Nadine Shen Molesky

December 14, 2016

COMP 116 Final Paper

The Attribution Problem in International Cyber Warfare

Abstract

In just the past year, gigabytes of sensitive information belonging to the US government and US private companies have been stolen by other countries, compromising our economic, political, and military systems. Not only do these attacks have lasting effects on individuals whose personal data is stolen, but also on all citizens who depend on these private and public services in their daily lives. To deter and retaliate these attacks, it is necessary to determine their original sources. However, the process of attributing an attack to a source has been a difficult issue in the world of cybersecurity. This paper will examine the reasons the attribution problem exists, techniques used by attackers to hide their identities, and techniques used by investigators to attribute an attack. Some recent and large international cyber attacks will be examined, including the Sony breach and the Democratic National Convention breach. Finally, current and future government efforts related to the attribution problem, and proposed solutions to this problem, will be discussed.

Introduction

The cyber world is integral to the lives of most US citizens. For every new efficiency and capability that technology blesses us with, one hundred new vulnerabilities and dangers arise. These vulnerabilities threaten the security of our government, our companies, and our individual citizens every day. Our government has been developing

breakthrough offensive and defensive tactics to combat cyber attacks from other countries for years. However, the quality of our offensive tactics is no use if we don't know whom to attack, and many defensive tactics depend on knowing who is attacking us. This is precisely why the attribution problem is so important. Attribution is the act of determining the perpetrator of an attack or breach on a computer or network. Accurate attribution is extremely difficult because hackers can easily forge the identities and locations of their computers. Attribution is most concerning right now at the international scale, because cyber warfare is at the forefront of our problematic relations with many countries – especially Russia, China, and North Korea.

Importance of this Topic to the Community

I chose this topic because I found it concerning that there was an alarming lack of compelling evidence that this year's Democratic National Convention attacks originated in Russia, yet our government and many media sources officially attributed Russia as the source of the attack. Investigating the source of this attack, which may have cost Clinton the election, is relevant to everyone in the country because it may uncover whether our current President-elect achieved his position legitimately.

The attribution problem at the international scope has many implications for everyone in the community because it is imperative in helping defend the US from large-scale cyber attacks. When other countries steal sensitive data from US individuals, companies, or the government, it can affect the media, politics, the economy, and national security. With the right technology, an enemy country could take down our country's electrical power, prevent the US military command from communicating with their forces

electronically, disrupt our equities and bond markets, or tamper with vital networks such as power grids, transportation systems, or sanitation systems.

Without attribution, defense is impossible. We cannot retaliate or defend in many cases without knowing who was the attacker. Furthermore, improving our attribution techniques is the first step to deterring attackers. If attackers knew that they could be identified easily, they would be less inclined to attack. Even determining some clues about the attacker, such as language of origin, or their network penetration techniques, can dramatically narrow a list of highly dangerous terrorists.

Although this paper is focused on the technical aspect of international attribution, it is important to note that attribution is not only technical. Attribution starts with technical analysis – when technical experts look for attacker signatures in places like IP addresses and router logs. The next step is operational analysis, where intelligence analysts consider the context of an attack, and combine political analyses with the technical analysis. The final step is strategic analysis, where leaders look at the evidence, and make a decision on how to respond. There are many situations where it is beneficial for a politician to ignore or not respond to an attack – for example, if the attacker was from a country that is an important ally.

However, the technical step is the most crucial step for many reasons. First, it is the least developed, most difficult, and most time-consuming step. Second, it is a bottleneck because it is the first step in the whole chain. And third, the actual hard evidence, in the eyes of an international court or in the eyes of simple citizens, is the evidence at the technical level.

The purpose of this paper is also to educate the community about the attribution problem. In the words of Chris Finan, a former director of cybersecurity legislation in the Obama administration, when discussing attribution, "there's a disconnect between the rhetoric and what people assume is possible because of Hollywood and CSI" (Source 9). I hope that this paper will teach people that cyber attribution is not as easy as the media portrays it to be.

The Root of the Attribution Problem

Mike McConnell, former Director of the NSA and former Director of National Intelligence, stated in 2010 that we need to "reengineer the Internet to make attribution…more manageable" (Source 10). The root of the attribution problem is not any flaws in our government's strategy, resources, personnel, or education – it is the basic structure of the Internet. The Internet was not originally meant to be used as globally and as openly as it is used today. Designed in the late 1960s, the Internet (originally called ARPANET) was created for the military with the sole intention of sending data packets across a network in the most efficient manner possible. The reasoning behind this was that if data was lost as the result of a nuclear war or if other critical damage occurred, it would be imperative to the nation's security interests for this data to be restored as fast as possible. Security was not a concern for the designers because it was *intended for use in a trusted military environment*. Since the Internet was meant to be used by members of the same team, the ability to easily trace a packet or communication was not built in. Later, when the Internet was expanded to become a worldwide system used by billions, there was unfortunately no movement to make the

transmissions more secure, or to trace them. This is the basis for the Internet's lack of security and the difficulty of tracing a communication.

Other aspects of the fundamental structure of the Internet make attribution difficult. First, the design of TCP/IP is flawed in that communications between networks have no single point of control. Georgetown information security researcher Dorothy Denning remarks that to "trace an intruder, the investigator must get the cooperation of every system administrator and network service provider on the path" (Source 11). This makes attribution difficult, especially when these administrators belong to foreign countries, and getting them to cooperate may require a significant amount of waiting and jumping through bureaucratic hurdles. Second, the design of TCP/IP makes IP spoofing methods easy, which is the heart of the attribution problem - if people could not fake their electronic identities, attribution would be easy. This method is described in greater detail in the next section.

Methods of Hiding One's Identity

There exist many ways for attackers to hide or forge their identities, mostly stemming from the flaws in the fundamental structure of the Internet as described above.

IP Spoofing

IP spoofing is a broad term for many ways of impersonating another device, and allows attackers to hide their identity by manipulating IP header information. Among the types of attacks that use IP spoofing are Denial of Service attacks (overloading networks to make them dysfunctional), ARP spoofing attacks (linking an attacker's MAC address with a victim's IP address, allowing them to steal information), and DNS Server spoofing attacks (modifying a DNS in order to reroute a domain name to a different IP address,

allowing the attacker to spread malware). Spoofing a machine's location and identity is easy due to both the weak structure of network transfer protocols, and the availability of "crime-as-a-service" anonymization tools. Due to these tools, some hackers don't even need to know anything about computers. The 2014 Internet Organized Crime Threat Assessment report states that "almost anyone" can be a cybercriminal due to these easily available services.

Botnets

Another method that attackers can use to perform malicious activity without compromising their identities is a botnet. A botnet is a network of computers infected with malware controlled by a remote hacker. Also known as a "zombie network", hackers can then use this network to deliver Distributed Denial of Service Attacks (overloading networks to make them dysfunctional) or other types of attacks. Attribution is difficult in this case because the attacks are sent from many remote computers unrelated to the original hacker.

Tor

An extremely popular method for hiding one's identity is Tor. Tor, originally called "The Onion Router", is a free anonymity software used by over 1.5 million people each day. Tor works by directing Internet traffic through a global network of anonymous proxy servers connected by virtual encrypted tunnels. This way, observers of network traffic cannot detect the location of the origin or destination of a network transmission. The Tor website states that its purpose is to protect users against traffic analysis and to ensure "personal freedom and privacy, confidential business activities and relationships, and state security" (18). However, most people use Tor for illegal activity. A study from

King's College in London, published in February 2016, found that 57% of the sites designed for Tor facilitate criminal activity. Besides Tor, many other methods of anonymization exist, including using proxies or VPN services – but Tor is the most widely used.

Non-Technical Methods

There are other less technical methods that many hackers use in order to make attribution more difficult. Many international attackers plan attacks so that they are multistage and multijurisdictional. For example, an attacker could reside in Russia, establish a botnet in Ethiopia, have this botnet send malware to another botnet in China, and finally have the computers from China execute a large attack on US computers. This makes attribution very difficult, because the attributors need to piece together all the stages, and gather evidence from different governments who may be uncooperative. On top of that, many attackers purposefully choose to route their attacks through countries that lack means of international cooperation, legal standards for prosecuting cyber criminals, or standards for internet service providers to keep data logs to trace communications.

Methods of Attributing an Attack

Although the US government does not disclose its technical methods of determining the source of a hack for security reasons, an article by David Wheeler compiling methods of attribution was published in 2003 for the Institute for Defense Analyses, a non-profit corporation whose purpose is to conduct research and provide information for the United States Department of Defense. A summary of selected methods and potential obstacles to their implementation follows.

Store Logs and Traceback Queries

Routers log information about packets that are sent through a network. These logs may store a conversation or only a subset of information. An investigator can then query a preceding router if the log contains something related to the message, and trace back the packets to the source.

In an international cyber warfare scope, this would require policy that both international and domestic internet service providers keep records of complete logs for a certain amount of time, and cooperate with the US government to disclose the logs. This would likely raise disputes about consumer privacy.

Forward-Deployed Intrusion Detection Systems

An intrusion detection system is traditionally a system running on a defender's network that monitors for specific or unusual attack patterns and sends an alert to a system administrator if an attack is detected. A *forward-deployed* IDS is one that is placed close to the attacker's network (in secrecy) instead of the defender's network. This is more desirable for attribution because it provides more information on the attacker's location than if the attack has to be traced back through various locations.

This method presents many policy and jurisdictional obstacles. Scaling this type of system beyond one administrative domain would raise issues of security vulnerabilities of the system, trust between domains, and system compatibility issues. Scaling would also raise privacy concerns, because the government would need the ability to inspect the full contents of packets passing through US networks.

Hack-back

In hack-back, an investigator attempts to attribute the source of an attack by gaining control of subsequent hosts in a backwards path from the victim's computer to the attacker's computer. This method is named "hack-back" because it is common to gain control of the intermediate hosts by "hacking" – by exploiting the same vulnerability in each host that the original hacker used.

This method has obvious legal obstacles. If the original methods of hacking that the attacker used to gain control of certain hosts were illegal, they may still be illegal for an investigator. If some of the intermediate hosts belong to private citizens, gaining control of those hosts would also spark privacy concerns and require at least a warrant.

A more extensive description of each method, along with more methods, can be found in Wheeler's report (Source 31).

Recent Events Highlighting the Attribution Problem

The 2014 Sony Hacks

In November 2014, Sony was the victim of a hack that leaked private employee emails, social security numbers, healthcare information, unreleased films and scripts, and wiped out more than 70% of Sony's computers. The hackers also threatened to attack movie theaters on the release of "The Interview", a comedy about assassinating Kim Jong-Un, which North Korean leadership had already expressed anger about. The hack was speculated to be in response to the creation of this movie. This was not the first cyber attack on Sony, which was already largely known within the cyber community to be one of the least secure large companies, since they have followed bad practices such as not encrypting their data and storing passwords in a file called "passwords".

After a thorough investigation, the FBI and President Obama publicly named North Korea as the source of the attack, and Obama imposed new sanctions on North Korean government officials in response. This was a huge event in the context of attribution in international cyber warfare because this was the first time the US officially charged a foreign government with a cyber attack on the US.

To this day, there remains a debate within the cybersecurity community as to whether the US government's attribution of the hack to North Korea was accurate. This debate stems largely from the fact that the government decided to only release a partial amount of the evidence towards the attribution.

The evidence that the FBI did decide to release was this: 1) There were similarities in code, algorithms, methods, and compromised networks to malware previously developed by North Korea; 2) There was significant overlap in the infrastructure (such as IP addresses used) used in this attack and other attacks previously linked to North Korea; 3) The tools used in the attack have similarities to a cyber attack in March 2013 by North Korea on South Korea. The FBI introduced this evidence by first stating that this was only a *partial* amount of the evidence found due to security concerns.

Critics of the US' attribution of North Korea state that this evidence only shows that the attacks had characteristics of prior North Korean attacks, but another nation could have been spoofing a North Korean attack. If the US knows the signatures or North Korean attacks, it is not unlikely that another country might as well. The release of only partial evidence makes it impossible for these critics to trust the attribution of this attack.

Proponents of the US attribution of North Korea state that they believe the FBI out of trust for our government cybersecurity experts. Some researchers from Trend

Micro and Mandiant/FireEye examined the evidence and confirmed that the data breach originated in North Korea, and released more specific evidence from their investigations. Furthermore, other cybersecurity professionals took it upon themselves to do their own research. Kaspersky Lab researcher Kurt Baumgartner noted other similarities between the Sony hack and other hacks attributed to North Korea that were not listed in the FBI's evidence release, in support of the FBI's position.

Many people criticized the government for making a public attribution of North Korea while only providing partial evidence for proof. This made every citizen's decision on whether to believe the attribution a matter of whether or not they trust the government. It set a precedent that implied that citizens should trust the government without proof, which is dangerous to a country founded on such free thought as the United States. Many members the cybersecurity community chose not to trust the government because the nature of cybersecurity, and every field of science for that matter, is to not trust any statement without evidence. Therefore, distrust of public attribution by many members of the public is inevitable in a national security context. The government understandably cannot release sensitive information, but also wanted justification from the masses for their attribution and subsequent response to the attacker. Unfortunately, they could not have both.

The Sony hacks highlighted the relevance of the attribution problem in an international cyber warfare context and illustrated the difficulty that the US government faces in gaining public approval and justification during cyber attribution while also being sensitive to security needs.

The 2016 Democratic National Convention Hacks

The story of the 2016 DNC hacks is virtually the same story as the 2014 Sony hacks – except this time, Russia was the alleged culprit, not North Korea. When thousands of emails from leadership of the Democratic National Committee were leaked before the US 2016 election, the US government formally accused Russia of hacking the DNC's networks and attempting to rig the election in Donald Trump's favor. However, different organizations within the US government disagree on this attribution. The CIA formally attributed Russia, with the Department of Homeland Security and the Office of the Director of National Intelligence agreeing, but the FBI concluded that there was a lack of evidence.

The current evidence attributing Russia consists of statements released by private security firms like CrowdStrike, which is problematic itself because these companies have a direct financial interest in pinpointing a malicious actor. The evidence so far is that some IP addresses, domain names, metadata, phishing emails, links, and a conversation with the attacker, all related to the attack, were found to be associated either with Russian intelligence units nicknamed Fancy Bear and Cozy Bear, the Russian language, or Moscow itself. This evidence is not enough. Examining each piece of evidence individually leads to the conclusion that each piece of evidence is linked to Russia only loosely. Furthermore, even the claim that Fancy Bear and Cozy Bear work for the Kremlin is still speculative in the intelligence community.

As with the Sony attack, there is no direct proof of the attribution – only circumstantial proof, suggesting that another country could have just been pretending to look like Russia in its hacks. James Scott, senior fellow at the Institute for Critical Infrastructure Technology, states that other countries could easily mimic the signatures of

Fancy Bear and Cozy Bear. Referring to the process of hacking a remote machine in a different country to make it look like an attack originated there, he states, "this process is so common and simple that's its virtually 'Script Kiddie 101' among malicious cyber upstarts" (Source 27).

This repeating pattern of the US publicly blaming other nations for cyber attacks with an underwhelming amount of evidence available to the public, as seen in both the Sony hack and the DNC hack, is problematic. The burden of proof for publicly blaming another government for a cyber attack should be much larger, because the implications include such large-scale responses such as starting a war.

In the next section I detail our country's current efforts in the context of international attribution.

The Present: Current Government Efforts in Attributing Cyber Attacks

In the midst of this pessimistic paper, it is imperative to note that the US government has put forth many worthwhile policies and organizations to strengthen our nation's cybersecurity. Strategies and task forces including the International Strategy for Cyberspace (2011), the Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (2013), and the Defense Science Board Task Force on Cyber Deterrence (2014) all started successful policy initiatives. Government organizations such as the Pentagon's Defense Cyber Crime Center and the Cyber Command are dedicated to solving cybersecurity issues and have thousands of employees dedicated to improving the nation's cyber defense and response.

However, attribution is sparsely mentioned in any of these reports. After analyzing many cybersecurity policies, improving our nation's attribution techniques and

research is only mentioned briefly in the Cyberspace Policy Review (2009), the DoD Cyberspace Policy Report (2011), and a Blueprint for a Secure Future (2011).

Since official documents barely mention efforts towards attribution, what we do know about current government efforts on attribution is very unofficial. One speculated attribution technique is that the government uses data from the NSA's monitoring of telecommunications metadata to aid in attribution (the very same processes that were revealed by Edward Snowden). A New York Times article, an NSA spokeswoman, and a 2012 NSA strategic document have all confirmed that the government in fact did use that data to aid in the attribution of cybercriminals.

It is under debate whether this mass surveillance has truly ended. In the aftermath of the chaos resulting from Snowden's revelations, the USA Freedom Act was passed, which imposed some new limits on the bulk collection of telecommunication metadata on US citizens. However, many critics believe that the mass surveillance will continue under some legal loopholes such as Executive Order 12333 and Section 702 of FISA. Even if this specific NSA surveillance ended, it is likely that other types of surveillance are still used by the government to aid in attribution of cybercriminals. In fact, long after Snowden was convicted for his crimes, Obama stated in a speech, "we cannot prevent cyber threats without some capability to penetrate digital communication" (Source 30).

When Obama leaves the White House, we can only hope that the next President will focus more on attribution. At the given time, this seems unlikely.

The Future: Trump's Proposed Cybersecurity Efforts

While President-Elect Donald Trump placed a heavy emphasis on the importance of cybersecurity in his campaign, he has never directly mentioned the ongoing issue with

attribution. Furthermore, his publicly made plans for cybersecurity have been lacking in concreteness. His website lists a high-level 4-step plan to increase our cybersecurity efforts, but his closest indication of dealing with attribution is that he plans to "develop offensive cyber capabilities to deter attacks and respond appropriately" (Source 4). While this is an ideal vision, it lacks any policy details. His lack of concreteness may have been on purpose, which may be an indication of a larger issue – that cyber security is so poorly understood that going into more detail would lack any appeal to the public (and potential voters).

It is problematic that Trump places so much emphasis on offensive tactics without even addressing the attribution issue. He has frequently made statements on improving cyber offense, stating that he would like Cybercom (U.S. Cyber Command) to have the ability to launch "crippling cyber counter attacks. And I mean crippling, crippling" (Source 2). He also plans to further invest in cyberweapons contractors, indicating offensive plans. However, it is foolish to promise so much striking back without mentioning the attribution problem, as one cannot strike back at someone without knowing their identity or location.

Another problem with Trump's current plan is a lack of qualified personnel. Trump has not appointed or indicated that he plans to appoint any experts in cybersecurity to political positions, and none of the people Trump has appointed to security-related positions have any background in computer science – including Michael Flynn (appointed National Security Advisor), K.T. McFarland (appointed Deputy National Security Advisor), and Michael Pompeo (appointed director of the CIA). Furthermore, there is already a problem with the limited number of government

employees in cybersecurity, due to the fact that many of them switch to the private sector due to the higher pay. It is also projected that about 5-10% of Obama's current employees, including those in cybersecurity, will resign before the Trump administration is in power, which makes this problem even worse.

Obama put together a Commission on Enhancing National Cybersecurity, which released a report on December 2, 2016, whose purpose was to advise Trump on policies to improve cybersecurity, and included many concrete and useful cybersecurity recommendations. However, it is unknown whether Trump will follow any of the recommendations in the report, given that he has no obligation to.

Action Items: Proposed Solutions for the Main Barriers in International Attribution

In this section, I reiterate some current barriers to international cybercrime attribution in the US, and suggest proposed solutions.

One of the largest barriers to international cybercrime attribution is the lack of international cooperation. Many attackers use attacks that span many different countries, each with its own policies, tracking procedures, and cybercrime prosecution standards. This makes it extremely difficult for investigators, as they must jump through many different legal and bureaucratic hurdles to collect necessary data from each country. The first solution to this is to create strict, uniform global policies holding states and individuals in those states accountable for cybercrime originating from their countries. The second solution concerns the fact that many hackers route attacks through countries that do not have the means or will to keep data logs of Internet communications. A global initiative should be put in place to help these countries establish this and have a uniform standard for data collection. Furthermore, countries should cooperate to share data in

investigations, and the US should begin to form partnerships in order to facilitate this. The formation of an international organization to combat these issues would be ideal. I would encourage the next President to work diplomatically with international leaders and organizations to put these policies in place.

Another large barrier to attribution, as stated earlier in the paper, is that the fundamental structure of the Internet makes it easy to fake a computer's identity and location. Completely restructuring the Internet, as suggested by Mike McConnell, would be impossible and inefficient at this point of its maturity. However, it would be beneficial for the Department of Defense to modify its own computers and networks to improve attribution efforts. David Wheeler of the Institute for Defense Analyses suggests doing this by "hardening routers and hosts, so exploiting them as intermediaries is more difficult, limiting spoofable protocols, disabling broadcast amplification/reflection, and implementing network ingress filtering" (Source 31). Furthermore, although changing the underlying structure of the Internet may be impossible, the government could start to implement small changes to compensate for these underlying problems, such as mandating that all new servers log all packets and only accept authenticated packets.

Finally, attribution is only a downstream solution to combatting an international cybersecurity attack. Simultaneous upstream solutions need to be implemented at the same time to *prevent* attacks in the first place. Among the most important of these upstream issues is the lack of security in commercial products. Every major international cyber attack has occurred on either commercial hardware or software that had security vulnerabilities. This is partially due to the fact that companies are not liable for a lack of security in the products the sell. Therefore, one policy suggestion is to incentivize

companies to create more secure products with stricter legal consequences for having security vulnerabilities. Companies are most concerned with making money, so the potential legally-induced financial losses need to be larger for companies to be more stringent with their security protocols. Furthermore, data-gathering or tracing technologies could be integrated into these products to help the government with attribution at the same time as prevention. (This was unsuccessfully attempted when the NSA attempted to monitor telecommunications metadata, but the government could cooperate with private companies in many other ways).

The insecure software and hardware sold by many companies is not even the root of the problem. The root of the problem is the employees at these companies. And the root of that problem is the education of those employees. Security is an afterthought at most companies because it is an afterthought in most university Computer Science departments. Many educators in the field of cybersecurity even report pushback from faculty when they attempt to establish security courses or requirements. Ming Chow, a security professor Tufts University, states that learning to code without having a required computer security course is analogous to learning wood shopping without being required to learn safety procedures or wear safety gear. Therefore, I would suggest national and state-level policy initiatives to mandate cybersecurity education for computer science students.

Conclusion

Unjustified attribution can be a ticking time bomb. The US government could start a war by inaccurately attributing an attack to a state actor or by acting in response to a speculated attribution. Especially when we deal with such easily explosive countries

such as North Korea, our government should be more conservative and more private with how it points its fingers. We need to keep in mind that cyber attribution is almost *always* circumstantial.

Our government also needs to have more policies fixed on focusing the attribution problem. There is a concerning lack of policy in this area.

As a closing note, we must not forget that our nation's computer defenses should not depend on attribution, due to its high level of uncertainty. Attribution is a downstream solution. Attribution and prevention efforts need to be given equal resources.

As we begin the next Presidency, we can only hope that the United States government will devote more efforts to the attribution problem.

References

1) https://www.linkedin.com/pulse/cyber-security-attribution-hrc-dnc-russians-chinese-you-washington

2) http://blog.cybersecuritylaw.us/2016/11/06/us-presidential-election-2016-clinton-and-trump-on-cybersecurity/

3) http://www.techrepublic.com/article/cybersecurity-in-president-trumps-america-the-first-100-days/

4) https://www.donaldjtrump.com/policies/cyber-security

5) https://www.cyberscoop.com/trump-national-cybersecurity-plan/

6) http://www.forbes.com/sites/seanlawson/2016/12/03/technologists-and-security-experts-warn-of-trumps-cybersecurity-plans/#f78cb977b115

7) http://fortune.com/2016/11/16/trump-cyber-security-team-and-policy-slow-to-take-shape/

8) https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf

9) http://www.dailydot.com/layer8/attribution-cyberattack-poker-game/

10) https://books.google.com/books?id=p7EyCgAAQBAJ&pg=PA38&lpg=PA38&dq=cyber+attribution+current+policies&source=bl&ots=jobiiREJX8&sig=gwwZxwmsGHjXtTs9OVzq_c6fD2I&hl=en&sa=X&ved=0ahUKEwjctoDs2u3QAhWFD8AKHVMvBDkQ6AEIOjAE#v=onepage&q&f=false

11) http://www.au.af.mil/au/aupress/digital/pdf/paper/cpp_0001_yannakogeorgos_cyber_ttribution_challenge.pdf

12) http://cdn.govexec.com/media/gbc/docs/gbc_dellsoftware_attribution_ib_designed_final.pdf

13) https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance

14) http://www.npr.org/sections/parallels/2016/12/12/505272992/the-russian-hacking-kerfuffle-what-we-do-and-dont-know

15) http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

16) http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html?sid=ST2010031901063

17) http://www.computerworld.com/article/2688411/report-crime-as-a-service-tools-and-anonymization-help-any-idiot-be-a-cyber-criminal.html

18) https://www.torproject.org/index.html.en

19) http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/

20) https://www.pkcsecurity.com/data/Cyber_Attack_Attribution.pdf

21) https://www.pkcsecurity.com/data/Cyber_Attack_Attribution.pdf

22) http://www.businessinsider.com/north-korea-sony-hack-2016-6

23) http://sony.attributed.to/

24) https://www.wired.com/2015/01/feds-got-sony-hack-right-way-theyre-framing-dangerous/

25) http://georgetownsecuritystudiesreview.org/2015/01/13/accurately-attributing-the-sony-hack-is-more-important-than-retaliating/

26) https://blog.kaspersky.com/sony-hack-north-korea/7072/

27) http://www.infosecurity-magazine.com/news/think-tank-dnc-hack-attribution/

28) https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/

29) https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election

30) https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

31) handle.dtic.mil/100.2/ADA468859