Portfolio Project: The 2014 Sony Data Breach and Attribution of Attacks in Cyber-Espionage

Stephen D. (Doug) Woodward

Managing Virtual and Cloud Systems: Fall17-B-8-ISM511-1

Portfolio Project, Module 8

Colorado State University Global Campus

Dr. Julia Smith

October 6, 2017

Portfolio Project: The 2014 Sony Data Breach and Attribution of Attacks in Cyber-Espionage

With the increased flexibility of cloud computing and, generally speaking, its lower costs, come the undesirable probability that the data assets of organizations exploiting these resources will experience a systems security breach exposing its data to the outside world. We continue to read headlines of companies and countries whose data assets have been hacked with stunning consequences. The recent disclosure of the massive attack at Equifax demonstrates how serious data breaches have become. 44% of the U.S. population had data pertinent to its identity breached.

However, an even more serious type of breach using hacking as a weapon of war has come into focus. The intent of this paper is to answer a series of questions about the Sony data breach of 2014 as a well-known example, and conclude with a summation of those factors that identify whether a nation state has foisted a data security breach ("in the cloud") against an adversary. The questions this paper seeks to answer in the first portion of this paper are:

1. What went wrong (in the major "cloud breach" at Sony Pictures)?
2. Why did it occur (what failures in security were determined afterwards)?
3. Who was responsible (what evidence was produced that identified the culprit)?
4. Could this event have been prevented (what measure or steps could have been taken?)
5. What advice should Sony Pictures take to prevent a similar breach in the future?

The second portion of the paper will examine the challenges in attributing a cyber-attack (or cyber-espionage) based on the "fingerprints" left by its actors. It will be argued that scholarship has compellingly challenged the authenticity of any claim that the source of an attack can be known with certainty except in those cases where the attackers are unsophisticated, its source easily ascertained, or publicly admitted. The conclusion: Attribution comprises a political statement made by its victims, not a technical one that can be proven with irrefutable evidence.

Thesis

With the supposed Russian hacking of the Democratic National Committee (DNC) in 2016, the specter of "state-sponsored" hacking (nation states breaking into strategic information to attack their enemies), has moved front and center. The most famous example of a state sponsored data breach occurred at Sony Pictures, carried out by North Korea, to financially harm Sony for distributing a movie "The Interview," a comedy starring Seth Rogen and James Franco, which mocked North Korean leader, Kim Jong Un (the movie was slated for release on December 25, 2014). While there was some debate as to who carried out this attack, this event has now been widely accepted as an authentic example of a state-sponsored terrorist attack.

So, in addition to answering some fundamental questions about what happened at Sony that increased the probability of attack, this paper will also consider the matter of *attribution* in cyber-attacks and cyber-terrorism.[1] That is, "How do we identify that a 'hack attack' was the result of a particular nation state's nefarious activity? What are the attributes that, like finger prints, tell us the hacking was political and not merely for notoriety or for profit?" The paper will attempt to demonstrate why assigning responsibility to a particular nation state in carrying out an act of cyber-warfare constitutes a high-stakes game based on suspect accusations which limit clear outcomes. Thus, the allegations of those in the Democratic Party in the U.S., that Russia conducted a cyber-attack on the DNC, much less the never-made-public evidence that Russia colluded with Donald Trump (somehow related to this attack), remains highly suspect due to the inexactness of attribution. In summary, attributing the Sony attack to North Korea is one thing. Attributing a possible DNC email attack to Russian cyber-espionage is quite another.

---

[1] Note: when using less common words as cyber-attacks, cyber-terrorism, and cyber-crime, for clarity and consistency sake, the paper will standardize on their hyphenated forms.

Background

Stockburger (2016) states that Sony Pictures was the victim of a highly-publicized DDoS (Distributed Denial of Service) attack by North Korea on the brink of distribution of the Sony film, "The Interview." The film was an account of a fictional assassination of Kim Jong Un. Korea's Ministry of Foreign affairs said that "the country would take 'a decisive and merciless countermeasure' if the United State government permitted Sony to make its ultimate attack." Additionally, enormous amounts of data, including digitized future Sony films and personal data of Sony employees, was stolen. To be more specific, McCarthy (2015) in a Huffington Post article, summarized the incident as follows: "In late November, hackers breached Sony's servers and leaked a wide range of data. This included internal documents on Sony employees and actors, as well as copies of unreleased Sony movies such as *Annie*, *Mr. Turner*, *Still Alice*, and *To Write Love on Her Arms."*

The incident created a firestorm. Chon (2015) writing for the *Financial Times*, cites FBI Director, James Clapper, who called the incident "the most serious attack ever made against the United States" (para. 13). U.S. Senator John McClain, the incoming chairman of the Armed Services Committee, used the incident to declare that the-then Obama Administration had done little in the way of preventive measures to protect the country's infrastructure (public and private) from state-sponsored terrorism. However, while McClain hinted that Sony Pictures should not have given in to terrorists' demands by shelving the film, he primarily employed the incident to criticize President Obama for doing too little to protect American institutions from cyberspace attacks. An article in the on-line magazine, *Inside Cybersecurity,* quoted McClain:

> "By effectively yielding to aggressive acts of cyber-terrorism by North Korea, that decision sets a troubling precedent that will only empower and embolden bad actors to use cyber as an offensive weapon even more aggressively in the future," McCain said.

> "But, make no mistake," McCain added. "The need for Sony Pictures to make that decision ultimately arose from the administration's continuing failure to satisfactorily address the use of cyber weapons by our nation's enemies." (para. 5-6)

The incident led to a letter from Chairman of the Senate Foreign Relations Committee, Robert Menendez, to the-then Secretary of State, John F. Kerry, in which he stated, "Through cyber-attacks North Korea was able to inflict significant economic damage on a major international company. In addition, in the face of violent cyber-threats, Sony Pictures made the decision not to release a motion picture which the North Korean regime found objectionable – in part due to coercive threats of 9/11 style attacks on theaters planning to show the film *The Interview."*

What Went Wrong and Why Did It Occur?

The attack carried out a number of hostile acts, exploiting several glaring weaknesses with Sony Pictures' systems. Landau (2016) writing on cyber-surveillance, offered up that the North Korean hackers threatened to delete data from Sony's servers and then release to the public confidential information, "including emails and personnel records, that they had lifted from those servers. When there was no response from the company, the hackers carried out their threats." Lin (2016) writing an extensive paper on attribution (to which we will turn in the concluding portion of this paper), commented that, "In the case of the 2014 Sony hack, the perpetrators … behaved in ways that were similar to the behavior of criminals like serial killers who 'stage' the crime scene, arranging it to send a message or conceal involvement" ("How Attribution Judgments Are Made" section, para. 8). This detail contributed to some doubts as to whether North Korea was the real perpetrator. We will discuss this matter below.

Tsotsis (2014) detailed the complaint by two Sony employees in *TechCrunch* through which we learn additional details of what went wrong. Tsotsis conveys that Christina Mathis

and Michael Corona filed a federal court complaint against Sony, alleging that "the company did not take enough precautions to keep employee and employee family data safe" (para. 4). Furthermore, the complaint references a technical blog noting that Sony knew of the insecurity on its network and accepted the risk. The complaint asserts Sony sought (unsuccessfully) to protect its films from DDoS attacks, but it did next to nothing to protect employee data. It also cites instances of Sony failing to adequately inform former employees of the situation, "referring to the free credit-card monitoring that Sony offered after the December 2 hack as insufficient" (para. 5). Tsotsis also notes what Kashmir Hill (the editor of Fusion's *Real Future*) reported – that when the hack occurred, there were only eleven people assigned to the Sony information security team. One former employee opined, "The real problem lies in the fact that there was no real investment in or real understanding of what information security is" (para. 7). Another matter made evident from the hack, "sensitive files on the Sony Pictures network were not encrypted internally or password-protected" (para. 7).

Was North Korea Responsible?

The U.S. government quickly asserted it was certain North Korea was responsible. Writing for NBC News, Dienst (2014) states, "The officials told NBC News the hacking attack originated outside North Korea, but they believe the individuals behind it were acting on orders from the North Koreans." Still, there are reasons to question the North Korean attribution. "Much of the US Government's evidence seems to come from some IP addresses that were hard-coded into the data deletion malware that has previously been associated with attacks from the country (although the FBI claimed it had also used psychological profiling techniques)" (para. 4). We learn that North Korea, at the time at least, had a dearth of IPv4 addresses (1024). And since deleting data remains an unusual technique for cyber-criminals, it is deemed unlikely to be associated

with nation-state actors. *Cloudmark*, a noteworthy security firm, said that it had identified one North Korean IP address as being a machine known to be infected with malware, and which had been blacklisted by anti-spam services. This could explain that, "even if North Korean IP addresses were used, they could have been exploited as proxies from outside the country" (para. 5).

A great amount of data was "exfiltrated" off of Sony servers. This issue deals with whether North Korea had the bandwidth to accomplish such data theft. According to Cloudmark, "the entire country has just one ISP and a single link to the wider Internet." However, it is certainly conceivable that external locations were used to download and store data (several films yet to be released). In fact, some files downloaded were "traced to the Regis Hotel in Bangkok" (para. 6). Additionally, security firm *Norse* said it had found discussions on secret online forums. It suggests the involvement of upset ex-employees, probably working with "hacktivists" who felt Sony's anti-piracy stance should be disregarded and circumvented (para. 7).

But the evidence still stands in favor of the U.S. government's position. Landau (2016) acknowledges that many doubted the FBI's assertion about North Korea as the perpetrator. However, additional support came, perhaps ironically, from Edward Snowden's disclosures concerning the scope of global surveillance. It revealed the pertinent fact that U.S. intelligence operatives had previously gained access to the North Korean networks. The U.S. had placed instrumentation inside the North Korean network. This allowed the intelligence service to monitor North Korean activity. Landau asserts that U.S. authorities conclusively demonstrated the Sony infiltration and attack was North Korea's work. They revealed this in January 2015 and convinced most doubters through this revelation. Lin (2016) concurs with this assessment stating, "Such instrumentation was reportedly part of the attribution to North Korea of the attack against

Sony Pictures Entertainment in 2014." Lin indicates that the U.S. can pre-position "instrumentation" after (presumably) a policy decision has been made that a specific "adversary may launch future intrusions and that an investment in anticipatory emplacement of such instrumentation is therefore justified" ("Attributing Malicious Cyber Activity to a Machine" section, para. 10). Of course, the public must be willing to accept as true what the government tells us. Trusting that the intelligence services of the U.S. government always tell the truth, is no longer a given, especially in light of the fact that intelligence officials like former Director of National Intelligence James Clapper, have misled Congress in the case of the National Security Agency surveilling the American public (Johnson, 2013).

It should be noted that the U.S. apparently conducted a so-called proportional attack on North Korea. Stockburger (2016) states after "U.S. officials traced the attack back to North Korea using the U.S.'s own cyber-operation… North Korea suffered widespread Internet outages" (p. 553). Petkis (2016), in a study of what is a "proportionate response," acknowledged that unlike what the U.S. may have done in reaction to North Korea, responses do not have to be of the same kind, "which in this context means the United States would not be limited to a 'hack back' or responsive cyber-attack. Yet if the U.S. response is kinetic, proportionality will be harder to justify" (p. 1450). That is, if the U.S. responds with kinetic retribution, its critics will argue that its attacker may have only stolen information, damaged information processing equipment, or data contained on it, while the U.S. potentially harmed human lives. Nevertheless, one could safely assume that cyber-espionage will inevitably be considered a *casus belli*, and eventually lead to kinetic attacks.

Could the Sony Breach Have Been Prevented? What Should Be Done by Sony and Other Corporations to Protect Its Data?

Indeed, Landau (2016) contends that the Sony incident allowed the U.S. to "put the world on notice: anonymous attackers are unlikely to remain anonymous" (p.31) The author proffers that although the National Security Agency (NSA) has been irresponsible and possibly guilty of unlawful activity, information about our cyber-surveillance capabilities coupled with the government's willingness to disclose how effective its cyber-weapons are (whether offensive and defensive) "has increased our ability to deter cyberattacks." Landau judges it to be a good thing for both security and privacy, whether domestic or foreign. (Of course, privacy rights' advocates would no doubt suggest this constitutes a big price to pay for continuous eaves-dropping on U.S. citizens).

Assuming the allegations made by the two employees who brought a claim against Sony in federal court, the company appears understaffed in cyber-security measures given the value of the assets stored on their servers. Their methods and standards for passwords and user names were elementary. Security at Sony was unsophisticated. In addition to labeling a file on their system named, "Passwords," the company ignored other common security measures. Kashmir (2014) contends, "One issue made evident by the leak is that sensitive files on the Sony Pictures network were not encrypted internally or password-protected" (para. 6). Thus, the "hack" didn't need to be especially hi-tech. Then again, given what we know about North Korea's information systems and sole connection to an internet hub, it couldn't have been complex. Thus, robust security measures commensurate with standards of other corporations, may have been sufficient to defeat the attack.

However, it is also the case that the U.S. could have done more to protect the internet (now officially in the hands of the United Nations – see *The Guardian*, March, 2016), and its use in the United States. Malawer (2015), addressing the issue of economic cyber-espionage from China,

stresses the need for rules to be agreed internationally that govern cyber-space. He begins by discussing the Uruguay Round Agreements, which includes the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) established in 1995. He contends that any effective international legal remedy to commercial cyber-espionage must creatively apply the terms of TRIPS (p. 1). He continues on to cite a number of concrete steps that have been taken to improve the situation. Malawer quotes Tom Donilon, the one-time U.S. National Security Advisor, who spoke at the Asia Society in 2013 of the then-current administration's focus on cyber-security. Donilon stated:

> [Cybersecurity] is not solely a national security concern or a concern of the U.S. government. Increasingly, U.S. businesses are speaking out about their serious concerns about the sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale... As the President said in the State of the Union, we will take action to protect our economy against cyber-threats (p. 2).

In May 2014, the U.S. indicted five members of the Chinese military for hacking into corporation computer networks in order to steal trade secrets. This indictment was a first. In 2015, the specific response to the North Korean attack on Sony was to impose economic and trade sanctions for the current-day "hermit kingdom." These were restricted to trade and financial sanctions, primarily directed at North Korea's arms industry (for export), but also included sanctions against specific government and intelligence officials. Malawer argues the U.S. should submit an action at the World Trade Organization (WTO) for its consideration in hopes to establish precedents for dealing with cyber-crime and cyber-espionage.

There is little doubt, the world requires something such as Malawer proposes. As Landau noted (2016), China's cyber-crime constituted "the greatest theft of intellectual property in human

history" (p. 29). Likewise, Malawer (2015) states, "the havoc produced by the recent North Korean cyber-attack on Sony glaringly demonstrates the need to take first steps in creating global rules for the cyber domain" (p.7). Subsequently, Malawer cites the Center for Strategic and International Studies (2013) which concluded "Some cyber threats can only be addressed through indirect action, using agreements on trade or law enforcement cooperation to restrain cyber espionage, the use of proxies, or nonstate, but an important step in tackling the technological advances in cyber-espionage and promoting a rules-based system of global governance" (p. 52). Malawer argues bringing an action at the WTO would use existing institutions and agreements to address this newest national security threat to the United States and the competitiveness of U.S. firms worldwide. (p. 7)

In addition to incorporating best practices for security measures, it could be recommended that Sony work with other corporations to support efforts by the U.S. Government to enact measures that clarify the legal premises upon which "the rule of law" can be established in "cyber-space." As Malawer points out, there are major initiatives to establish the rules of the road regarding the protection of intellectual property and to penalize individuals, groups, or even nation states who choose to attack an adversary or rob desired intellectual assets from public or private institutions they exploit.

Clapper, Lettre, and Rogers (2017) point out that progress has been made. They note that in 2015, G20 leaders affirmed that no nation state should conduct or support cyber-enabled theft of intellectual property that seeks to provide a competitive advantage to companies or commercial sectors. In conclusion, Malawer (2015) asserts that since Chinese cyber activity was redressed by U.S. penalties, there has been no example of stolen data exploited for commercial gain.

Attribution and its Challenges

Establishing "whodunit" comprises no easy exercise. In a landmark paper on the subject, Rid and Buchanan (2015) base their analysis of the current science of attribution on three assumptions. These assumptions are the premises of conventional wisdom, not what they propose is in fact the truth. The first false assumption is that the problem is intractable, "created by the underlying technical architecture and geography of the Internet" (p. 5) Presumably, the internet would have to be redesigned to fix the problem. The second false assumption seems curious upon first hearing, but definitive once understood: "for any given case, the problem can either be solved, or not be solved" (p. 6). In other words, the investigation either leads to a definite identification or winds up at a dead-end. Conventional wisdom supposes that when it comes to finding a culprit, arriving at a probability percentage isn't calculable. Unlike the weather where the meteorologist assigns a percentage probability to rain or snow, it is thought that the only percentages which can be assigned in attribution are *100 percent* or *zero*. Lastly, the third false assumption concerns the ease of interpreting the evidence. Rid and Buchanan state that conventional wisdom asserts cyber-sleuths don't find it difficult to discern the facts. Rather, finding the evidence constitutes the real trick. Once seized upon, it is falsely assumed the "facts" are easy to decipher. Again, this is how Rid and Buchanan characterize the status quo; their paper aims to propose a different set of assumptions.

The authors assert that "actual attribution of cyber events is already more nuanced, more common, and more political than the literature has acknowledged so far" (p. 6). Surprisingly, perhaps, they argue that "attribution is what states (nations) make of it" (p.7) They contend that attribution is as much an art as a science. That is, it is not black-or-white, but constitutes varying

shades of gray. Additionally, they label it a "team sport" (p. 7) because no one mind can consider all the factors involved in determining who the culprit is. And they expressly state that, "attribution is a function of what is at stake politically" (p. 7). Furthermore, they assert, "guided by non-forensic sources of intelligence, or by the broader geopolitical context — sometimes even by intuition — the possibility of malicious activity may be identified before technical indicators flag it, or indeed even before it begins." (p. 9)

After presenting their proposed process of attribution (which they label the "Q model"), Rid and Buchanan discuss the limits or constraints that must be acknowledged. They indicate three factors influencing the quality of attribution. These three are a (1) function of available resources, (2) a function of available time, and (3) "a function of the sophistication of the adversary" (p. 32). While they contend that attribution is growing easier because of technology directed at the problem and the education of cyber-detectives, it also grows harder because states' hacking agents get smarter and catch-on regarding how best to avoid detection.

Former Director of National Intelligence (DNI), James Clapper, in his submission to Congress (2015), unwittingly confirms Rid and Buchanan's final ambivalent assessment, and confirms that intelligence investigators have their hands full finding the perpetrators. Clapper stated that while cyber-security personnel will make progress in attributing cyber-operations and tying events to infrastructure or tools that could facilitate rapid attribution. Nonetheless hackers will get smarter too. They will achieve improvements in tradecraft, the use of proxies, and the creation of cover groups or institutions that rapid, high-confidence attribution of responsibility for state-sponsored cyber-operations (Ackermann and Tillman, 2016). Finally, the Rid and Buchanan assert that while liberal democracies may wish to remain clandestine, authoritarian regimes might could care less about being

caught. The willingness to conduct cyber-espionage without hiding their tracks will make it easier for attackers to exploit cyber-space.

What Are the Choices Nation States Will Make About Cyber-Warfare?

Lin (2016) presents a simplified list of Healey's nation-state taxonomy regarding cyber-attacks as provided in Healey's paper, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks (2011)." Simplifying the words further with brief explanations for each position: A state:

- Might be incapable of detecting hacking activities inside its borders.
- Might prohibit hacking activities (cyber-intrusions of various kinds), but have no ability to enforce the prohibition against bad actors.
- Could tolerate hacking activities. They might neither outlaw nor prosecute perpetrators.
- Could encourage hacking activities by providing support "under the table" (that is, supplying intelligence or suggestions to hackers on how to improve their skills).
- Could direct hacking activities. It could "outsource" hacking to third-parties.
- Could conduct hacking activities with its civil servants or military. Special units could be devoted to cyber-attacks.

United States' policy fits within the last category. President Obama's administration unofficially directed U.S. intelligence services to devise and potentially conduct a cyber-attack against Russia as a result of an alleged attack by Russia on the DNC in the summer of 2016, in order to aid Donald Trump in the 2016 Presidential race. Mortimer writing for the *Independent* (2016), reported that "The White House is considering launching an unprecedented cyber-attack against Russia in retaliation for their alleged interference in the US election, intelligence officials say" (para.

1). Additionally, "current and former officials have said that the CIA has been asked to deliver options for 'clandestine' cyber operations designed to 'embarrass' the Russian government" (para. 2).

This is not out of character for the U.S. The infamous Stuxnet virus, developed for and used against Iran, was reportedly created by the United States in concert with Israel. This attack was the subject of a recent documentary, *Zero Days* (2016), which illustrated the techniques employed in the attack and the strained relationship that resulted between the United States and Israel, after Israel extended the virus' capability well beyond that to which the U.S. had agreed up-front.

Were the Exposed DNC Emails a Cyber-attack or Just a Leak?

The issue of attribution on cyber-attacks has become the subject of an intense political controversy that still rages in the U.S. political arena. The pertinent issue involves thousands of highly controversial emails, mostly from candidate Hillary Clinton's campaign director, John Podesta, that were stored on the server at DNC headquarters. The issue has narrowed to whether the emails, made public by WikiLeaks in July by its founder Julian Assange, had come into its possession through a Russian "hack" or whether the offensive (and perhaps incriminating) emails had been leaked by a DNC employee, Seth Rich, to WikiLeaks. Adding to the intrigue: Seth Rich was murdered in early summer, 2016, and Assange intimated on a television interview in Europe that Seth Rich was the source. He also insisted that the DNC emails had not come into WikiLeaks' possession through the cyber-attack of any nation state. According to Assange, the massive email cache was "leaked" not "hacked." The debate became whether the damaging emails (which likely decided the Presidential election), could be traced back to a Russian cyber-attack, or were simply handed off through an operative using a thumb drive. The questions are: "What evidence exists that it was the Russians whodunit? Had they conducted a cyber-attack on the DNC? Did they forward the emails to WikiLeaks?

Was it done to help Donald Trump's election campaign by smearing Hillary Clinton's campaign through linking chairman Podesta with the unsavory emails he apparently originated?"

This controversy was fueled even further by the confusion over whether the-then Director of National Intelligence, James Clapper actually testified to Congress that 17 intelligence agencies supported an allegation in which Russia was deemed responsible for the purported cyber-attack on the DNC. Because of Clapper's inarticulate explanation of his view of the truth, it was less clear whether conclusion originated from a report issued by the Office of the DNI, or whether this was simply the conclusion drawn by presidential candidate Hillary Clinton as a campaign sound bite?

On October 7, 2016, Homeland Security and the Office of the DNI released a joint statement on the involvement of Russia in the supposed DNC "hack." As reported by *Politifact.com* ("Hillary Clinton blames high-up Russians for WikiLeaks releases," October 9, 2016), the official statement asserted that "The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations" (para. 7). Their joint statement added that the recent hacks "are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process" (para. 8). The contention of their statement left nothing to doubt. The Russians did a hack and apparently, they did it to help Donald Trump win the Presidency.

However, it was later reported by Reuters (2016, December 12) that the Office of the Director of National Intelligence (ODNI) that oversees the 17 intelligence agencies referenced to add weight to the claim, did not embrace the view that Trump colluded with the Russians and was benefitted by the DNC cyber-attack as a party in that action. Likewise, it should be noted

the FBI did not agree with the DNI assessment either. Additionally, USA Today questioned whether the DNI (Clapper) had actually ever testified before Congress to the effect that Russian interference was a clear-cut case of collusion between the Russians and Trump, and even re-opened the matter of whether the Russian interference was actually the purported assault upon the DNC servers. Published on *azcentral.com* (affiliated with *USA Today*) in an article entitled, "Did Obama's director of national intelligence say there is no evidence of Trump-Russian collusion?" (June 7, 2017), it was reported that Clapper had indicated on the television show, *Meet the Press (*May 7, 2017), there was nothing in the October 7, 2016 report confirming the allegation of collusion between now-President Trump and Russian hackers. The obfuscation of the "facts" and the supposition of cyber-espionage grew. Furthermore, it became clearer that no proof would be proffered that Russia conducted a cyber-attack, that if they had their efforts did not affect the outcome of the election, and it whatever they achieved never involved members of the Trump campaign.

Conclusion

Of course, Russia denies that they played any part in the U.S. elections. Likewise, they contend they did not hack the DNC. Again, it should be underscored that while the Obama Administration, through its Homeland Security Administration and the Office of the DNI asserted Russia had participated in a cyber-attack on the DNC (with alleged unmistakable Russian fingerprints), the intelligence agencies never produced specific evidence of Russian involvement for public consumption. We can safely conclude that this was due to the fact that the evidence didn't exist or the DNI and the intelligence services (all 17 of them), did not wish to disclose how they knew the Russians were to blame by admitting what fingerprints (methods and tactics) they are able detect when conducting a cyber-investigation in which Russia might be the source of an attack.

This brings us back to the thesis set out in this paper, that nation states may actively participate in cyber-espionage, but without specific evidence derived from several distinct sources, we must be hesitant to judge as true the victimized nation's allegations of attribution. Placing blame on powerful enemies to justify retaliatory actions, without the guilty party admitting to their actions, may be like throwing darts. As Lin (2016) noted, "nations implicated by the United States in various malicious cyber activities, say that it is impossible to attribute such activities to any particular actor and that there is no definitive evidence suggesting their involvement; hence, they say, all accusations amount to nothing more than speculation" ("Government Views on Attribution" section, para. 10). The Russian response can also be seen to align with the view expressed by Rid and Buchanan (2015) who suggested that, while attribution can be a matter of probability influenced by evidence – albeit inconclusive – the judgment on the accuracy of the assessment remains highly suspect because it is subject to the political aims of the accuser. As documented earlier on page 11 of this report quoting Rid and Buchanan, "attribution is what states (nations) make of it" and "attribution is a function of what is at stake politically." Clearly, the political issues were extraordinary and the allegation of cyber-warfare against the U.S. by Russia, especially given the lack of publicly provided information by the intelligence services of the U.S., has to be taken with a grain of salt. If acknowledged to be so, all the more reason to question the wisdom of counter-attacking with a "proportional response" as the Obama Administration indicated they were preparing to do, tossing aside the consequence that a kinetic war might possibly follow on the heels of a retaliation in a cyber-war, with the *casus belli* only partially proven.

The data breach at Sony by North Korea appears to be a case where the perpetrators were "caught red-handed" (pun not intended). In contrast, the lack of evidence presented regarding possible Russian intrusion and whether it conducted an attack on the DNC wasn't conclusive.

This is doubly so given the circumstances regarding (1) a more plausible alternative explanation put forth by Julian Assange of WikiLeaks, (2) the unsolved Seth Rich murder which might have been due to politically-motivated malfeasance based upon the supposition that Rich has leaked the information by the unsophisticated means of exfiltrating information with a thumb drive, and (3) the hot political climate surrounding a Presidential election when hyperbole triumphs. It must be resolved that authorities and elected officials be exceedingly cautious when drawing conclusions on the identity of cyber-espionage actors.

In conclusion, the uncertainty of identifying cyber-culprits, for the time being at least, continues to be a constraint that promises cyber-warfare by nation states will increase, and not decrease, as those accountable for cyber-security would have us believe.

References

Ackermann, S. & Tillman, S. (2017, February 9). "US Intelligence chief: we might use the internet of things to spy on you," *The Guardian.* Retrieved from https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

Chon, G. (2015, January 08). FBI makes case against N Korea for Sony hack. *Financial Times*. Retrieved from https://csuglobal.idm.oclc.org/login?url=https://search-proquest-com.csuglobal.idm.oclc.org/docview/1652216373?accountid=38569.

Clapper, J. (2015). Worldwide threat assessment of the US intelligence community, *Testimony to the Senate Armed Services Committee*. Retrieved from https://www.dni.gov/ files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

Clapper, J., Lettre, M., & Rogers, M. (2017). Foreign cyber threats to the United States. *Hampton Roads International Security Quarterly,* 1.

Dienst, J. (2014, December 18). North Korea behind Sony hack: U.S. officials, NBC News. Retrieved from https://www.nbcnews.com/storyline/sony-hack/north-korea-behind-sony-hack-u-s-officials-n270451.

Farrell, M. (2016, March 14). Quietly, symbolically, US control the internet just ended. *The Guardian*, Retrieved from https://www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana.

Goldsborough, R. (2011). The next (and current) theater of war. *Tech Directions, 71*(1), 12.

Hosenball, M., Landay, J. (2016, December 12). Top U.S. spy agency has not embraced CIA assessment on Russia hacking – sources. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-trump-intelligence/exclusive-top-u-s-spy-agency-has-not-embraced-cia-assessment-on-russia-hacking-sources-idUSKBN14204E.

Inside Cybersecurity. McCain blames white house for fallout from 'North Korea's cyber-attack on Sony pictures'. (2014). Retrieved from https://csuglobal.idm.oclc.org/login?url=https://search-proquest-com.csuglobal.idm.oclc.org/docview/1639922386?accountid=38569.

Johnson, L. (2013, August 13) "James Clapper, Director of Intelligence who misled Congress, to establish surveillance review group," *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2013/08/13/james-clapper_n_3748431.html.

Landau, S. (2016). Cybersurveillance and the new frontier of deterrence. *Current History,115*(777), 29-31.

Lewis, J. (2013 February). *Conflict and negotiation in cyberspace,* Center for Strategic & International Studies.

Lin, H. (2016). Attribution of malicious cyber incidents: From soup to nuts. *Journal of International Affairs, 70*(1), 75-137,11.

Malawer, S. (2015). Chinese economic cyber espionage: U.S. litigation in the WTO and other diplomatic remedies. *Georgetown Journal of International Affairs, 16*(SI), 158.

McCarthy, K. (2015, March 10). 32 data breaches larger than Sony's in the past year. *Huffington Post.* Retrieved from http://www.huffingtonpost.com/kyle-mccarthy/32-data-breaches-larger-t_b_6427010.html.

Mortimer, C. (2016, October 15). Obama administration asks CIA to prepare revenge cyber-attack against Russia. *Independent*. Retrieved from http://www.independent.co.uk/news/world/politics/obama-us-government-cia-cyber-attack-against-russia-retaliation-hacking-fancy-bears-a7363321.html.

Network Security. Doubts remain over whether North Korea was responsible for massive hack of Sony Pictures. (2015). *Network Security*, 2015(1), 1-2.

Petkis, S. (2016). Rethinking proportionality in the cyber context. *Georgetown Journal of International Law, 47*(4), 1431-1458.

Rid, T., & Buchanan, B. (2015) Attributing cyber attacks, *The Journal of Strategic Studies, 38*(1–2), 4–37.

States News Service (2014, December 19). Chairman Menendez writes Secretary Kerry on North Korea's cyber-terror attack on Sony Pictures. (2014, December 19).

Stockburger, P. (2016). Known unknowns: state cyber operations, cyber warfare, and the *jus ad bellum*. *American University International Law Review, 31*(4), 545-591.

Tsotsis, A. (2014, December 16). Employee data breach the worst part of Sony hack, *TechCrunch.* Retrieved from https://techcrunch.com/2014/12/16/hack-sony-twice-shame-on-sony/.