of cyber vandalism. However, the attack on November 24 was not just vandalism. The URLs at the bottom of the screen led to lists of files that #GOP claimed it exfiltrated from Sony, as well as email addresses to contact #GOP members.[13] The material showed that #GOP was able to exfiltrate Sony's protected content.

North Korea and Black Market Media

The Interview was not the first time that Hollywood mocked the supreme leader of North Korea [*Team America: World Police* (2004) is another film in the same vein]. However, changes in the world are making the country more fearful of exposure to Western media. North Korea is a famously closed country that does not allow free flow of international media. Part of this is for control purposes; the North Korean government fears that exposure of Western media to its citizens could incite tremendous pressure for social reform.

North Korea has had a flourishing information black market for the past decade. Tools to deliver media, such as radios (that can tune into South Korean stations), DVDs, and flash drives enter the country via smugglers or tied to balloons. Those that are not found during police sweeps are passed from household to household. Many of the people involved with these smuggling campaigns are defectors from North Korea living in South Korea or elsewhere. The outside media exposes North Koreans to the world as it exists outside the country's borders and provides a view counter to the messages from state-controlled media.[14, 15] Therefore, it is in the best interest of North Korea's government to limit the negative depictions of it from the beginning.

Two URLs pointed to servers registered under Sony's domain name, another was under Brazil's top-level

[8] Peter Elkind, "Inside the Hack of the Century. Part 2: The storm builds," *Fortune* (June 26, 2015), http://fortune.com/sony-hack-part-two/.

[9] Mark Seal, "An Exclusive Look at Sony's Hacking Saga," *Vanity Fair* (March 2015), https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

[10] Imgur, "I used to work for Sony Pictures. My friend still works there and sent this to me. All of Sony has been hacked," *Imgur* (image-sharing site), November 24, 2014, https://imgur.com/qXNgFVz.

[11] Nicole Arce, "Sony was Warned of Impending Cyber Attack in Extortion Email, Reveal Leaked Messages from Inboxes of Top Executives," *Tech Times* (December 9, 2014), http://www.techtimes.com/articles/21770/20141209/sony-was-warned-of-impending-cybertattack-in-extortion-email-leaked-email-boxes-of-top-executives-reveal.htm.

[12] Lorenzo Franceschi-Bicchierai and Christina Warren, "Hackers Sent Extortion Email to Sony Executives 3 Days Before Attack," *Mashable* (December 8, 2014), http://mashable.com/2014/12/08/hackers-emailed-sony-execs/.

[13] Xiphos Research, *A Sony Story: An Examination of the SPE Breach*, December 18, 2014, http://xiphosresearch.com.

[14] Andy Greenberg, "The Plot to Free North Korea with Smuggled Episodes of 'Friends,'" *Wired* (March 1, 2015), https://www.wired.com/2015/03/north-korea/.

[15] News Desk, "How Media Smuggling Took Hold in North Korea," *PBS News Hour* (December 18, 2016), https://www.pbs.org/newshour/world/media-smuggling-north-korea.

domain, and a fourth was under Russia's domain. The URL that linked to Sony's servers—the URL in the spe.sony.com domain—indicated that the attackers compromised the network to a degree that allowed them to use Sony's namespace on the public Internet.[16] The attackers claimed to have taken a huge volume—100 terabytes—of data; ultimately, roughly 200 gigabytes was released.[17, 18]

"I used to work for Sony Pictures. My friend still works there and sent this to me. All of Sony has been hacked." 2014

Figure 2. Image Displayed on Computer Monitor at Sony on November 24, 2014 (Imgur)

> [This attack] would have slipped or probably got past 90% of internet defenses that are out there.
>
> *– Joe Demarest, Federal Bureau of Investigation (FBI) Deputy Director*

In the wake of the attack, articles in the press pointed to deficiencies in Sony's cyber security. Elements of the greater Sony Corp., inspired by multiple intrusions into the Sony PlayStation Network in prior years, had been improving the security of their servers; those improvements unfortunately were not adopted at Sony.[19] Sony's lack of security also extended to physical vulnerabilities. On November 3, weeks before the #GOP attack was made public, a team from the threat intelligence firm Norse Corp. claimed that, while waiting to speak with Sony executives, they were able to walk directly into the unlocked and unguarded information security office housing unlocked computers with access to private information on Sony's international network.[20]

Even if Sony exercised best practices for cyber security, the sophistication of the attack may have made its success inevitable. Kevin Mandia, whose company was hired by Sony to lead the internal investigation, said the attack was "an unparalleled and well planned crime, carried out by an organized group, for which neither SPE [Sony] nor other companies could have been fully prepared."[21] While the attack was not as complex as Stuxnet, which relied on four zero-day exploits,[22, 23] it displayed a level of targeting, preparation, and planning beyond the now-common distributed denial-of-service attacks.[24]

[16] Xiphos Research, *A Sony Story: An Examination of the SPE Breach*, December 18, 2014, http://xiphosresearch.com.

[17] Risk Based Security, *A Breakdown and Analysis of the December, 2014 Sony Hack*, December 5, 2014, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/.

[18] Janko Roettgers, "No, the HBO Hack Wasn't Seven Times Bigger Than the Sony Hack," *Variety* (August 4, 2017), http://variety.com/2017/digital/news/hbo-hack-no-sony-hack-1202515967/.

[19] John Gaudiosi, "Why Sony Didn't Learn from Its 2011 Hack," *Fortune* (December 24, 2014), http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

[20] Peter Elkind, "Inside the Hack of the Century. Part 1: Who was manning the ramparts at Sony Pictures?" *Fortune* (June 25, 2015), http://fortune.com/sony-hack-part-1/.

[21] Brent Lang, "Sony Hack 'Unparalleled and Well Planned Crime,' Cyber Security Firm Says," *Variety* (December 6, 2014), http://variety.com/2014/film/news/sony-hack-unparalleled-cyber-security-firm-1201372889/.

[22] David Kushner, "The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program," *IEEE Spectrum* (February 26, 2013), http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[23] A zero-day exploit is a flaw in a code that has not been discovered by the broader community. Due to their complexity, usually these exploits are only the workings of sophisticated state-funded cyber programs.

[24] A "distributed denial of service" attack is an attempt to overload a system by sending numerous requests in parallel.

The attack began with careful preparation well in advance of November 24. According to the post-attack analysis conducted by the FBI, Sony's network was first breached in September 2014. The attackers accessed the Sony network by sending phishing emails to Sony employees and established phony websites to harvest credentials and gain access to Sony systems.[25, 26] From there, the attackers were able to maintain a presence on the Sony network to search for weak points and execute a series of attacks to compromise other systems and steal data.

North Korea's Government

The North Korean ambassador very specifically claimed that *The Interview* was an "act of war" in his letter to the UN. While the language appears preposterous from a US perspective, the claim might not be ridiculous to the North Koreans. In the United States, the government's authority is not tied to the person holding the presidency: a president who responded to satire, of the type in *The Interview*, as an attack on the nation would be ridiculed in the United States. North Korea is not a government founded on principles of authority as understood in the United States. In North Korea, the authority of the Kim family is enshrined in the North Korean constitution.[27] Seen in that light, North Korea's "act of war" statement, equating ridicule aimed at Kim Jong-un to an attack on the nation itself reinforced the principles by which the government asserts its authority over the people.

Stealing data was not the only goal. While attackers bent on espionage try to remain undetected, the #GOP clearly wanted to cause damage. Once Sony's data had been exfiltrated, the attackers modified Sony's computers and servers in a way that maximized disruption. The attack included corruption of the systems' disk drives by removing the low-level information needed for booting up. This destruction served no espionage purpose, nor did it further the extortion demands; such an action appears primarily intended to inflict financial damage on Sony.

> The folks who did this didn't just steal practically everything from the house; they burned the house down.
>
> *– Michael Lynton*

Sony disconnected its network from the Internet as soon as it realized it was compromised. By then, it was too late to stop the most damaging aspects of the attack. Thousands of computers and hundreds of servers were rendered useless.[28] Operations at Sony were significantly hindered in the weeks following the attack, pushing the company back to technologies it could still trust. Modern company smartphones were discarded, and old Blackberries were recovered from storage. The communications networks were shut down entirely. Ancient business practices were also resurrected; paper check cutters were pulled out of storage, and the face-to-face meetings became the norm for information sharing.[29]

Meanwhile, as Sony struggled, the #GOP publically released the exfiltrated data over the ensuing weeks. The #GOP also sent messages to Sony, its employees, and movie theaters. The #GOP communicated either directly via email or posted messages to

[25] David Bisson, "Sony Hackers Used Phishing Emails to Breach Company Networks," *Tripwire* (April 22, 2015), https://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/.

[26] David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," *New York Times* (January 18, 2015), https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?mcubz=1&_r=0.

[27] Heonik Kwon and Byung-Ho Chung, *North Korea: Beyond Charismatic Politics* (Maryland: Rowman & Littlefield Publishers, Inc., 2012).

[28] Peter Elkind, "Inside the Hack of the Century. Part 1: Who was manning the ramparts at Sony Pictures?" *Fortune* (June 25, 2015), http://fortune.com/sony-hack-part-1/.

[29] Associated Press, "Sony CEO Breaks Down Hack Response, Google Role in 'The Interview' Release," *Mercury News* (January 9, 2015, updated August 12, 2016), http://www.mercurynews.com/2015/01/09/sony-ceo-breaks-down-hack-response-google-role-in-the-interview-release/.

websites such as Github and Pastebin.[30, 31] The leaks included yet-unreleased films and scripts, personally identifiable information including social security numbers and employee medical records, and email correspondences highlighting amusing gossip as well as confidential business practices.

Media and Internet Industry Relationships

Some of the released information put longstanding tensions between Hollywood and technology companies back into the spotlight. Perhaps the most significant example of this was from the email leaks between Hollywood studios regarding "Project Goliath," a secret joint legal fund between major film studios to target "Goliath," their codename for Google, for copyright infringement.[32] According to the emails, Project Goliath was designed as a continuation of the failed 2011 Stop Online Piracy Act (SOPA), which was a push by Hollywood companies to hold technology companies responsible for the actions of users who upload copyrighted material.[33] SOPA would have undermined the "safe harbors" provision of the Digital Millennium Copyright Act that protected websites from liability for content held to infringe on copyright.[34] That type of legislation attacks the heart of the business of the technology companies. The technology companies and their allies were successful in defeating SOPA in Congress, but leaked Sony emails showed that the defeat did not put the issue to rest in Hollywood.

Still, the demands at this time were ambiguous; further adding to the confusion, the attack made no connection to North Korea or direct mention of *The Interview*.

The Cyber-Security Industry Responds

> There are strong indications of North Korean involvement.
>
> *– Tom Kellermann*

> I now see this was done by North Korea.
>
> *– Simon Choi*

> In this world, you can fake everything.
>
> *– Jaime Blasco*

> Just weird.
>
> *– Bruce Schneier*

Sony made only guarded statements immediately after the attack but quickly reached out to the cyber-security industry. Sony hired Mandiant (part of FireEye) to investigate the attack.[35] Mandiant and its founder, Kevin Mandia, rose to prominence in 2013 by publishing evidence that the Chinese People's Liberation Army was responsible for a series of cyber attacks that stole hundreds of terabytes of data from over 141 organizations, most of them in the United States.[36] Mandiant, like Sony, did not publicly discuss the ongoing investigation (the earliest example the authors found of Kevin Mandia

[30] Risk Based Security, *A Breakdown and Analysis of the December, 2014 Sony Hack*, December 5, 2014, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/.

[31] Dan Kedmey, "Hackers Reportedly Warn Sony Pictures Not to Release The Interview," *Time* (December 9, 2014), http://time.com/3624994/hackers-sony-the-interview-seth-rogen/.

[32] Russell Brandom, "Project Goliath: Inside Hollywood's Secret War against Google," *Verge* (December 12, 2014), http://www.theverge.com/2014/12/12/7382287/project-goliath.

[33] Julianne Pepitone, "SOPA Explained: What It is and Why It Matters," *CNN Money* (January 20, 2012), http://money.cnn.com/2012/01/17/technology/sopa_explained/.

[34] Lee A. Hollaar, "Copyright of Digital Information," chap. 3 in *Legal Protection of Digital Information*, (Online Version, 2002), http://digital-law-online.info/lpdi1.0/treatise33.html.

[35] Jim Finkle and Ron Grover, "Sony hires Mandiant after cyber attack, FBI starts probe," *Reuters* (November 30, 2014), http://www.reuters.com/article/us-sony-cybersecurity-mandiant/sony-hires-mandiant-after-cyber-attack-fbi-starts-probe-idUSKCN0JE0YA20141201.

[36] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

discussing the case was at Recode's Code Enterprise Series event in April 2015).[37]

Unlike Mandiant, who was directly hired to investigate the attack, many other private cyber-security companies carried out independent investigations and discussed their findings openly. These companies operate within a cyber ecosystem that includes private sector firms and government organizations that find mutual benefit by operating cooperatively. The private sector participants benefit from the publicity that comes with visible engagement in notable cyber events, but the nature of the Internet itself makes it difficult to draw definitive conclusions from observed behavior on the Internet.

Ambiguity is ubiquitous on the Internet. Nearly everything can be manipulated: locations, content, and identities. That makes attribution a common difficulty with cyber attacks, which was no different for the Sony cyber attack. The Internet does not inherently need to trace identities through the network to operate because the interconnections between different operators do not track individual communications sessions, as with telephone calls. Actions by attackers to shroud their identity, combined with misdirection by attention seekers, can complicate attribution. Still, technical means exist to correlate activity with people and organizations.

In the case of Sony, the first credible attributions came from the private-sector, cyber-security firms, building on an established history of investigations of cyber attacks. A sophisticated cyber attack draws on tools and techniques that develop over time and likely have been used before. Based on analysis of past attacks and what was known about the Sony attack, some private-sector security firms attributed the November 24 attack to North Korea as early as the first week of December.[38] The actions of the Sony attackers were similar to those who performed the "DarkSeoul" attack on March 20, 2013, which damaged the networks of South Korean financial systems and television broadcasters.[39, 40, 41]

Two groups, the WhoIs Team and the NewRomanic Cyber Army Team, took credit for the March 2013 attack; security firms concluded that the two are essentially the same group.[42] The computer security industry, represented by companies like TrendMicro, carried out analyses of these attacks and developed a familiarity with the tools and techniques used there (refer to Figure 3).

Similarities between the March 2013 and #GOP attacks were apparent,[43] including the uncommon (at the time) tactic of wiping the system boot records of infected computers (thirty thousand in the March 2013 attack[44] versus about three thousand in

[37] Arik Hesseldahl, "FireEye's Kevin Mandia Talks About the World After the Sony Hack (Full Video)," *Recode* (April 30, 2015), https://www.recode.net/2015/4/30/11562068/fireeyes-kevin-mandia-talks-about-the-world-after-the-sony-hack-full.

[38] Brandon Bailey and Youkyung Lee, "Experts: The Sony Hack Looks A Lot Like Previous Attacks On South Korea," *Business Insider* (December 4, 2014), http://www.businessinsider.com/experts-the-sony-hack-looks-a-lot-like-previous-attacks-on-south-korea-2014-12.

[39] Kim Zetter, "Logic Bomb Set Off South Korea Cyberattack," *Wired* (March 21, 2013), https://www.wired.com/2013/03/logic-bomb-south-korea-attack/.

[40] Brian Krebs, "The Case for N. Korea's Role in Sony Hack," *Krebs on Security* (blog), December 14, 2014, https://krebsonsecurity.com/tag/dark-seoul/.

[41] David M. Martin, *Tracing the Lineage of DarkSeoul*, SANS Institute, 2016, https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787.

[42] Brian Krebs, "The Case for N. Korea's Role in Sony Hack," *Krebs on Security* (blog), December 14, 2014, https://krebsonsecurity.com/tag/dark-seoul/.

[43] Kurt Baumgartner, "Sony/Destover: Mystery North Korean Actor's Destructive and Past Network Activity. Comparisons with Shamoon and DarkSeoul," *Securelist* (December 4, 2014), https://securelist.com/destover/67985/.

[44] Jerin Mathew, "Hacking at Sony has Similarities with Earlier Attacks in Middle East and South Korea," I*nternational Business Times* (December 5, 2014), http://www.ibtimes.co.uk/hacking-sony-has-similarities-earlier-attacks-middle-east-south-korea-1478128.

the #GOP attack).[45] The technical analysis and contemporaneous reporting of statements by unnamed government officials[46] attributed the March 2013 attack to North Korea.

Figure 3. One of the Messages Sent by Whols Team in March 2013[47, 48]

The Cyber-Security Ecosystem

The cyber-security ecosystem includes a combination of private entities and government organizations that play a variety of roles to protect users. Familiar names in cyber security, such as Symantec and FireEye, specialize in protection of user devices and servers by looking for known malware that may be inadvertently downloaded to a user's computer.

Cyber-security firms and the FBI also work to identify new malware. If malicious code is discovered, it is often shared with other companies, usually through a government intermediary such as the FBI or the US Computer Emergency Readiness Team.[49] Individual companies and the FBI then search for identifying characteristics of malicious code and try to find connections to prior attacks. If a company is able to find enough similarities and strong evidence identifying the party responsible for the prior attack, the common attributes of the attack form the basis for attribution of the new attack. Private industry may be motivated to publish the information to hasten public sentiment toward an attribution, while the FBI may want to keep the information private for the sake of building a case for prosecution. Different motivations of private industry and the FBI often result in different courses of action from such attribution.

In addition to the aforementioned organizations that detect malware, Internet service providers such as AT&T and content distribution networks such as Akamai monitor traffic levels across the Internet. These entities are able to identify and take action against certain attacks, such as distributed denial of service.

Cyber-security experts were not all in agreement that North Korea was responsible for the #GOP attack. Some experts agreed that technical analysis pointed toward North Korea but disagreed with the conclusion based on general objections rather than specific claims of insufficient evidence. For example, Jaime Blasco, a cyber-security expert from AlienVault, noted that "you can fake everything" online; cyber-security researcher

[45] Peter Elkind, "Inside the Hack of the Century. Part 1: Who was manning the ramparts at Sony Pictures?" *Fortune* (June 25, 2015), http://fortune.com/sony-hack-part-1/.

[46] Grace Oh, "(2nd LD) N. Korea 'strongly' suspected of masterminding cyber attacks: Seoul official," *YonHap News Agency* (March 21, 2013), http://english.yonhapnews.co.kr/national/2013/03/21/55/0302000000AEN20130321003552315F.HTML.

[47] Kim Zetter, "Logic Bomb Set Off South Korea Cyberattack," *Wired* (March 21, 2013), https://www.wired.com/2013/03/logic-bomb-south-korea-attack/.

[48] Joshua Cannell, "Who is 'Whois'?" *Malwarebytes Labs* (March 26, 2013, last updated March 30, 2016), https://blog.malwarebytes.com/cybercrime/2013/03/who-is-whois/.

[49] "Automated Indicator Sharing (AIS)," US-CERT, U.S. Department of Homeland Security, accessed November 1, 2017, https://www.us-cert.gov/ais.

Bruce Schneier said that North Korea retaliating for a movie was "just weird."[50]

North Korea's Benefit from Attacks from the #GOP and WhoIs Team/NewRomanic Cyber Army Team Attacks

The North Koreans did not appear to receive any financial benefits from either the 2014 attack on Sony or the March 2013 attack on South Korean television broadcasters and financial systems. Rather, these attacks demonstrated their ability to employ asymmetric operations, perhaps as a deterrent. One commentator, Choe Sang-hun from *The New York Times*, went so far as to say that the March 2013 attack was an intentional message from North Korea that it could attack South Korean infrastructure without resorting to traditional warfare.[51] If the North Koreans intended to demonstrate an asymmetric capability, the attacks by WhoIs and the #GOP could be considered successful.

As with any body of evidence, different communities will come to different conclusions based on their experiences and world views. For Schneier, a technical expert, the evidence collected by cyber-security firms was not enough to outweigh his perspective on national security issues. For Blasco, the possible manipulation of technical data layers doubt over the analyses. Ultimately, confidence in attribution will differ among different audiences with varying expertise and perspectives.

The US Government Attributes the Attack to North Korea

> The world will be full of fear. Remember the 11th of September 2001.
>
> *– #GOP, December 16, 2014*

> The FBI announced today and we can confirm that North Korea engaged in this attack.
>
> *– President Obama, December 19, 2014*

The government's engagement escalated once the rhetoric from the attackers became extreme. The #GOP messages through December 15 threatened Sony and its employees; this escalated on December 16 when the #GOP demanded that theaters pull the film, insinuating that theaters refusing to comply should "remember the 11th of September 2001."[52]

The number of theaters planning to show the film dropped precipitously in the days following the #GOP threat of violence. Although the Department of Homeland Security quickly stated that this threat was unfounded,[53] Sony allowed theater chains to pull the film at their discretion, and the five largest chains in North America pulled the film within twenty-four hours.[54] The National Association of Theatre Owners subsequently allowed individual

[50] Brandon Bailey and Youkyung Lee, "Experts: The Sony Hack Looks a Lot Like Previous Attacks on South Korea," *Business Insider* (December 4, 2014), http://www.businessinsider.com/experts-the-sony-hack-looks-a-lot-like-previous-attacks-on-south-korea-2014-12.

[51] Choe Sang Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *New York Times* (March 20, 2013), http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?_r=0.

[52] Kevin Roose, "Sony Pictures Hackers Make Their Biggest Threat Yet: 'Remember the 11th of September 2001,'" *Fusion* (December 16, 2014), http://fusion.net/story/34344/sony-pictures-hackers-make-their-biggest-threat-yet-remember-the-11th-of-september-2001/.

[53] Shelli Weinstein, "No Active Plot against Movie Theaters, Says Department of Homeland Security," *Variety* (December 16, 2014), http://variety.com/2014/film/news/no-active-plot-against-movie-theaters-says-department-of-homeland-security-1201380993/.

[54] Linda Ge, "5 Major Theater Chains Pull 'The Interview' After Sony Hack Threat," *Wrap* (December 17, 2014), https://www.thewrap.com/major-theater-chains-pull-the-interview-after-sony-hack-threat/.

theatres to pull the film,[55] which caused another cascade of cancellations. Around the same time, New Regency studios canceled a nascent project starring Steve Carell, also with a plot involving North Korea.[56]

Before the December 16 threat, the US government said very little publicly about the attack. That changed quickly after the threat of violence. On December 19, in historic statements, both the FBI and the president attributed the attack to North Korea.[57, 58] The president said, "[North Korea] caused a lot of damage, and we will respond. We will respond proportionally, and we'll respond in a place and time and manner that we choose."

The attribution was highly visible but lacked specifics. The FBI issued a press release that spoke to the need to protect sensitive sources and methods. Kevin Mandia later observed that the president's support of FBI attribution was a way to shift the question for the public from "is it North Korea or not?" to "do you believe the president or not?"[59]

The president also expressed his disappointment in Sony for pulling the film from theaters, likening the cyber threat to breaking-and-entering intimidation tactics.[60] Arguably, Sony's decision was already made for them by the many theaters refusing to show the film. The cautious behavior of the private sector is understandable because an attack that injures or kills moviegoers could have potentially far-reaching consequences for the industry. While certainly an understandable response by private industry, succumbing to threats is counter to the government interest in ensuring that the nation does not give in to blackmail. Competing equities are, and will continue to be, a major factor in private sector cooperation with the government.

> I am deeply skeptical of the FBI's announcement.
>
> *– Bruce Schneier, December 22, 2014*

> Despite what I wrote at the time, I now believe that North Korea was responsible for the attack.
>
> *– Bruce Schneier, September 28, 2015*

Confidence in an attribution often requires confidence in the evidence presented as well as a belief that the attributor is credible. Public confidence in the attribution by the FBI and White House was less than complete.[61] Before the attribution, commentary in the press was mixed, and the initial attribution by the government caused some cyber-security experts to lean toward the belief that North Korea was responsible. However, many reputable commentators doubted the credibility of the FBI. The FBI is limited to investigating domestic crimes, which makes questionable any attribution to a foreign state without compelling evidence.

[55] Linda Ge, "Sony Hack: NATO Says Theaters 'May Delay' 'Interview' Release," *Wrap* (December 17, 2014), https://www.thewrap.com/sony-hack-nato-says-theaters-may-delay-interview-release/.

[56] Mike Fleming, Jr., "North Korea-Based Thriller with Gore Verbinski and Steve Carell Canceled," *Deadline* (December 17, 2014), http://deadline.com/2014/12/north-korea-thriller-gore-verbinski-steve-carell-canceled-new-regency-1201328532/.

[57] Barack Obama, "Remarks by the President in Year-End Press Conference," *The White House*, The United States Government (December 19, 2014), https://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

[58] FBI National Press Office, "Update on Sony Investigation," (December 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[59] Arik Hesseldahl, "FireEye's Kevin Mandia Talks about the World after the Sony Hack (Full Video)," *Recode* (April 30, 2015), https://www.recode.net/2015/4/30/11562068/fireeyes-kevin-mandia-talks-about-the-world-after-the-sony-hack-full.

[60] Barack Obama, "Remarks by the President in Year-End Press Conference," *The White House*, The United States Government (December 19, 2014), https://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

[61] Kim Zetter, "Experts are Still Divided on Whether North Korea is Behind Sony Attack," *Wired* (December 23, 2014), https://www.wired.com/2014/12/sony-north-korea-hack-experts-disagree/.

Furthermore, the president's role is ultimately political, and a statement from that office does not necessarily add much *technical* credibility.

Film Released Through Video on Demand and in Theaters

Immediately after the film was pulled from theaters, Sony began to look to release the film as video on demand (VOD). However, many cable, satellite, and digital companies with VOD distribution capabilities rejected the offer out of fear for becoming targets themselves.[62]

Sony eventually struck a deal with Google and Microsoft to release the film as VOD on December 24.[63] Google and Sony came to an agreement mere days after the Project Goliath email was leaked; the conjunction nicely illustrates the shared and competing interests of the entertainment industry and the technology companies.

Between the week spanning Sony's decision to pull *The Interview* and its intended Christmas Day release, roughly three hundred independent theaters ultimately decided to show the film on Christmas Day. Multiple other VOD providers agreed to show the film by New Year's Day. The film was available on Netflix by the end of January 2015. Although the film may have generated more revenue in the absence of the #GOP threats, the film was not a total financial loss, realizing roughly $46 million by January 20 (the film reportedly cost $44 million to make).[64] However, because of the complexity of the attack on Sony, approximate losses to the company would not be known until financial statements were released in the ensuing months.

Multiple commentators also expressed a general distrust of government. The decision to invade Iraq in 2003, which was justified in part by unsupported and ultimately discredited claims that Iraq was about to acquire nuclear weapons, served as a touchstone for those inclined to question the attribution on general principles.[65, 66]

Although it is common practice for the FBI to perform an attribution without releasing sensitive sources and methods, less visible actions were taken concurrently by multiple government organizations to confirm North Korea's involvement. Those actions were acknowledged in later public statements.

In early January 2015, Fordham University hosted an International Conference on Cyber Security, which included keynote speeches by heads of the National Security Council, FBI, and National Security Agency (NSA).[67, 68, 69] The NSA speech was particularly interesting because, until then, the relationship between the intelligence community and law enforcement was not openly discussed.

[62] Associated Press, "Sony CEO breaks down hack response, Google role in 'The Interview' release," *Mercury News* (January 9, 2015), http://www.mercurynews.com/2015/01/09/sony-ceo-breaks-down-hack-response-google-role-in-the-interview-release/.

[63] Ibid.

[64] Adam B. Vary, "'The Interview' Has Made Nearly Seven Times More Online than at the Box Office," *BuzzFeed News* (January 6, 2015, updated on January 20, 2015), https://www.buzzfeed.com/adambvary/the-interview-tops-31-million-in-online-sales?utm_term=.trNK4JXnE#.ybGQM5j3V.

[65] Bruce Schneier, "Did North Korea Really Attack Sony?: It's Too Early to Take the U.S. Government at Its Word," *Atlantic* (December 22, 2014), http://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/.

[66] Steven Bellovin, "Did the DPRK Hack Sony?" *CircleID* (December 19, 2014), http://www.circleid.com/posts/20141219_did_the_dprk_hack_sony/.

[67] ADM Michael S. Rogers, "Special Keynote Address by ADM Michael S. Rogers, Commander, U.S. Cyber Command, Director, National Security Agency, Chief, Central Security Service," (remarks, Fordham University, Fifth International Conference on Cyber Security (ICCS 2015), New York, NY, January 8, 2015), https://www.nsa.gov/news-features/speeches-testimonies/speeches/fordham-transcript.shtml.

[68] James B. Comey, "Addressing the Cyber Security Threat," (speech, Fordham University, International Conference on Cyber Security, New York, NY, January 7, 2015), https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

[69] James R. Clapper, "National Intelligence, North Korea, and the National Cyber Discussion," (remarks, Fordham University, International Conference on Cyber Security, New York, NY, January 7, 2015, https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2015/item/1156-remarks-as-delivered-by-dni-james-r-clapper-on-national-intelligence-north-korea-and-the-national-cyber-discussion-at-the-international-conference-on-cyber-security.

At the conference, Admiral Mike Rogers, head of the NSA, confirmed that the NSA worked closely with the FBI during this investigation:

> *We were asked to provide our technical expertise. We were asked to take a look at the malware. We were asked to take a look at not just the data that was being generated from Sony, but also what data could we bring to the table here. 'Here's other activity and patterns we've observed from this actor over time.'*

The NSA's delay in stating its involvement is understandable. Exposing cyber capabilities can cause targets to implement countermeasures that compromise the capabilities. The NSA revealed its involvement in an investigation that stemmed from an entertainment film, ultimately drawing more attention to some of its capabilities and operations. These releases of information may reduce the NSA's abilities to use the same tools in the future.

The NSA's admission of involvement with the attribution impacted expert opinions of the government's attribution to North Korea. Those technical capabilities give the agency credibility among the technologically savvy. In addition to the on-the-record statements at the International Conference on Cyber Security, *The New York Times* published an article on January 18, in which government sources, many speaking off the record, described how the NSA knew North Korea was behind the attack.[70] The NSA's role as the government's signals intelligence resource gives it tools not available to the FBI. Bruce Schneier was the cyber-security expert who originally said the notion of North Korea's involvement in the attack was "just weird." He was very skeptical about the FBI's attribution to North Korea due to a lack of evidence, and up until just before the Fordham conference, he speculated it could be the work of Russian nationals.[71] He was ultimately convinced that the government attribution was correct after the NSA stepped forward and the subsequent *New York Times* article was published.[72] Schneier's reassessment suggests that, for technical experts, statements made by those with a stronger reputation for technical credibility can carry more weight than those from law enforcement or even the president.

North Korea's Response

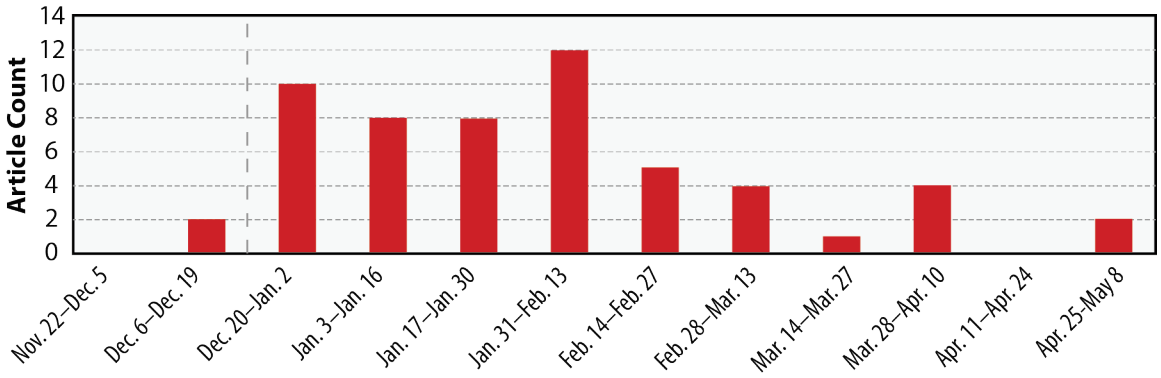
North Korea made *The Interview* a controversy very early and in a very visible way through official statements at the UN on the release of the trailer. To understand North Korea's response to the publicity surrounding the attack and to the attribution by the president, we analyzed news published by North Korean state-controlled media.

The North Korean media comprises state-run television, radio, and print sources. Reporters without Borders ranked North Korea 179th in its 2016 Press Freedom Index, beating out only Eritrea in press freedom. For our purposes, the lack of free press provides a window into the government's reaction to the attribution; any media from the country is likely to be very close to the official stance of the North Korean government. We were unable to find many North Korean video and radio clips during our search. We were, however, able to find print sources through *KCNA Watch*, an "aggregator of official DPRK media output" that displays English translations of news from North Korean media (some North Korean news outlets also publish in

[70] David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks before Sony Attack, Officials Say," *New York Times* (January 18, 2015), http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

[71] Bruce Schneier, "We Still Don't Know Who Hacked Sony: Welcome to the World Where It's Possible to Tell the Difference between Random Hackers and Governments," *Atlantic* (January 5, 2015), http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/.

[72] Bruce Schneier, "Good Article on the Sony Attack," *Schneier on Security* (blog), September 28, 2015, https://www.schneier.com/blog/archives/2015/09/good_article_on.html.



This graph shows all articles between June 2014 and May 2015 in the *KCNA Watch* database that mention "Sony." The first article to mention Sony since the June 11 trailer was on December 7. The dashed line denotes the date of the attribution by the president and the FBI.

Figure 4. Articles about Sony in the North Korean State-Controlled Media

English; *KCNA Watch* collects articles from these sources as well).[73] Figure 4 displays the article counts from these sources. The articles found in the search are listed in the appendix.

Although cyber-security firms attributed the attack to North Korea soon after the November 24 discovery of the attack, the North Korean government's response in the media was limited until after the FBI and President Obama's attribution on December 19. Before the United States attributed the attack to North Korea, the little news from North Korea mainly praised the work of the cyber attackers while denying any involvement.[74, 75] After the US government's attribution, the North Korean media published a flurry of articles defending its innocence and proposing the United States conducts a joint investigation with them[76] (the United States rejected the proposal).[77]

The articles continued well after the attack, inveighing against sanctions and US statements about human rights. The arguments published in the North Korean articles also showed similarities to arguments from US cyber-security experts published in the US media, such as a criticism of the FBI's attribution without evidence and the fact that the attackers could have changed their coding patterns to appear to originate from North Korea.[78, 79]

[73] "About the KCNA databases," KCNAWATCH, accessed November 1, 2017, https://kcnawatch.co/about-the-kcna-databases/.

[74] KCNA.co.jp (English), "Spokesman of Policy Department of NDC Blasts S. Korean Authorities' False Rumor about DPRK," *KCNAWATCH* (July 12, 2014), https://kcnawatch.co/newstream/1451896532-387188787/spokesman-of-policy-department-of-ndc-blasts-s-korean-authorities-false-rumor-about-dprk.

[75] Pyongyang Times, "Injustice invites just reaction," *KCNAWATCH* (October 12, 2014), https://kcnawatch.co/newstream/1450714889-110735967/injustice-invites-just-reaction.

[76] KCNA.kp (En), "DPRK Foreign Ministry Rejects U.S. Accusation against Pyongyang over Cyber Attack,) *KCNAWATCH* (December 20, 2014), https://kcnawatch.co/newstream/1452117603-936205400/dprk-foreign-ministry-rejects-u-s-accusation-against-pyongyang-over-cyber-attack/.

[77] Reuters and Associated Press, "U.S. Rejects North Korean Call for Joint Probe of Hacking Attacks," *RadioFreeEurope Radio Liberty* (December 21, 2014), http://www.rferl.org/a/united-states-north-korea-sony-/26754902.html.

[78] KCNA.kp (En), "DPRK Foreign Ministry Rejects U.S. Accusation against Pyongyang over Cyber Attack," *KCNAWATCH* (December 20, 2014), https://kcnawatch.co/newstream/1452117603-936205400/dprk-foreign-ministry-rejects-u-s-accusation-against-pyongyang-over-cyber-attack/.

[79] KCNA.co.jp (English), "U.S. Urged to Honestly Apologize to Mankind for Its Evil Doing before Groundlessly Pulling up Others," *KCNAWATCH* (December 21, 2014), https://kcnawatch.co/newstream/1451896297-354499225/u-s-urged-to-honestly-

> The U.S. State Secretary is going to justify the production of the movie hurting the dignity of the supreme leadership of a sovereign state while trumpeting about the freedom of expression.
>
> *– KCNA*

North Korea may have been concerned that *The Interview* would inspire its citizens to question the dominance of the Kim family. Despite North Korea's attempted isolation from most of the rest of the world, Western media is frequently smuggled into the country via China and South Korea (see the sidebar titled "North Korea and Black Market Media"). Concerns that *The Interview* would be smuggled into North Korea were soon confirmed; pirated copies of *The Interview* were delivered from China less than two days after the film was released online.[80] In another instance, thousands of copies were sent over using helium balloons.[81]

The Aftermath

> We will respond proportionally, and we'll respond in a place and time and manner that we choose.
>
> *– President Obama, December 19, 2014*

President Obama promised "proportional response," not retaliation in kind. Following a long history of practice in US–North Korea relationships, the United States chose to respond in the economic domain. The government imposed sanctions on January 2, 2015.[82] Critics from varied ideological backgrounds did not view these sanctions as effective. *The New York Times* noted that six decades of sanctions were not able to modify North Korea's behavior, and the Heritage Foundation stated in early 2016 that the sanctions were far reaching but only weakly implemented over the course of a year.

The United States has the ability to engage in sophisticated cyber operations and could have chosen to respond in kind, but it is unclear whether it did. Three days after the December 19 attribution, the Internet in North Korea went out for eight hours.[83, 84] Dyn, an Internet performance management company, described the days leading up to the Internet outage as "a long pattern of up-and-down connectivity, followed by a total outage, [which] seems consistent with a fragile network under external attack."[85] A denial-of-service attack affecting the North Korean network could be executed with modest technical capability. The US government did not admit involvement; State Department Spokeswoman Marie Harf said, "We aren't going to discuss, you know, publicly operational details about the possible response options . . . as we implement our responses, some will be seen, some may not

apologize-to-mankind-for-its-evil-doing-before-groundlessly-pulling-up-others/.

[80] Andy Greenberg, "The Plot to Free North Korea with Smuggled Episodes of 'Friends,'" *Wired* (March 1, 2015), https://www.wired.com/2015/03/north-korea/.

[81] Julian Ryall, "The Interview Sent into North Korea by Balloon," *Telegraph* (April 8, 2015), http://www.telegraph.co.uk/news/worldnews/asia/northkorea/11521640/The-Interview-sent-into-North-Korea-by-balloon.html.

[82] David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea after Sony Case," *New York Times* (January 2, 2015), http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

[83] Cecilia Kang, Drew Harwell, and Brian Fung, "North Korean Web Goes Dark Days after Obama Pledges Response to Sony Hack," *Washington Post* (December 22, 2014), https://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.

[84] Peter Bright, "North Korea Drops Off the Internet in Suspected DDoS Attack," *Ars Technica* (December 22, 2014), http://arstechnica.com/information-technology/2014/12/north-korea-drops-off-the-internet-in-suspected-ddos-attack/.

[85] Jim Cowie, "Someone Disconnects North Korea – Who?" *Dyn* (blog) (December 23, 2014), http://dyn.com/blog/who-disconnected-north-korea/.

be seen."[86] Online hacking groups claimed "credit" for the retaliation against North Korea's Internet.[87] There is also the possibility that the North Korean Internet faced connectivity problems independent of an attack, as it is quite fragile, containing only four networks. (For comparison, Taiwan has 5,030 networks for a similar population.)[88] Dyn also noted that the pattern of the outage was "consistent with more common causes, such as power problems," and the *Washington Post* observed that North Korea suffered roughly fifteen disruptions in connectivity between January 2015 and May 2015.[89] Was the US government involved in the outage? The evidence is inconclusive.

Few options exist for deterring North Korea's bad behavior. Regardless of whether the United States launched a cyber attack on the North Korean Internet, the deterrent value of a retaliation in kind to the Sony attack is dubious; North Korea does not have the same dependence on its cyber assets as other countries. Further, the long history of US actions suggests that economic sanctions do not change North Korea's behavior. The United States reportedly pursued diplomatic efforts, including appeals to China.[90] Each of North Korea's four networks is connected to the Internet through China, which gives China the ability to monitor actions taken by the North Korean government. When shared interests exist, diplomacy can influence in the cyber domain; China's economic espionage has dropped drastically in recent years, which may have partially been due to diplomacy between the US and Chinese governments.[91, 92, 93]

Sony's Financial and Economic Losses

Sony's stated financial losses from the attack were published in its "Consolidated Financial Results for the Fiscal Year Ended March 31, 2015." Sony reported losses of $41 million from the attacks, primarily "related to investigation and remediation expenses relating to a cyber attack on Sony's network and [information technology] infrastructure which was identified in November 2014."[94] For comparison, Sony reported $501 million in operating income on over $8 billion in revenue the previous fiscal year. The $41 million likely only reflects setting up replacement information technology systems; Sony likely incurred other costs to improve

[86] Nicole Perlroth and David E. Sanger, "North Korea Loses Its Link to the Internet," *New York Times* (December 22, 2014), https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

[87] Cecilia Kang, Drew Harwell, and Brian Fung. "North Korean Web Goes Dark Days after Obama Pledges Response to Sony Hack." *Washington Post* (December 22, 2014). https://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.

[88] Jim Cowie, "Someone Disconnects North Korea – Who?" *Dyn* (blog) (December 23, 2014), http://dyn.com/blog/who-disconnected-north-korea/.

[89] Andrea Peterson, "For Most Countries, a Nationwide Internet Outage is a Big Deal. For North Korea, It's Routine," *Washington Post* (May 11, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/05/11/for-most-countries-a-nationwide-internet-outage-is-a-big-deal-for-north-korea-its-routine/.

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

[91] Reuters, "Chinese Economic Cyber-Espionage Plummets in U.S.," *Fortune* (June 20, 2016), http://fortune.com/2016/06/20/chinese-economic-cyber-espionage/.

[92] David Sanger, "Chinese Curb Cyberattacks on U.S. Interests, Report Finds," *New York Times* (June 20, 2016), https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html?_r=0.

[93] FireEye, "Red Line Drawn: China Recalculates its use of cyber espionage," Special Report, June 2016, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

[94] Sony News & Information, "Consolidated Financial Results for the Fiscal Year Ended March 31, 2015," No. 15-039E (April 30, 2015), http://www.sony.net/SonyInfo/IR/library/fr/14q4_sony.pdf.

its security posture. The exposure of personal information exposed Sony to further liabilities; a class-action lawsuit, alleging Sony did not adequately safeguard employee data or immediately notify current and former employees of the attack, was settled by Sony on April 6, 2016.[95, 96] Beyond financial losses, there are also greater economic losses which are difficult to quantify, including lost revenue from leaked films, lost intellectual property, and an increased loss in reputation—exacerbated by WikiLeaks, which made the entire database searchable.

Conclusions

The Sony attack evolved into a whole-of-nation US response against a cyber attack, with participation by the private sector, law enforcement, and the intelligence community. As with any case study, the conclusions developed here provide only a narrow window to understand the broader problems of nation-state actions in cyberspace and the role of cross-domain deterrence, but the lessons shed light on the interplay of the actors in a complicated cyber attack and point to areas for further study.

Divining the Motives of North Korea

The initial reaction by North Korea, a letter to the UN including the phrase "act of war" in response to a satirical film, may seem overblown or even irrational. The North Korean response—a carefully orchestrated cyber attack executed over many months—suggests that the North Koreans took the affront very seriously. While no definitive statement of North Korea's objectives is possible, the events described in this case study suggest two motives for the cyber attack.

First, the attack's destructive nature, damaging to Sony's reputation, its intellectual property, and even further its information technology infrastructure, can be seen as an attempt to inhibit the production of content North Korea deems offensive. While Hollywood is not likely to forego pursuing a profitable path to avoid offending North Korea, the costs of the attack, compounded by the poor financial performance of *The Interview*, should affect the studios' calculus.

Second, the North Korean government has tight but not complete control over the media consumed by its people. The government has a strong interest in maintaining control over its population and over the messages it receives when, as in this case, media portraying a counter-narrative becomes available. Militarily, the nation seeks to present a picture of armed forces arrayed against aggressive world powers who wish harm on the people; culturally, the same picture of a nation under attack furthers the objective to view content like *The Interview* not as creative expression or entertainment but as an assault on the values that define the nation. The UN statement at the beginning of the controversy over *The Interview* and the tenor of the statements from state-controlled media all point to a world hostile to North Korea, thereby serving the government's interest by providing a framing for the film should it be available to its people.

Attribution, Behavior, and Norms

The seminal event of this case study is the unprecedented public attribution of a cyber attack by the president to a foreign power. The attackers did not change their behavior after attributions by the private sector, but they stopped making threats after

[95] Dominic Patten, "Sony Attack: Studio Hit with First Class Action by Ex-Employees," *Deadline* (December 16, 2014), http://deadline.com/2014/12/sony-hack-lawsuit-class-action-ex-employees-1201327046/.

[96] Associated Press, "A judge has approved a multimillion dollar settlement in a class-action lawsuit filed by former Sony Pictures Entertainment employees whose private info was stolen in a massive data breach," *U.S. News and World Report* (April 6, 2016), https://www.usnews.com/news/entertainment/articles/2016-04-06/judge-approves-settlement-in-sony-pictures-hacking-case.

the attribution by the FBI and White House, despite continued public denials by North Korea. At the same time, the North Korean media increased its coverage of Sony and proclaimed its innocence.

Government Statements Do Not Convince Everybody

Some cyber-security experts were still unconvinced by the evidence provided by the government in January 2015. For example, John McAfee thought it was the work of civil libertarians,[97] and Robert Graham thought the US government was hiding something.[98] Interestingly, North Korean media mentioned McAfee as the founder of an "American information security company" who "said that the cyber attack was made by U.S. hackers with liberalist tendency, adding that he knows who did it but will not mention their names and that he could say with confidence that FBI was wrong in spreading the rumor."[99] Critics of an attribution either do not trust the evidence or feel that the evidence does not match their world view. It is important to assess the credibility of critics themselves; some are healthy skeptics who could be convinced with more evidence, while others have a separate agenda inconvenienced by the attribution and will therefore never accept the information.

While it is not possible to say with complete confidence that North Korea changed its behavior in response to the attribution, the experience suggests value in attribution to shape behavior. A coordinated effort across both government and the private sector for routinely attributing actions in cyberspace through techniques recognized as credible could improve adherence to norms and discourage malicious actions in cyberspace.

Attribution, Credibility, and Perceptions

The government is not alone in capability for attribution. The private sector attributed the event to North Korea very soon after the initial attack, demonstrating sophisticated analysis capabilities that were widely, albeit not universally, accepted as a basis for attribution. The evidence-based attributions of private industry, combined with the media reporting on North Korea's potential involvement due to the subject matter of *The Interview*, painted a credible picture that North Korea was involved with the attack. The aggressive engagement of these companies in shaping the public perception of cyber attacks means that public perceptions may be established before the government reveals evidence that is not available to the private sector and may lead to different conclusions.

Law enforcement and intelligence authorities also have a rich capability for attribution, but public statements from the government are unusual; in general, neither law enforcement's nor the intelligence community's interests advanced through public attribution. Law enforcement must protect the integrity of a criminal investigation, and the intelligence community has national security concerns due to the involvement of a foreign government.

In the Sony case, the US government made its rare public attribution after the threat of 9/11-style attacks on movie theaters. This was weeks after numerous private cyber-security firms provided analysis of North Korea's involvement in the cyber attacks. While public opinion was already shaped by the prior private-sector attribution, the government attribution also influenced the perceptions of some commentators in this case. Anecdotal evidence from

[97] David Gilbert and Gareth Platt, "John McAfee: 'I know who hacked Sony Pictures – and it wasn't North Korea,'" *International Business Times* (January 9, 2015), http://www.ibtimes.co.uk/john-mcafee-i-know-who-hacked-sony-pictures-it-wasnt-north-korea-1483581.

[98] Robert Graham, "Drums of Cyberwar: North Korea's Cyber-WMDs," *Errata Security* (blog), January 20, 2015, http://blog.erratasec.com/2015/01/drums-of-cyberwar-north-koreas-cyber.html#.Wihn2IanFhE.

[99] KCNA.kp (En). "Rodong Sinmun Blasts U.S. for Cooking up Story about DPRK's Cyber Attack." *KCNAWATCH* (January 29, 2015). https://kcnawatch.co/newstream/1452116597-438284559/rodong-sinmun-blasts-u-s-for-cooking-up-story-about-dprks-cyber-attack/.

Other Notable Cyber Attacks in US History

In February 2013, Mandiant released a report that attributed numerous cyber attacks worldwide, a vast majority in the United States, to the Chinese People's Liberation Army.[100] In May 2014, the United States filed cyber-espionage charges against five members of the Chinese military. Victims included companies in steel, solar, nuclear power, and specialty metals industries. According to the *Christian Science Monitor*, this indictment was the first the United States filed against a "state actor for economic cyber-theft."[101] However, the US intelligence community did not make any official statements.

In 2016, the Democratic National Committee fell victim to cyber attacks that exfiltrated tens of thousands of emails. The United States attributed this attack to Russian hackers. Rather than the FBI announcing an attribution, which was the case for the Sony attack, the announcement was made by the Department of Homeland Security and James Clapper, the director of national intelligence.[102]

Although the Chinese, Russian, and North Korean cyber attacks caused considerable problems for the US government, the motivations of these attacks appeared to differ. The Chinese attacks were performed to access trade secrets, while the North Korean and Russian attacks were related to influence operations. The North Korean attack hindered the release of films that cast the country in a bad light, while the Russian attack impacted elections.

Cyber attacks on US entities by nation-states are likely to continue in the future in the form of financial as well as influence operations. It is important to establish cyberspace norms to better clarify acceptable behavior.

this case study suggests that informed commentators looked critically on the source of the attribution and the evidence presented before accepting an attribution. If the government seeks to influence public opinion by attributing actions in cyberspace, the attribution needs to be credible. While the evidence from this single case study is limited, the intelligence community's public statements demonstrated an ability to influence opinion.

Information Sharing and Denial of Benefits

The Sony intrusion began months before becoming visible, and the damage from the attack could have been mitigated with earlier response actions by Sony. Through the course of the attack, very little evidence surfaced of government efforts to aid Sony directly and thereby deny benefits to North Korea. According to *The New York Times*, the NSA was watching the North Korean networks years before the cyber attack began. It is possible the NSA was aware of the attack on Sony long before it became public on November 24, based on its intelligence-gathering function. Under current law and policy, there would have been no justification to share that information with Sony. As noted earlier, the intelligence community has valid national security concerns and limits on how information can be used. Still, the events in this case raise an issue on effective whole-of-nation response to a cyber attack. While in the Sony case, the lack of information sharing did not lead to damage that represented a serious threat to national security, other private-sector assets comprising the nation's critical infrastructure can be a pressing issue for the federal government. More timely information sharing could have prevented damage to Sony; a future attack, of much greater significance, may be prevented through effective information sharing.

[100] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[101] Mark Clayton, "US Indicts Five in China's Secret 'Unit 61398' for Cyber-Spying on US Firms (+video)," *Christian Science Monitor* (May 19, 2014), http://www.csmonitor.com/World/Passcode/2014/0519/US-indicts-five-in-China-s-secret-Unit-61398-for-cyber-spying-on-US-firms-video.

[102] Ellen Nakashima, "U.S. Government Officially Accuses Russia of Hacking Campaign to Interfere with Elections," *Washington Post* (October 7, 2016), https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html.

As pointed out in many studies, including a study of intelligence information sharing by the National Infrastructure Advisory Council,[103] "Information sharing is perhaps the most important factor in the protection and resilience of critical infrastructure." This case study shows that effective response to a cyber attack can require significant coordination by different entities across the public and private sectors, highlighting the importance of a whole-of-nation response to sophisticated adversaries. While limited in significance compared to an attack on critical infrastructure, the Sony attack illustrates some of the challenges inherent in a multi-domain response to a sophisticated attack. National policy needs to lay out an effective means to respond in a more coordinated fashion across different government entities operating under different authorities. Policy, practices, and norms also need to evolve for more effective cooperation between the government and private sectors.

[103] Alfred R. Berkeley, III, Wesley Bush, Philip G. Heasley, James B. Nicholson, James A. Reid, and Michael J. Wallace, "National Infrastructure Advisory Council Intelligence Information Sharing: Final Report and Recommendations," U.S. Department of Homeland Security (January 10, 2012), https://www.dhs.gov/publication/niac-intel-info-sharing-final-report.

Appendix North Korea Articles

The following articles result from a search for the phrase "Sony" in the *KCNA Watch* database, a news aggregator containing English-translated (and English-language) articles from North Korean news sources (*KCNA Watch* is part of *NK Pro*, and the articles are behind a soft paywall).

Table A-1. Articles Including "Sony" in the *KCNA Watch* Database, June 1, 2014–May 5, 2015

Date		Source	Title
2014	Dec. 7	*KCNA*	Spokesman of Policy Department of NDC Blasts S. Korean Authorities' False Rumor about DPRK
	Dec. 10	*Pyongyang Times*	Injustice invites just reaction
	Dec. 20	*KCNA*	DPRK Foreign Ministry Rejects U.S. Accusation against Pyongyang over Cyber Attack
	Dec. 21	*KCNA*	U.S. Urged to Honestly Apologize to Mankind for Its Evil Doing before Groundlessly Pulling up Others
	Dec. 24	*Pyongyang Times*	DPRK NDC hits back at US' anti-DPRK conspiracy theory
	Dec. 25	*KCNA*	U.S. Human Rights Abuses Disclosed by Korean Media in U.S.
	Dec. 27	*KCNA*	Minju Joson Denounces S. Korean Authorities' Plot to Cook up Hideous Case
	Dec. 27	*KCNA*	U.S. Accused of Blaming DPRK for Cyber Attack
	Dec. 27	*KCNA*	U.S. Can Never Justify Screening and Distribution of Reactionary Movie: Policy Department of NDC of DPRK
	Dec. 28	*KCNA*	Rodong Sinmun Refutes S. Korean Puppet Authorities' Anti-DPRK Accusations
	Dec. 30	*Pyongyang Times*	NDC spokesman lambasts move to redistribute smear film
	Dec. 30	*KCNA*	Sony Pictures Entertainment Incident Is Misfortune Caused by U.S. Itself: Minju Joson
2015	Jan. 4	*KCNA*	DPRK FM Spokesman Slams U.S. for "New Sanctions"
	Jan. 6	*Pyongyang Times*	FM spokesman: Sanctions to backfire
	Jan. 12	*KCNA*	U.S. Sanctions against DPRK Denounced by S. Korean Organization
	Jan. 12	*KCNA*	U.S. Announcement of "Presidential Executive Order" against DPRK Denounced by British Organizations
	Jan. 12	*KCNA*	US "Presidential Executive Order" Denounced By British Organizations
	Jan. 15	*KCNA*	Statement of NDC Policy Department of DPRK Supported by British Organizations
	Jan. 16	*Rodong Sinmun*	Statement of NDC Policy Department of DPRK Supported by British Organizations
	Jan. 16	*KCNA*	South Koreans Condemn U.S. Sanctions against DPRK
	Jan. 17	*Rodong Sinmun*	South Koreans Condemn U.S. Sanctions against DPRK
	Jan. 20	*KCNA*	U.S. Is Chiefly to Blame for Disturbing Security of Cyber Space: KCNA
	Jan. 21	*Pyongyang Times*	Additional sanctions what for?
	Jan. 21	*KCNA*	S. Korean Organization Denounces U.S. for Fanning up Anti-DPRK Leaflet Scattering
	Jan. 22	*KCNA*	U.S. Is Arch Criminal of Harassing Peace on Korean Peninsula: DPRK Scholar
	Jan. 23	*Pyongyang Times*	Destroyer of cyberspace security
	Jan. 29	*KCNA*	Rodong Sinmun Blasts U.S. for Cooking up Story about DPRK's Cyber Attack
	Jan. 30	*Rodong Sinmun*	U.S. Should Not Cook up Story about DPRK's Cyber Attack
	Jan. 31	*KCNA*	U.S. under Fire in S. Korea for Putting Brake on Improvement of Inter-Korean Relations
	Jan. 31	*KCNA*	KCNA Commentary Accuses U.S. of Hacking at DPRK's Computer System

(continued)

Table A-1. ***(Continued)***

Date		Source	Title
2015	Feb. 1	*KCNA*	DPRK's Access to Nukes Is Product of U.S. Hostile Policy toward It: Russian Expert
	Feb. 2	*Rodong Sinmun*	U.S. under Fire in S. Korea for Putting Brake on Improvement of Inter-Korean Relations
	Feb. 4	*KCNA*	U.S. Imperialists Will Face Final Doom: DPRK NDC
	Feb. 5	*Rodong Sinmun*	U.S. Imperialists Will Face Final Doom: DPRK NDC
	Feb. 7	*KCNA*	CPRK Spokesman Blasts Provocative Remarks of S. Korean Chief Executive
	Feb. 8	*KCNA*	U.S. Criminal Acts of Blocking Improvement of North-South Ties and Reunification of Korea Indicted
	Feb. 9	*Rodong Sinmun*	CPRK Spokesman Blasts Provocative Remarks of S. Korean Chief Executive
	Feb. 10	*Rodong Sinmun*	U.S. Criminal Acts of Blocking Improvement of North-South
	Feb. 10	*KCNA*	U.S. Is Bound to Face Final Doom: Minju Joson
	Feb. 12	*Pyongyang Times*	US indicted for crimes against inter-Korean relations and reunion
	Feb. 15	*KCNA*	U.S. Cyber Strategy Assailed
	Feb. 19	*KCNA*	Korean in Russia Supports Statement of DPRK NDC
	Feb. 21	*Pyongyang Times*	S. Korean authorities urged to drop double-facedness
	Feb. 24	*KCNA*	Minju Joson Slams S. Korean Authorities for Trumpeting about "Dialogue"
	Feb. 27	*KCNA*	U.S. Accused of Mounting First State-sponsored Cyber Attack
	Feb. 28	*Rodong Sinmun*	U.S., Chieftain of First State-sponsored Cyber Attack
	Mar. 2	*KCNA*	Minju Joson Discloses U.S. Ultimate Purpose in Spreading "Theory of N. Korea's Hacking" on Its Company
	Mar. 3	*KCNA*	U.S. "Human Rights" Racket against DPRK and Tortures in Various Parts of World Slammed
	Mar. 11	*Pyongyang Times*	White paper lays bare US' human rights abuses
	Mar. 19	*Pyongyang Times*	Reasonable thinking needed
	Mar. 28	*KCNA*	U.S. Harsh Sanctions against DPRK Will Entail Catastrophic Consequences: Rodong Sinmun
	Mar. 30	*Rodong Sinmun*	U.S. Harsh Sanctions against DPRK Will Entail Catastrophic Consequences
	Mar. 31	*Uriminzokkiri*	US Harsh Sanctions against DPRK Will Entail Catastrophic Consequences
	Apr. 2	*KCNA*	KCNA Commentary Terms U.S. Worst Cyber Attacker
	May 1	*KCNA*	KCNA Commentary Accuses U.S. of Working Hard to Re-list DPRK as "Sponsor of Terrorism"
	May 5	*KCNA*	KCNA Commentary Denounces U.S. Anti-DPRK "Human Rights" Racket

Bibliography

"About the KCNA databases." *KCNAWATCH*. Accessed November 1, 2017, https://kcnawatch.co/about-the-kcna-databases/.

Arce, Nicole. "Sony was Warned of Impending Cyber Attack in Extortion Email, Reveal Leaked Messages from Inboxes of Top Executives." *Tech Times* (December 9, 2014). http://www.techtimes.com/articles/21770/20141209/sony-was-warned-of-impending-cybertattack-in-extortion-email-leaked-email-boxes-of-top-executives-reveal.htm.

Associated Press. "A judge has approved a multimillion dollar settlement in a class-action lawsuit filed by former Sony Pictures Entertainment employees whose private info was stolen in a massive data breach." *U.S. News and World Report* (April 6, 2016). https://www.usnews.com/news/entertainment/articles/2016-04-06/judge-approves-settlement-in-sony-pictures-hacking-case.

Associated Press. "Sony CEO Breaks Down Hack Response, Google Role in 'The Interview' Release." *Mercury News* (January 9, 2015, updated August 12, 2016). http://www.mercurynews.com/2015/01/09/sony-ceo-breaks-down-hack-response-google-role-in-the-interview-release/.

"Automated Indicator Sharing (AIS)." US-CERT, U.S. Department of Homeland Security. Accessed November 1, 2017. https://www.us-cert.gov/ais.

Berkeley, III, Alfred R., Wesley Bush, Philip G. Heasley, James B. Nicholson, James A. Reid, and Michael J. Wallace. *National Infrastructure Advisory Council Intelligence Information Sharing: Final Report and Recommendations*. U.S. Department of Homeland Security. January 10, 2012. https://www.dhs.gov/publication/niac-intel-info-sharing-final-report.

Bailey, Brandon, and Youkyung Lee. "Experts: The Sony Hack Looks A Lot Like Previous Attacks On South Korea." *Business Insider* (December 4, 2014). http://www.businessinsider.com/experts-the-sony-hack-looks-a-lot-like-previous-attacks-on-south-korea-2014-12.

Baumgartner, Kurt. "Sony/Destover: Mystery North Korean Actor's Destructive and Past Network Activity. Comparisons with Shamoon and DarkSeoul." *Securelist* (December 4, 2014). https://securelist.com/destover/67985/.

Bellovin, Steven. "Did the DPRK Hack Sony?" *CircleID* (December 19, 2014). http://www.circleid.com/posts/20141219_did_the_dprk_hack_sony/.

Bisson, David. "Sony Hackers Used Phishing Emails to Breach Company Networks." *Tripwire* (April 22, 2015). https://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/.

Brandom, Russell. "Project Goliath: Inside Hollywood's Secret War against Google." *Verge* (December 12, 2014). http://www.theverge.com/2014/12/12/7382287/project-goliath.

Bright, Peter. "North Korea Drops Off the Internet in Suspected DDoS Attack." *Ars Technica* (December 22, 2014). http://arstechnica.com/information-technology/2014/12/north-korea-drops-off-the-internet-in-suspected-ddos-attack/.

Cannell, Joshua. "Who is 'Whois'?" *Malwarebytes Labs* (March 26, 2013, last updated March 30, 2016). https://blog.malwarebytes.com/cybercrime/2013/03/who-is-whois/.

Clapper, James R. "National Intelligence, North Korea, and the National Cyber Discussion." (Remarks, Fordham University, International Conference on Cyber Security, New York, NY, January 7, 2015. https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2015/item/1156-remarks-as-delivered-by-dni-james-r-clapper-on-national-intelligence-north-korea-and-the-national-cyber-discussion-at-the-international-conference-on-cyber-security.

Clayton, Mark. "US Indicts Five in China's Secret 'Unit 61398' for Cyber-Spying on US Firms (+video)." *Christian Science Monitor* (May 19, 2014). http://www.csmonitor.com/World/Passcode/2014/0519/US-indicts-five-in-China-s-secret-Unit-61398-for-cyber-spying-on-US-firms-video.

Comey, James B. "Addressing the Cyber Security Threat." (Speech, Fordham University, International Conference on Cyber Security, New York, NY, January 7, 2015). https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

Cowie, Jim. "Someone Disconnects North Korea – Who?" *Dyn* (blog), Oracle, December 23, 2014. http://dyn.com/blog/who-disconnected-north-korea/.

DoD Defense Science Board. T*ask Force Report: Resilient Military Systems and the Advanced Cyber Threat*. January 2013. http://www.dtic.mil/docs/citations/ADA569975.

Elkind, Peter. "Inside the Hack of the Century. Part 1: Who was manning the ramparts at Sony Pictures?" *Fortune* (June 25, 2015). http://fortune.com/sony-hack-part-1/.

Elkind, Peter. "Inside the Hack of the Century. Part 2: The storm builds." *Fortune* (June 26, 2015). http://fortune.com/sony-hack-part-two/.

FBI National Press Office. "Update on Sony Investigation." (December 19, 2014). https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

Finkle, Jim, and Ron Grover. "Sony hires Mandiant after cyber attack, FBI starts probe." *Reuters* (November 30, 2014). http://www.reuters.com/article/us-sony-cybersecurity-mandiant/sony-hires-mandiant-after-cyber-attack-fbi-starts-probe-idUSKCN0JE0YA20141201.

FireEye. "Red Line Drawn: China Recalculates its use of cyber espionage." Special Report, June 2016. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Fleming, Jr., Mike. "North Korea-Based Thriller with Gore Verbinski and Steve Carell Canceled." *Deadline* (December 17, 2014). http://deadline.com/2014/12/north-korea-thriller-gore-verbinski-steve-carell-canceled-new-regency-1201328532/.

Franceschi-Bicchierai, Lorenzo, and Christina Warren. "Hackers Sent Extortion Email to Sony Executives 3 Days Before Attack." *Mashable* (December 8, 2014). http://mashable.com/2014/12/08/hackers-emailed-sony-execs/.

Gaudiosi, John. "Why Sony Didn't Learn from Its 2011 Hack." *Fortune* (December 24, 2014). http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

Ge, Linda. "5 Major Theater Chains Pull 'The Interview' After Sony Hack Threat." *Wrap* (December 17, 2014). https://www.thewrap.com/major-theater-chains-pull-the-interview-after-sony-hack-threat/.

Ge, Linda. "Sony Hack: NATO Says Theaters 'May Delay' 'Interview' Release." *Wrap* (December 17, 2014). https://www.thewrap.com/sony-hack-nato-says-theaters-may-delay-interview-release/.

Gibbs, Samuel. "Sony Hack Would Have Challenged Government Defences – FBI." *Guardian* (December 12, 2014). https://www.theguardian.com/technology/2014/dec/12/sony-hack-government-defences-fbi.

Gilbert, David, and Gareth Platt. "John McAfee: 'I know who hacked Sony Pictures – and it wasn't North Korea.'" *International Business Times* (January 9, 2015). http://www.ibtimes.co.uk/john-mcafee-i-know-who-hacked-sony-pictures-it-wasnt-north-korea-1483581.

Graham, Robert. "Drums of Cyberwar: North Korea's Cyber-WMDs." *Errata Security* (blog), January 20, 2015. http://blog.erratasec.com/2015/01/drums-of-cyberwar-north-koreas-cyber.html#.Wihn2IanFhE.

Greenberg, Andy. "The Plot to Free North Korea with Smuggled Episodes of 'Friends.'" *Wired* (March 1, 2015). https://www.wired.com/2015/03/north-korea/.

Hesseldahl, Arik. "FireEyes's Kevin Mandia Talks About the World After the Sony Hack (Full Video)." *Recode* (April 30, 2015). https://www.recode.net/2015/4/30/11562068/fireeyes-kevin-mandia-talks-about-the-world-after-the-sony-hack-full.

Hollaar, Lee A. "Copyright of Digital Information." Chap. 3 in *Legal Protection of Digital Information*. Online Version, 2002. http://digital-law-online.info/lpdi1.0/treatise33.html.

Hughes, Jason. "James Franco and Seth Rogen Are Going to Take Out Kim Jong-Un in 'The Interview' Trailer (Video)." *Wrap* (June 11, 2014). https://www.thewrap.com/seth-rogen-and-james-franco-are-going-to-take-out-kim-jong-un-in-the-interview-trailer-video/.

Hun, Choe Sang. "Computer Networks in South Korea Are Paralyzed in Cyberattacks." *New York Times* (March 20, 2013). http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?_r=0.

Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton." *Harvard Business Review* (July–August 2015). https://hbr.org/2015/07/they-burned-the-house-down.

Imgur. "I used to work for Sony Pictures. My friend still works there and sent this to me. All of Sony has been hacked," *Imgur* (image-sharing site), November 24, 2014. https://imgur.com/qXNgFVz.

Kang, Cecilia, Drew Harwell, and Brian Fung. "North Korean Web Goes Dark Days after Obama Pledges Response to Sony Hack." *Washington Post* (December 22, 2014). https://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.

KCNA.kp (En). "DPRK Foreign Ministry Rejects U.S. Accusation against Pyongyang over Cyber Attack." *KCNAWATCH* (December 20, 2014). https://kcnawatch.co/newstream/1452117603-936205400/dprk-foreign-ministry-rejects-u-s-accusation-against-pyongyang-over-cyber-attack/.

KCNA.kp (En). "Rodong Sinmun Blasts U.S. for Cooking up Story about DPRK's Cyber Attack." *KCNAWATCH* (January 29, 2015). https://kcnawatch.co/newstream/1452116597-438284559/rodong-sinmun-blasts-u-s-for-cooking-up-story-about-dprks-cyber-attack/.

KCNA.co.jp (English). "Spokesman of Policy Department of NDC Blasts S. Korean Authorities' False Rumor about DPRK." *KCNAWATCH* (December 7, 2014). https://kcnawatch.co/newstream/1451896532-387188787/spokesman-of-policy-department-of-ndc-blasts-s-korean-authorities-false-rumor-about-dprk.

KCNA.co.jp (English). "U.S. Urged to Honestly Apologize to Mankind for Its Evil Doing before Groundlessly Pulling up Others." *KCNAWATCH* (December 21, 2014). https://kcnawatch.co/newstream/1451896297-354499225/u-s-urged-to-honestly-apologize-to-mankind-for-its-evil-doing-before-groundlessly-pulling-up-others/.

Kedmey, Dan. "Hackers Reportedly Warn Sony Pictures Not to Release The Interview." *Time* (December 9, 2014). http://time.com/3624994/hackers-sony-the-interview-seth-rogen/.

Krebs, Brian. "The Case for N. Korea's Role in Sony Hack." *Krebs on Security* (blog), December 14, 2014. https://krebsonsecurity.com/tag/dark-seoul/.

Kushner, David. "The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program." *IEEE Spectrum* (February 26, 2013). http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Kwon, Heonik, and Byung-Ho Chung. *North Korea: Beyond Charismatic Politics*. Maryland: Rowman & Littlefield Publishers, Inc. 2012.

Lang, Brent. "Sony Hack 'Unparalleled and Well Planned Crime,' Cyber Security Firm Says." *Variety* (December 6, 2014). http://variety.com/2014/film/news/sony-hack-unparalleled-cyber-security-firm-1201372889/.

Mandiant. *APT1: Exposing One of China's Cyber Espionage Units*. 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Martin, David M. *Tracing the Lineage of DarkSeoul*. SANS Institute, 2016, https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787.

Mathew, Jerin. "Hacking at Sony has Similarities with Earlier Attacks in Middle East and South Korea." *International Business Times* (December 5, 2014). http://www.ibtimes.co.uk/hacking-sony-has-similarities-earlier-attacks-middle-east-south-korea-1478128.

Nakashima, Ellen. "U.S. Government Officially Accuses Russia of Hacking Campaign to Interfere with Elections." *Washington Post* (October 7, 2016). https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html.

News Desk. "How Media Smuggling Took Hold in North Korea." *PBS News Hour* (December 18, 2016). https://www.pbs.org/newshour/world/media-smuggling-north-korea.

Obama, Barack. "Remarks by the President in Year-End Press Conference." *The White House*, The United States Government (December 19, 2014). https://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

Oh, Grace. "(2nd LD) N. Korea 'strongly' suspected of masterminding cyber attacks: Seoul official." *YonHap News Agency* (March 21, 2013). http://english.yonhapnews.co.kr/national/2013/03/21/55/0302000000AEN20130321003552315F.HTML.

Patten, Dominic. "Sony Attack: Studio Hit with First Class Action by Ex-Employees." *Deadline* (December 16, 2014). http://deadline.com/2014/12/sony-hack-lawsuit-class-action-ex-employees-1201327046/.

Pepitone, Julianne. "SOPA Explained: What It is and Why It Matters." *CNN Money* (January 20, 2012). http://money.cnn.com/2012/01/17/technology/sopa_explained/.

Perlroth, Nicole, and David E. Sanger. "North Korea Loses Its Link to the Internet." *New York Times* (December 22, 2014). https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

Peterson, Andrea. "For Most Countries, a Nationwide Internet Outage is a Big Deal. For North Korea, It's Routine." *Washington Post* (May 11, 2015). https://www.washingtonpost.com/news/the-switch/wp/2015/05/11/for-most-countries-a-nationwide-internet-outage-is-a-big-deal-for-north-korea-its-routine/.

Peterson, Andrea. "Sony Pictures Hackers Invoke 9/11 While Threatening Theaters that Show 'The Interview.'" *Washington Post* (December 16, 2014). https://www.washingtonpost.com/news/the-switch/wp/2014/12/16/sony-pictures-hackers-invoke-911-while-threatening-theaters-that-show-the-interview/?utm_term=.58ccf6e899df.

Pyongyang Times. "Injustice invites just reaction." *KCNAWATCH* (October 12, 2014). https://kcnawatch.co/newstream/1450714889-110735967/injustice-invites-just-reaction.

Reuters. "Chinese Economic Cyber-Espionage Plummets in U.S." *Fortune* (June 20, 2016). http://fortune.com/2016/06/20/chinese-economic-cyber-espionage/.

Reuters and Associated Press. "U.S. Rejects North Korean Call for Joint Probe of Hacking Attacks." *RadioFreeEurope Radio Liberty* (December 21, 2014). http://www.rferl.org/a/united-states-north-korea-sony-/26754902.html.

Risk Based Security. *A Breakdown and Analysis of the December, 2014 Sony Hack*. December 5, 2014. https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/.

Roettgers, Janko. "No, the HBO Hack Wasn't Seven Times Bigger Than the Sony Hack." *Variety* (August 4, 2017). http://variety.com/2017/digital/news/hbo-hack-no-sony-hack-1202515967/.

Rogers, ADM Michael S. "Special Keynote Address by ADM Michael S. Rogers, Commander, U.S. Cyber Command, Director, National Security Agency, Chief, Central Security Service." (Remarks, Fordham University, Fifth International Conference on Cyber Security (ICCS 2015), New York, NY, January 8, 2015). https://www.nsa.gov/news-features/speeches-testimonies/speeches/fordham-transcript.shtml.

Roose, Kevin. "Sony Pictures Hackers Make Their Biggest Threat Yet: 'Remember the 11th of September 2001.'" *Fusion* (December 16, 2014). http://fusion.net/story/34344/sony-pictures-hackers-make-their-biggest-threat-yet-remember-the-11th-of-september-2001/.

Ryall, Julian. "The Interview Sent into North Korea by Balloon." *Telegraph* (April 8, 2015). http://www.telegraph.co.uk/news/worldnews/asia/northkorea/11521640/The-Interview-sent-into-North-Korea-by-balloon.html.

Sanger, David. "Chinese Curb Cyberattacks on U.S. Interests, Report Finds." *New York Times* (June 20, 2016). https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html?_r=0.

Sanger, David E., and Martin Fackler. "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say." *New York Times* (January 18, 2015). https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?mcubz=1&_r=0.

Sanger, David E., and Michael S. Schmidt. "More Sanctions on North Korea after Sony Case." *New York Times* (January 2, 2015). http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

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

Schneier, Bruce. "Did North Korea Really Attack Sony?: It's Too Early to Take the U.S. Government at Its Word." *Atlantic* (December 22, 2014). http://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/.

Schneier, Bruce. "Good Article on the Sony Attack." *Schneier on Security* (blog), September 28, 2015. https://www.schneier.com/blog/archives/2015/09/good_article_on.html.

Schneier, Bruce. "We Still Don't Know Who Hacked Sony: Welcome to the World Where It's Possible to Tell the Difference between Random Hackers and Governments." *Atlantic* (January 5, 2015). http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/.

Seal, Mark. "An Exclusive Look at Sony's Hacking Saga." *Vanity Fair* (March 2015). https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

Sony News & Information. "Consolidated Financial Results for the Fiscal Year Ended March 31, 2015." No. 15-039E (April 30, 2015). http://www.sony.net/SonyInfo/IR/library/fr/14q4_sony.pdf.

Symantec. *2016 Internet Security Threat Report*. 21. https://www.symantec.com/content/dam/symantec/docs/security-center/archives/istr-16-april-volume-21-en.pdf.

United Nations, General Assembly Security Council. Letter dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations addressed to the Secretary-General. A/68/934–S/2014/451, June 27, 2014.

Vary, Adam B. "'The Interview' Has Made Nearly Seven Times More Online than at the Box Office." *BuzzFeed News* (January 6, 2015, updated on January 20, 2015). https://www.buzzfeed.com/adambvary/the-interview-tops-31-million-in-online-sales.

Weinstein, Shelli. "No Active Plot against Movie Theaters, Says Department of Homeland Security." *Variety* (December 16, 2014). http://variety.com/2014/film/news/no-active-plot-against-movie-theaters-says-department-of-homeland-security-1201380993/.

Xiphos Research. *A Sony Story: An Examination of the SPE Breach*. December 18, 2014. http://xiphosresearch.com.

Zetter, Kim. "Experts are Still Divided on Whether North Korea is Behind Sony Attack." *Wired* (December 23, 2014). https://www.wired.com/2014/12/sony-north-korea-hack-experts-disagree/.

Zetter, Kim. "Logic Bomb Set Off South Korea Cyberattack." *Wired* (March 21, 2013). https://www.wired.com/2013/03/logic-bomb-south-korea-attack/.

Acknowledgments

The authors extend their appreciation to the following individuals for their support of this project: Jill Newton, Jeff Dunne, Robert Nichols, Ian MacLeod, Muayyad Al-Chalabi, and Erin Hahn for study review and James Scouras for general study synthesis, review, and guidance.

About the Authors

Dr. Antonio DeSimone is the Chief Scientist for Communications Systems at the Johns Hopkins University Applied Physics Laboratory (JHU/APL) and the principal technical leader of JHU/APL's efforts in national and nuclear command and control communications. Prior to joining JHU/APL, Dr. DeSimone held senior management positions in Lucent's Optical Networking Unit and Lucent Digital Video. At AT&T WorldNet, he led pioneering research and development efforts in Internet services. He started his career at Bell Laboratories, where he worked in network design, performance analysis, network and computer security, and wireless networking. Dr. DeSimone holds ten patents in data networking, web caching, and related technologies, and he has authored numerous technical publications. He earned a Ph.D. and Sc.M. from Brown University and a B.S. from Rensselaer Polytechnic Institute, all in Physics.

Dr. Nicholas Horton is a National Security Analyst at JHU/APL. While at JHU/APL, he has worked on a variety of projects involving national security and national health. Dr. Horton earned a Ph.D. and M.S. in Applied Physics from Cornell University and B.S. in Physics from Rollins College.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY