The Blame Game
Attribution in the 2016 Elections

Norman Young

December 15, 2016

Abstract

From the Democratic National Convention email hack to password leaks of major online corporations, attacks on sensitive information of national security concern have become increasingly frequent in recent years. As a result, there is an ever-increasing pressure in political culture to improve the way we secure our data, as well as to locate and combat the source of these cyber attacks, as soon as possible. Election season especially is a time when people look to influential political figures for answers on who to blame when information is breached. The problem, however, is that attributing these malicious actions online to a single source has proven to be a difficult, and even impossible task at times. This topic of who to blame and how to fight back was recently brought up in a presidential debate during the US 2016 elections. This paper will attempt to look at the attribution problem in the light of the candidates' responses. With a large portion of the population uninformed on security matters, can public figures accurately give answers about cyber security concerns? Finally, we will propose action items and relevant applications to combat the attribution problem, and discuss whether or not it is a problem that can ever be completely solved.

1 Introduction

On September 26^{th} 2016, the topic of cybersecurity was finally brought into the national spotlight during the first of three presidential debates. Public debates have been essential in the election process for both informing voters about the candidates' views, as well as educating voters about current issues. For this very reason, cybersecurity plans being brought to the forefront of a national debate for the first time, with millions of people watching, has huge ramifications and implications for the future of cybersecurity in the United States.

As with all topics of debate, the issue of cybersecurity is far from black and white. With the boom of technology and technological devices in the past twenty years, the basic and most pressing questions are still left unanswered, including questions of attribution and deterrence. Who can we blame, and how do we fight back or defend ourselves? These are, essentially, the same questions moderator Lester Holt asked the candidates in that first debate according to the Washington Post transcript: "Our institutions are under cyber attack, and our secrets are being stolen. So my question is, who's behind it? And how do we fight it?"

This paper attempts to investigate the issues of cyber attribution and deterrence in light of the responses that were said in the debate. By looking at these responses, and the motivation behind them, we can better understand what popular opinion is on the topic, regardless of whether that opinion is right or wrong. In no way does this paper attempt to solve the problems of the field, problems that have existed since the very beginning of information technology. Instead, we will look at the responses to tell us two things: (1) popular schools of thought among policy makers regarding cybersecurity, as well as seeing whether or not these claims are grounded in reality, and (2) what the future holds for cybersecurity policy. In looking to the future, we will look particularly at President-Elect Trump's administration's plans for answering the questions of attribution and deterrence. Finally, we will propose some action steps that both the current and upcoming administrations need to take in order to move in a progressive direction.

2 To the Community

The problems of cyber attribution and deterrence run much deeper than simply knowing who to blame and having clear plans of retaliation when we do get attacked. Attitudes about these issues are shaped by years upon years of both technical and political knowledge. A big problem today is that many people in the field either know one side or the other. Engineers responsible for implementation are unaware of important political attitudes towards cybersecurity, and policymakers are just as ignorant of the technical aspects of the problem. One major aim of this paper is that by informing more technically-oriented people about policy and popular opinion, and informing more policy-oriented people about the technical realities of attribution and deterrence, we can begin to break down the walls that make communication difficult between the two groups.

3 Behind the Questions

Lester Holt's questions on cybersecurity mark one of the first times that the topics of cybersecurity became the focus in a national debate. If anything, the past year has shown that an increase reliance on new technologies also means an increased risk of potential information exploitation. The Democratic National Convention email hack back in July successfully interfered with the election process (Tait). The DDoS attack that brought down many Internet services in October was said by experts to be "likely the largest of its kind in history" (Woolf). With multiple incidents of large scale cyber attacks in 2016 alone, it is fitting that this question is asked during an important election. We will continue by looking at the two main questions Lester proposes, and understanding the motivation behind each question.

3.1 "Who's behind it?": A Background on Attribution

At its core, this first question asks the candidates for a solution to the cyber attribution problem: when our sensitive information from our cyber institutions are exploited and used for malicious intent, who do we blame? According to a Dartmouth paper published in 2008, cyber attribution is defined as having the ability to

find the source and identity of an attacker in a given cyber attack (Hunker). However, effective attribution has proven to be nearly impossible because of the many ways to stay anonymous when online, along with the Internet's complex infrastructure. Hackers have the ability to destroy logs and any other trace evidence that would give them away once they gain the correct access privileges. Additionally, while the anonymization of users in various Internet services is often a valuable feature, it also sets up obstacles for effective attribution. Other tricks such as spoofing IP and email addresses, and using virtual private networks also add to the difficulties of cyber attribution. Because of increasingly complex methods and technologies, the ability to properly attribute attacks to the correct individuals and locations becomes more and more difficult everyday.

Because attacks are becoming increasingly frequent, successfully maintaining operations has become more important than attributing all attacks. The difficulty of attribution has made governments and businesses focus less on properly attributing attacks and focus more on preventing attacks. As a result, because of this low focus on attribution, there is very little policy, and a lot of grey area on how to respond to larger-scale attacks, such as the ones that occurred earlier this year.

The reason cyber attribution remains a substantial problem today is because without sufficient attribution, policies and laws - detailing the proper steps to take if an attack is conducted - cannot be formed. This applies both on an international and national level. Under international law, a counterattack of any form is only permitted if and only if the original attack is properly attributed (Kostadinov). On a national level, attribution is similarly necessary so that the government and businesses can fairly prosecute individuals or groups responsible. While technical tools can facilitate attribution, sufficient attribution is often unattainable in sophisticated malicious attacks. In many cases, techniques outside of a technical investigation of the information infrastructure are needed to aid in sufficient attribution. Over time, American intelligence agencies have accumulated a plethora of information on hacking techniques, targets, and patterns. Using this information, along with technical analyses of specific attacks, American intelligence groups have the ability to accurately recognize high-profile state attackers. While behavior from one individual hacker to the other can be random and erratic, state actors have set resources they use and set rules to follow, so with the right resources, recognizing their methods would not be too difficult.

Alternatively, proper attribution of many cyber attacks boils down to catching mistakes made by the attacker. Examples such as poor code and a failure to remove information that would give the attackers away make attributing the right culprits quite easy. Later on, we will see examples of both behavior-matching and mistake-catching as tools for attribution of the recent cyber attacks that influenced the 2016 elections.

3.2 "How do we fight it?": A Background on Deterrence

While this paper focuses mainly on attribution, deterrence is closely linked and must be mentioned. Holt's latter question asks the candidates for a plan to deter attackers. With the attribution problem being as difficult as it is, it is easy to have a pessimistic view on cyber deterrence. The logical argument seems to be that if we are not able to sufficiently attribute an attack, we have no grounds to create

deterrence strategies. However, as discussed above, we have tools and strategies that might not give us a definitive answer, but will nonetheless give us a pretty good idea. The question, however, still remains: can deterrence against cyberattacks be feasible without definitive attribution? According to a paper in the Journal of Cybersecurity, it was found that deterrence works where it is needed most, but fails in most other cases. In other words, deterrence is successful against cyberattacks when the stakes are high, because there are more resources and time dedicated to deterring those attacks. However, in most cases, stakes are lower, so it would be more feasible to increase defense instead of offense (Lindsay).

4 The Candidates' Responses: Reality or Fantasy?

Understanding the candidates' responses to these questions tell us popular opinions and attitudes on cybersecurity. With the difficulty of cyber attribution and deterrence at both technical and political levels, however, we know that these questions do not yet have a definitive and clear answer. Given that fact, we will investigate whether or not the claims that the candidates make are actually grounded in truth.

4.1 Clinton's Response: Russia's Role in Recent Attacks

Hillary Clinton's response begins by mentioning two different kinds of cyber attack adversaries that the United States currently faces: independent hacking groups, and state actors. She continues by explaining that Russia is "the most recent and troubling" (Blake) of these state actors, blaming them for multiple cyber attacks, including the Democratic National Convention hack that shook up the election in early summer of 2016. However, does Clinton have a right to blame Russia when the attribution problem is rampant in the cyberworld? To answer this, we must look at the possible evidence that might point to Russia's involvement in recent cyber attacks.

4.1.1 Cozy Bear and Fancy Bear

Over the years, cybersecurity firms such as Crowdstrike have built a library of hacking techniques in order to catch repeat offenders. As a result, they have eventually been able to recognize the work of two separate Russian hacking groups, which Crowdstrike has nicknamed Cozy Bear and Fancy Bear. After the Democratic National Committee hack, one of the most damaging cyber attacks in recent history, Crowdstrike was hired to find the source of the hack. Within one day, the firm saw signs of work by both Russian groups (Lipton).

Cozy Bear's methods are characterized mainly by spearphishing campaigns. According to Crowdstrike's analysis of the DNC hacks, hackers that are part of Cozy Bear typically include a malicious link in targeted emails, through which hackers would be able to receive a number of Remote Access Tools. With these tools, they can gain access to private networks and find sensitive information. Crowdstrike notes that Cozy Bear's advanced and extensive checks "demonstrate a well-resourced adversary with a thorough implant-testing regime that is highly attuned to slight configuration issues that may result in their detection, and which would cause them to deploy a different tool instead" (Alperovitch). Specifically in the DNC hack,

Cozy Bear seems to have used a Powershell backdoor coupled with a Python script to gain administrator access to the DNC system.

Attacks from the second identified Russian hacking group, Fancy Bear have been identified in a number of different countries. They have been observed to target defense and military information, specifically information that matches the interests of the Russian government. According to the CTO of Crowdstrike, Dmitri Alperovitch, the similar behaviors of these two groups largely rules out cybercriminals and most countries other than Russia (Lipton). Additionally, Fancy Bear many tools to use for hacking, and are known for making phishing sites on spoof domains. Fancy Bear used advanced malware to gain remote access, as well as anti-forensics techniques (erasing logs, replacing timestamps, etc.), to perform the DNC hack.

4.1.2 Guccifer 2.0

The day after the DNC announced that they had been hacked by Russian groups, the personality known as Guccifer 2.0 appeared online, claiming to be the culprit of the DNC hacks. He claims that the United States wrongly blamed Russia for the source of the attacks, and then proceeded to put U.S. documents with sensitive information online to prove his identity.

However, this persona was soon exposed to be fake. After conversing with Guccifer 2.0, it was clear that there were inconsistencies in his communication. Claiming to be Romanian, he could not communicate fluently in a way that only native Romanian speakers could (Lipton). Moreover, it was found that Microsoft Word documents posted by Guccifer 2.0 was edited by someone under a Russian name, an unfortunate operational security failure on the part of the Russian hackers (Tait).

4.1.3 Implications

It does seem that Clinton's claims do in fact have factual backing. Although pure and definite cyber attribution continues to be a problem as technology grows, there is a number of facts pointing to Russia as the source of the attacks. The United States has already acted accordingly, formally accusing Russia for hacking the DNC. Just recently, there has been news of Russia possibly influencing the election for a desired narrative. However, there are still unclear rules and policies on proper deterrence of such attacks.

4.2 Trump's Response: Attribution Defeatism

Trump's response to Lester's questions take quite a different stance from Clinton's. To some people's surprise, Trump took a much more "safe" stance on this topic, and did not definitively give an answer on who he thinks is behind the recent attacks. Instead, he focused on what came about from the attacks, which was the leaked information from the DNC. He emphasized that the likelihood of Russia as the perpetrators is just as high as any other country. On a surface level, it seems that Trump is addressing the difficulty of cyber attribution. Near the end of his response, he states that "the security aspect of cyber is very, very tough. And maybe it's hardly doable" (Blake). Trump's response mirrors what many people think about the future of cybersecurity and the attribution problem: that it is extremely difficult, and might not be achievable in the near future. Instead of attributing

blame to other countries, Trump says that one of the only things that America can do is increase its defense and skill set to match those of competing countries'.

While both candidates encouraged advancing cybersecurity technology, Clinton made a stance and attributed the recent attacks to Russia, while Trump made no such claims. Who is right? The complex nature of the attribution problem makes it extremely hard to tell. However, by understanding these different schools of thoughts amongst policymakers, we hope that both coders and policymakers can begin to communicate and move towards a positive direction.

5 Looking to the Future

What does the attitude of our current President-Elect towards the cyber attribution problem mean for the coming years? As it seems that he is keen on keeping good relations with Putin, if the accusations of cyberattack against Russia go nowhere by the time his administration comes in, it is likely that those investigations will be dropped. More time and money will be spent on increasing defense strategies to be the most secure nation, and perhaps there will be more control given to the policymakers in terms of deciding the future of cybersecurity. Trump remarked in his response that perhaps cybersecurity is "hardly doable" (Blake). It will be interesting to see what the future holds in light of that statement. Will he invest money and resources to make cybersecurity better, or think of it as a lost cause, and halt progress in the field altogether? First and foremost, Trump's campaign slogan resounds. In order to make America great again, it seems likely that he will have to make difficult decisions in the years to come.

6 Action Items

Especially in light of recent events, there is much to be done. First, we implore that future President Trump continue to investigate Russia's involvement in recent hacks. Although the attribution problem does seem technically infeasible, evidence collected over the years tell a different story. Of course, the amount of definitive evidence needed for proper attribution in cybercrime is always up for debate, but at the moment, there is too much evidence pointing to Russia to just ignore. Stopping these investigations into Russia and ignoring facts for the sake of complete attribution would mean several steps back for any possibility of future deterrence.

Furthermore, a more complete policy framework of attribution and deterrence related to cybercrime is necessary in order to move forward. After looking at the evidence from the recent attacks, it is obvious that a clearer framework is required to navigate dealing with cybercrimes across international borders. The current rule of needing "proper attribution" for a counterattack might need to be adjusted for cybercrime, purely because we can only heavily, but not definitively, attribute with the arsenal of tools that we currently have. We must move forward with creating policy for deterring future attacks, for the sake of our national security.

Finally, we advise that both the current and future president should begin having more discussions about prominent issues in cybersecurity, and encourage having discussions with experts that are not just policy makers. With more communication inside and out of the field, a deeper understanding of the issues can arise, leading to

progressive results. Public discussions of cybersecurity issues help keep the public informed on potential cybersecurity risks. It is promising to see the topic brought up in a national debate, but progress can continue or halt depending on the transition from one presidency to the next, so we encourage that those with the power to keep the conversation going.

7 Conclusion

There exists an ever-increasing pressure to have definitive details about cybercrimes, especially during this election season. The problem of attribution and deterrence in the complex infrastructure that is the web, however, often prevents us from being able to do so. In order to find answers of any sort, we have to go beyond pure technical attribution, and make strong conclusions using previous knowledge and experience. Perhaps the definition of a "proper" attribution must be changed to fit the needs of responding to cyberattacks. Or perhaps rules previously set in place do not apply as much out in the cyber world. Whatever the case, our national security currently hinges on many secrets that are hosted in the cyber world. We need to take the proper steps and precautions to prevent exploitation of this information, and continue having discussions about attribution and deterrence. Cyberwarfare is a real type of war that we are fighting, and by not discussing these important issues, we are choosing to lose.

References

Alperovitch, Dmitri. (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee. Retrieved from https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Blake, Aaron. (2016, September 26). The first Trump-Clinton presidential debate transcript, annotated. Retrieved from https://www.washingtonpost.com/news/the-fix/wp/2016/09/26/the-first-trump-clinton-presidential-debate-transcript-annotated/.

Hunker, Jeffrey, Hutchinson, Bob, & Margulies, Jonathan. (2008). Role and Challenges for Sufficient Cyber-Attack Attribution. Dartmouth College. Retrieved from http://www.scis.nova.edu/ cannady/ARES/hunker.pdf.

Kostadinov, Dimitar. (2013, February 1). The Attribution Problem in Cyber Attacks. Retrieved from http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/.

Lindsay, Jon R. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, 1(1),pp. 53-57.

Lipton, Eric, Sanger David E., & Shane, Scott. (2016, December 13). The Perfect Weapon: How Russian Cyberpower Invaded the U.S. Retrieved from http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Tait, Matt. (2016, July 28). On the Need for Official Attribution of Russia's DNC Hack. Retrieved from https://www.lawfareblog.com/need-official-attribution-russias-dnc-hack.

Woolf, Nicky. (2016, October 26). DDoS attack that disrupted internet was largest of its kind in history, experts say. Retrieved from https://www.theguardian .com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.