EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

Cyber Chutzpah: The Sony Hack and the Celebration of Hyperbole

Hal Berghel, University of Nevada, Las Vegas

There's nothing about the recent Sony hack that withstands close scrutiny. The story began as bunk, took a spin around blather and hooey, and then seems to have come to rest on drivel.

I've restrained myself from commenting on the Sony hack until now. This entire story has been stuck on stupid, but after Sony CEO Kazuo Hirai's underwhelming talk at the 2015 Consumer Electronics Show in Las Vegas (my fair city), I can hold back no more. It's time to pull what little common sense is left of this story out of the Orwellian memory hole and try to get the narrative back on track.

Hirai said, "[Sony employees] were unfortunately the victims of one of the most vicious and malicious cyberattacks that we've known certainly in recent history .... And I have to say that freedom of speech, freedom of expression, freedom of association, those are [the] very important lifeblood—lifelines—of Sony and our entertainment business" (http://time.com/3655462/sony-chief-executive-hacking). This is hyperbole and drama befitting a Mickey Spillane novel—the Sony hack is *not* in the upper echelon of cyberattacks! It's not even in the second or third tiers. As a matter of fact, apart from the embarrassing executive emails that were leaked, it's not even very interesting.

Furthermore, if Sony really believed in freedom of expression, it wouldn't have fired its corporate communications executive Charles Sipkins over an alleged snub of cochairman Amy Pascal (www.rttnews.com/2430666/sony-executive-leaves-after-e-mail-reportedly-sought-his-firing.aspx). Sony's corporate stance on this offends the senses.

In the grand scheme of things, the Sony hack seems to be a rather pedestrian compromise of a security-challenged computer network. Examples of "vicious and malicious cyberattacks" are easy to find: consider the Trojan horse software hack by the US that led to the 1983 Trans-Siberian Pipeline explosion—reportedly the largest non-nuclear explosion in recorded history.[1] Now *that's* vicious and malicious.

Or, one might point to the Operation Olympic Games attack that used the Stuxnet worm to destroy uranium centrifuges at an Iranian fuel enrichment facility (www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html). Once again, this qualifies as a vicious and malicious cyberattack. Since both of these examples involve cyberkinetic attacks on sovereign nations, they remain politically charged, so we'll pass over the geopolitical motives in silence.

For something to qualify as vicious and malicious, an action must have consequences that are savage, brutish,

violent, or fatal. Detestable and spiteful conduct usually won't qualify. Attacks against sovereign nations? Yes. Hacks of corporate computer networks? Not so much. The Sony hack is closer to MafiaBoy, the Google Gmail hack, the Solar Sunrise hack, and Albert Gonzalez's compromise of T.J. Maxx and Heartland Payment Systems than it is to the Siberian and Stuxnet examples. It's just another installment in the never-ending evolution of digital crime.

There's plenty of wiggle room in the continuum of state-involved criminal activity: state-sponsored, state-proxied, state-tolerated, state-aware, kleptocratic, narco-kleptocratic, and so on. But we need to be circumspect when we start assigning these tags to the countries involved. We didn't threaten and sanction Nigeria for its connection to the Nigerian 419 phishing scams, nor did we threaten and sanction Russia for the Gameover ZeuS botnet and Cryptolocker ransomware, even though both countries knew, or should have known, that these cybercriminal activities took place on their soil.

WHAT DO WE KNOW AND WHEN DID WE KNOW IT?

So why was Sony targeted? We've been led to believe that it was the North Korean supreme leader's reaction to the plot of the Sony motion picture *The Interview*, which involves the assassination of Kim Jong-un. By most accounts, the perpetrator is an anonymous hacking group called the Guardians of Peace, which is speculated to be a cyberattack group acting on behalf of the North Korean government. But if this *were* a North Korea–sponsored hack, wouldn't they have instructed their agents to conceal this connection? To borrow a phrase from Thomas Hobbes's *Leviathan*, history has shown that the lives of the perpetrators may become "nasty, brutish, and short." History has also shown that when nation-states are involved in cyber-conflicts, any clues left behind are most likely false flags. Over the past 65 years, the US Central Intelligence Agency has shown the entire global community the value of plausible deniability.

I'm not saying that Kim Jong-un is incapable of cyberwarfare. But how much would he gain by drawing attention to himself over an ego-motivated incident like this? This doesn't seem to be a sensible occasion for a "nana-nana-boo-boo" moment.

Let's look at the reported evidence. The US Federal Bureau of Intelligence (FBI) initially reported that North Korea was the likely source of mischief (www.politico.com/story/2014/12/fbi-briefed-on-alternate-sony-hack-theory-113866.html). But the time stamps of some of the recovered files showed that downloads might have been done at USB speeds, suggesting an inside job (www.4thmedia.org/2014/12/breaking-we-can-conclusively-confirm-north-korea-was-not-behind-sony-hack). The FBI then revised its account to suggest that the North Koreans may have subcontracted freelance hackers to do their bidding (http://in.reuters.com/article/2014/12/30/northkorea-cyberattack-idINL1N0UD1IB20141230). So, the source and rationale at this point seems to be a moving target. However, FBI Director James Comey still holds firm that North Korea must somehow be to blame. When asked upon what solid evidence this hypothesis is based, we get the time-worn shibboleth "trust me."

Consider two of Comey's statements in a recent *Wired* article (www.wired.com/2015/01/fbi-director-says-north-korean-hackers-sometimes-failed-use-proxies-sony-hack). He initially states, "I want to show you, the American people, as much as I can about the why, but show the bad guys as little as possible about the how. … This will happen again and we have to preserve our methods and our sources." Then, in an effort to neutralize the critics, he says, "They don't have the facts that I have. They don't see what I see."

First, let's deal with the issue of how the FBI came to "know" what it claims. According to *Wired*, "Comey now says that the hackers in the attack failed on multiple occasions to use the proxy servers that bounce their Internet connection through an obfuscating computer somewhere else in the world, revealing IP addresses that tied them to North Koreans." Really? Are we to believe that hackers with the full financial and military backing of the North Korean government—the same government that has resources enough for a missile program (www.bbc.co.uk/news/world-asia-17399847)—doesn't have sufficient resources to hire competent hackers who know how to spoof IP addresses and use proxy servers? Does this sound reasonable to you? Script kiddies know this much!

If this is true, Kim Jong-un is getting ripped off by his cybermercenaries. Such claims should be viewed with considerable suspicion. Also, I have no idea what, if anything, Comey means by "preserving our methods and sources," if it doesn't involve subpoenas and warrants. The technical "methods" for analyzing network attacks are taught in SANS (www.sans.org) classes. Any claim that FBI network forensics specialists have a monopoly on network traffic analysis is preposterous.

As for the "facts," I seriously doubt that Comey did the network traffic analysis himself. The facts in his possession would probably be better characterized as reportage. Perhaps it might have been more accurate for Comey to say, "The summary that was presented to me [by …] seems compelling." But I think the suggestion that Comey has possession of and is in a position to interpret ground-truth data is a bit of a stretch. I, for one, would feel much more comfortable relying on the opinions of those who have appropriate backgrounds in digital forensics. For all we know, Comey is making representations that have been filtered by layers of mid-level management with little or no understanding of the technological issues, or, worse yet,

through political filters to ensure that the leadership stays on message. Recall also that Iraq's supposed possession of weapons of mass destruction, uranium yellowcake from Niger, aluminum tubes for centrifuges, and the Prague connection with Al-Qaeda were all reported as certainties.

That said, unlike some of the other leaders of the military–industrial–intelligence community, Comey is a bureaucrat. He was the deputy attorney general that appointed Patrick Fitzgerald to investigate the outing of Valerie Plame as a covert CIA officer (a violation of federal law). Nothing much came from the investigation (note that Scooter Libby's sentence, resulting from his conviction for making false statements and obstructing justice, was commuted), but we can't fault Comey for that.

Comey also refused to re-certify the National Security Agency's (NSA's) domestic bulk metadata collection program in 2004, which sent shockwaves through the White House. Comey, along with Attorney General John Ashcroft, Assistant Attorney General Jack Goldsmith, FBI Director Robert Mueller III, and others, threatened to resign if George W. Bush didn't bring the NSA's program in line with the law.[2,3] Again, nothing much came of this due to subsequent decisions by the FISA (Foreign Intelligence Surveillance Act of 1978) Court and the passage of the 2007 Protect America Act. But in both cases, Comey et al. positioned themselves on the right side of history, at least in terms of these issues. So let's try to give Comey the benefit of the doubt (although he's making it difficult with his pronouncements).

Doubts about the North Korean connection aren't without substance (http://marcrogers.org/2014/12/21/why-i-still-dont-think-its-likely-that-north-korea-hacked-sony; http://blog.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack; and www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198). Bruce Schneier also has links to relevant data on his blog (www.schneier.com/blog/archives/2014/12/more_data_on_at.html).

Of course, if a connection between an adversary and a hostile act is never proved, bureaucracies might appeal to cognitive dissonance theory and confirmation bias. Taking this into account, the "absence of evidence is evidence of clever deceit." Logicians refer to this as a variety of "the argument from ignorance." However you wish to characterize the phenomena, it has been used masterfully for 50 years by neoconservatives—for example, Team B's claims of Soviet economic and military superiority while the country was imploding, and Donald Rumsfeld's dismissal of the failure to find weapons of mass destruction in the second Iraq war as irresponsible impatience by the media. Don't be surprised to see this kind of illogical belief perseverance resurface again in this context.

> Accusing attribution during an ongoing investigation is like painting falling leaves: the results are sloppy and unlikely to have enduring value.

EMAIL PROPRIETY 101

Some of you are old enough to remember the first principle of email propriety: don't include things in email that you're not willing to post on your office door. Apparently, some of Sony's ill-mannered executives never embraced this refrain. A choice selection of leaked email from Sony co-chair Amy Pascal and producer Scott Rudin were found to be injudicious and of questionable taste. (A summary timeline may be found at www.usmagazine.com/celebrity-news/news/sony-hack-key-events-from-leaked-emails-terror-threats-20141812.) Could it be that entertainment executives are occasionally petty, imprudent, and ill-tempered? Color me surprised! For over a century, entertainment executives have given substance and form to the expression "warm, caring, sensitive, and fair-minded"—especially when dealing with talent (actors, directors, artists, screenwriters, and the like). So who would have thought that an occasional racist thought might creep into their light-headed correspondence? Why, even a cursory review of the list of Academy Award winners will dispose of any thought of bias and discrimination in Hollywood. There's no more minority or gender bias in the entertainment industry than in, say, professional sports or politics, for goodness' sake. And no less, either! There's nothing remotely newsworthy in the leaked email that I can see. Gossipy? Yes. Newsworthy? No.

Now, if I haven't yet convinced you that this story is stuck on stupid, I've got a hole card. Politicians and bureaucrats pushed the story over the event horizon of dumb. First, President Obama made accusations that were apparently based only on the fungible intelligence I mentioned. These days, such accusations are predictable ingredients of an intelligence-state narrative. Obama castigated North Korea for the apparent "act of cybervandalism" (www.theguardian.com/us-news/2014/dec/21/obama-us-north-korea-state-terror-list-sony-hack) as he promised a "proportional response" (drones?)—even with the absence of concrete evidence. Then Sony decided to withhold the holiday release of *The Interview*. Obama criticized this action (www.theguardian.com/us-news/2014/dec/19/obama-sony-the-interview-mistake-north-korea). Not willing to concede the last point, Sony Entertainment CEO Michael Lynton responded that Sony sought advice from the White House without effect

UPDATE

The official "truth" continues to be a moving target (www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html, and www.theregister.co.uk/2015/01/19/nsa_saw_sony_hack). The latest FBI and NSA revelation is that they were monitoring North Korean network traffic all along, so they could easily trace the traffic back to the source in real time. Although this explanation seems the more likely than earlier ones, it still doesn't seem complete. For one thing, it leaves open the question of why the government didn't use a tech company intermediary to inform Sony that it should tweak its firewalls.

I look at these latest revelations as a last attempt to find some story that simultaneously satisfies the public curiosity, deflects media criticism, and doesn't make the agencies involved look incompetent. The intelligence agencies don't seem to understand that when a story arc begins with an absurdity or falsehood, the audience will never willingly suspend disbelief through to the final act. I still claim that critical pieces of the Sony hack narrative are missing, and that there's more to this than meets the proverbial eye. Stay tuned.

(www.theguardian.com/film/2014/dec/18/fbi-north-korea-sony-pictures-hack-the-interview). And so it goes. I'm confident that, were he still with us, Aldous Huxley would have said that this story does little more than feed mankind's almost infinite appetite for distraction from the more important affairs of our times.

KNOWN KNOWNS?

Someone hacked Sony. At this point, the finger-pointing and narrative is dominated by agendists who seek to create a usable history for themselves and their patrons. I'm not claiming that Kim Jong-un and North Korea aren't involved in the Sony hack. I'm claiming that it's irresponsible to make such accusations until verifiable proof is determined. Certainly the July 2009 distributed denial-of-service attacks against US and South Korean interests point to North Korean involvement, so we know that North Korea is capable of cybertransgressions. But in this case, the incomplete and unreliable evidence that's being offered amounts to little more than smoke and mirrors. The Sony hack story has all the substance and veracity of Nessie and Sasquatch sightings.

But let's be realistic. Searching for Nessie, Sasquatch, and the Guardians of Peace carries no penalty for the media. If the filmed search didn't find Nessie where expected, that's one more place we can rule out. We then get a few talking heads to follow up: "I never believed that Nessie would go there," "We're reviewing our evidence to see where we went wrong," and so on. Even if we can't conclusively prove that the Guardians of Peace are working for Kim Jong-un, we can find some senior government official to report that they probably are. That's almost the same thing as saying they might be, which is just one semantic smidge away from having no idea. But reporting that we have no clue won't sell much advertising. And, after all, we can always use some variant of the argument from ignorance to retroactively cover sloppy reporting.

In the meantime, Sony gets some much-needed free advertising for a film with an arguably tasteless plotline. This may be the real story: political satire works best when the audience isn't bludgeoned with crude character assassination, suggestions of cruelty, and comical disrespect. Making films that make sport of killing political leaders is just poor form and relies more on shock value than creativity. Moviegoers would be better served by a re-screening of Charlie Chaplin's 1940 classic *The Great Dictator* and using their imagination to port the concepts over to current affairs.

It's up to enlightened audiences to reject this background noise for what it is; mass media has every incentive to tilt toward coverage of the inane. And governments would be well advised to avoid attaching military and economic consequences to crimes against corporations, especially when such crimes have no national security implications. It's also a good idea to avoid prejudging the outcome of an ongoing investigation that involves world leaders. The tough talk and bogus claims from all directions, the threats and sanctions based on spotty evidence, and the accusations and counter-accusations serve us all poorly. Accusing attribution during an ongoing investigation is like painting falling leaves: the results are sloppy and unlikely to have enduring value. Thus far, reporting on the Sony hack has been banal in the extreme.

REFERENCES

1. T.C. Reed, *At the Abyss: An Insider's History of the Cold War*, Presidio Press, 2004.
2. B. Gellman, *Angler: The Cheney Vice Presidency*, Penguin Press, 2009.
3. M. Isikoff and D. Corn, *Hubris: The Inside Story of Spin, Scandal, and the Selling of the Iraq War*, Crown, 2006.

HAL BERGHEL is an ACM and IEEE Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.