# *Hacking as a Metaphor: How #russianhacking Influenced Cybersecurity Discourse*

by Justin Flick

## Introduction

Cybersecurity has become one of the most discussed and least understood issues in American discourse. As internet-connected technology continues to permeate further into the lives of everyday people, the interest and controversy around cybersecurity will continue to increase. Unfortunately, there is a significant amount of misinformation surrounding cybersecurity. This has recently come to a head during the 2016 United States presidential election, in which accusations of Russian hacking, unsecured email servers, and unauthorized wiretapping were flung around with impunity. Specifically, accusations that the Russian government "hacked" the election by releasing private Democratic National Convention (DNC) emails in order to change the outcome of the election have proliferated throughout mainstream news and created substantial confusion on what "hacking" really constitutes. The "Russian hacking," as it has been termed, is arguably the most publicized cybersecurity incident in history, and has also been the catalyst for mainstream press to disseminate wildly sensationalized and inaccurate information regarding cybersecurity.

My research aims to analyze the implications of the discourse surrounding the Russian hacking and how this discourse reflects broader societal trends. In order to provide a holistic perspective for this analysis, I approached this idea from both a quantitative and qualitative perspective. The quantitative portion consisted of a Naïve-Bayes sentiment analysis of tweets (Twitter posts) containing #russiahacking and/or #russiagate. The qualitative portion looks at the use of the term "hacking" to describe this incident and draws on George Lakoff's contemporary theory of metaphor to examine how the term "hacking" itself has become shorthand for the metaphor of technology-as-magic. Though there are other metaphors for hacking, technology-as-magic will be analyzed as the central metaphor for hacking in this paper. Finally, I examine the implications of the use of this metaphor on both a macro- and micro-level through the lens of Allen C. Johnston and Merrill Warkentin's Fear Appeals Model.

## Background

The 2016 United States presidential election was a uniquely contentious affair between two candidates that were highly polarized by both the public and the mainstream media. *Politico Magazine* called it "the dirtiest Presidential race since '72" (Cummins, 2016). Republican Donald J. Trump, empowered by an alt-right base, faced off against establishment Democrat Hillary Clinton. Clinton entered the campaign mired in a cybersecurity controversy. She had been under congressional investigation for the use of a private email server during her time as a Secretary of State during President Barack Obama's first term. Throughout the initial stages of the campaign, Clinton and Trump faced off regarding these emails, and it continued to escalate and drive a national conversation on cybersecurity.

The Clinton email scandal would soon be relegated behind a larger cybersecurity scandal. In September of 2015, the Federal Bureau of Investigation informed the Democratic National Committee that one of their computers had been compromised by "the Dukes," a cyberattack team linked to the government of Russia. The DNC thought this was a prank call (Sanger & Shane, 2016). Later, on June 15th, 2016, a hacker known as Guccifer 2.0 leaked a large number of emails that had been stolen from the DNC. These included emails located on the DNC server, campaign strategy documents, and the vulnerabilities of the DNC network (Nussbaum, 2017).

## Qualitative Method

Although there are many competing methods for rhetorical analysis, I find that metaphor analysis provides the unique benefits of both a) providing a framing tool for the implication of rhetorical analysis and b) being easier to understand due to a conceptual reduction to a colloquialism. George Lakoff writes heavily about the use of metaphor as an explanation of rhetoric, and in fact argues that we frame our worldly experiences through metaphors. For example, it is not uncommon to refer to a period time where one is experiencing a large number of negative feelings as one being "down in the dumps." In this way, the idea of being "down" becomes used metaphorically as a replacement for negative. In the same way, Lakoff argues that political discourse is rife with metaphor. He says, "We tend to understand the nation metaphorically in family terms: We have *founding fathers*. We send our *sons and daughters* to war. We have *homeland* security. The conservative and progressive worldviews dividing our country can most readily be understood in terms of moral worldviews that are encapsulated in two very different common forms of family life: The Nurturant Parent family (progressive) and the Strict Father family (conservative)" (Lakoff, 2016). Using this concept, we can frame political ideas as metaphor in order to easily understand the rhetoric used in political discourse and the implications therein.

Metaphor can be a productive lens for rhetorical analysis. However, what defines a metaphor? How does one classify an idea as a metaphor? Regarding these concerns, Rudolph Schmitt argues that Lakoff provides little functional guidance. Schmitt says, "the last publication of Lakoff and Johnson leads to the assumption that metaphorical models, forming the framework of collective thought, have already essentially been identified in their basic form. Both positions bypass the often difficult task of identifying metaphors and reconstructing their contextual meaning" (Schmitt 2005). Luckily, Schmitt offers a method for determining metaphor that is based upon Lakoff's work. The method offers 3 criteria that a word or phrase must meet in order to be considered metaphor. One can classify something as metaphor if:

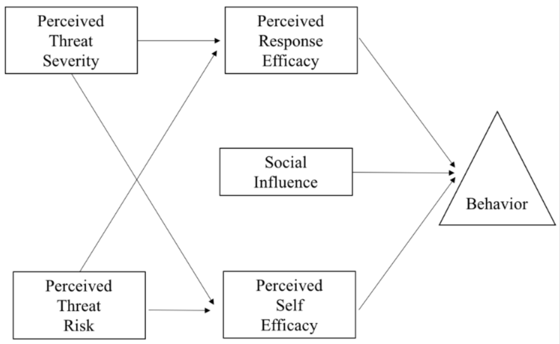
a. a word or phrase, strictly speaking, can be understood beyond the literal meaning in the context; and

b. the literal meaning stems from an area of sensoric or cultural experience (source area),

c. which, however, is transferred to a second, often abstract, area (target area).Schmitt's method offers an appropriate framework through which one can determine metaphor, as it offers praxis to Lakoff's theory. Later, I will argue that the term "hacking" fulfills these three requirements, and thus can be considered a metaphor on its own.

Once one has evaluated whether a term is metaphor, how does one evaluate the implications of the use of said metaphor? Although far more generalized methods exist, I argue that the Fear Appeals Model is the optimal model through which to evaluate the implications of cybersecurity discourse, including the metaphors contained therein. In this model, perceived threat risk refers to the how susceptible an individual believes he or she is to a cybersecurity threat (see Figure 1).

**FIGURE 1: FEAR APPEALS MODEL**



From Johnston and Warkentin (2010).

These perceived notions about the threat lead to a second set of cognitive evaluations under this model. In this case, perceived response efficacy refers to how effective an individual believes the prescribed response is. For example, when dealing with identity theft, the generally prescribed responses include contacting one's bank and freezing accounts when one suspects they may be a victim of identity theft. In this case, this response is generally perceived as effective, and thus one moves to a tertiary level of cognition where one evaluates their own efficacy at implementing the prescribed solution. In the case of identity theft, for most individuals, it is not a monumental task to call one's bank to freeze their accounts. Thus, individuals become more likely to respond in the prescribed way when they perceive it as effective and easy to do.

Ultimately, the analysis prescribed by the Fear Appeals Model terminates in individuals performing certain behaviors. However, there is an independent variable in this model that must always be accounted for outside the tradition flow of the model: social influence. Social influence can be viewed as something resembling social norm, where the generally expected behavioral norms influence one's behavior in response to a cybersecurity threat. Johnston and Warkentein's third hypotheses of the Fear Appeals Model states, "social influence will have a positive effect on end user intentions to adopt recommended individual computer security actions." As I will argue later in this paper, metaphor can modify multiple elements of the model, but at the very minimum, an analysis using this model should be able to justify metaphor as a social influence modifier, especially in the context of Lakoff's framing of metaphors as ideas "we live by."

Ultimately, by utilizing this model, one could functionally evaluate macro-level influences on cybersecurity behavior. Traditionally, this model has been applied on a smaller scale to influencing factors in an organizational environment. However, as the model only intends to provide a framework for evaluating factors that ultimately influence both preventative and responsive cybersecurity behavior, there appears to be no issues with scaling the model to evaluate macro-level influences.

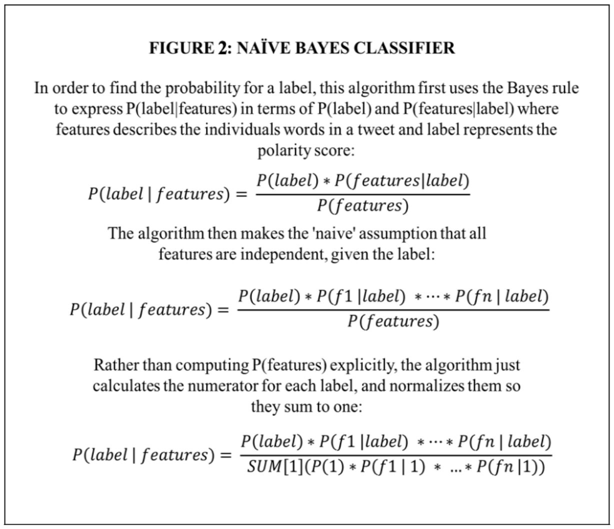


**FIGURE 2: NAÏVE BAYES CLASSIFIER**

In order to find the probability for a label, this algorithm first uses the Bayes rule to express P(label|features) in terms of P(label) and P(features|label) where features describes the individuals words in a tweet and label represents the polarity score:

$$P(label \mid features) = \frac{P(label) * P(features|label)}{P(features)}$$

The algorithm then makes the 'naive' assumption that all features are independent, given the label:

$$P(label \mid features) = \frac{P(label) * P(f1 \mid label) * \cdots * P(fn \mid label)}{P(features)}$$

Rather than computing P(features) explicitly, the algorithm just calculates the numerator for each label, and normalizes them so they sum to one:

$$P(label \mid features) = \frac{P(label) * P(f1 \mid label) * \cdots * P(fn \mid label)}{SUM[1](P(1) * P(f1 \mid 1) * \ldots * P(fn \mid 1))}$$

From Deyasi et al. (2016).

## Quantitative Method

As a method for sentiment analysis, Naïve Bayes classification is a machine learning function intended to classify text based upon Bayes' algorithm. This algorithm states

$$P(c|x) = \frac{P(C|X)P(c)}{P(x)}$$

where P(c|x) is the posterior probability of class (target) given predictor (attribute) and P(x|c) is the likelihood which is the probability of predictor given class (see Figure 2; Deyasi et al., 2016). As applied to text classification and sentiment analysis, Naïve Bayes relies upon the assumption that every input value is generated by first choosing a class label for that input value, and then generating each feature, entirely independent of every other feature (Bird et al., 2009).

In order to perform the sentiment analysis, I had to overcome the challenge of acquiring a large enough dataset to justify my conclusions. Twitter offers an Official API (Application Programming Interface) that allows one to scrape data directly from Twitter's database, but it has a maximum limit on the number of records it will return and only allows one to access tweets from the past 7 days. I found these limits to be a roadblock to establishing a conclusive sentiment analysis, so I decided that I would have to develop my own software to collect the dataset, cleanse the data, and perform the sentiment analysis.

I chose to use Naïve-Bayes classification for the sentiment analysis for a couple different reasons. First, it was the most accessible from a technical perspective. Second, when applied to social media posts, it boasts an 80% accuracy rate in deducing the correct sentiment (Troussas et al., 2013). The Naïve-Bayes methods assigns a polarity score between -1 and 1, based upon natural language processing, and the lexicon dictionaries it is trained with. For the analysis and visualization of the data, I utilized Tableau to calculate maximum and minimum polarity scores, average polarity, and median polarity. Additionally, I labeled tweets with a sentiment score between -1 and -.001 as "Negative," tweets with a sentiment score between .001 and 1 as "Positive" and tweets with a sentiment of 0 as "Neutral."

The idea behind using sentiment analysis as a tool for analyzing rhetoric is simply that it could be helpful to have data justifying one's interpretation of rhetoric. Although there is an anonymization element built into Twitter, I specifically chose to further isolate the authors from their tweets by removing any Personally Identifiable Information (PII) from my dataset. In the end, I managed to collect a dataset spanning 5 years and almost 300,000 tweets. I would argue that such a large dataset would allow me to reduce the weight of potentially problematic tweets.

Although there can be some concerns about the accuracy of sentiment analysis, by utilizing a score based on every word in a tweet rather than simply taking the score from the strongest word in a tweet (as done in other sentiment analysis methods), this method ensures that positive or negative modifiers are taken into account. In the context of examining rhetoric surrounding the Russian hacking incident, it may seem puzzling to utilize a quantitative method to deduce the effects of rhetoric. However, the method I utilize for acquiring data and perform sentiment analysis on that data allowed me to gain insight into a far larger dataset compared to traditional rhetorical analysis. Using my scraper application, I collected a dataset of almost 300,000 tweets, each a unique piece of rhetoric that could be analyzed. However, by utilizing sentiment analysis on this data, I am able to offer an empirical justification for the analysis I perform on the discourse surrounding the hacking. I think this mixed-method approach allows me to draw a holistic conclusion about the rhetoric I examine.

## Qualitative Results and Conclusions

Is hacking truly a metaphor as I would position it? Allow me to work through Schmitt's method. Schmitt (2005) first says that to be metaphor, "a word or phrase, strictly speaking, can be understood beyond the literal meaning in the context." It would appear "hacking" fits this description perfectly. The term "hacker" is often associated with something almost akin to the wizards of fantasy lore, capable of inexplicable tasks that create almost supernatural effects on what we perceive as the "real world." Shows like *Mr. Robot*, movies like *War Games*, and video games like *Watchdogs* offer a portrayal of hackers as capable of bringing down societal infrastructure with the press of a key, while offering little explanation for how this is done. Thus, when cybersecurity incidents occur in everyday life, they are quickly branded as a "hacking" even if they do not necessarily fit the technical definition of a hack.

Schmitt's second qualification for metaphor indicates that "the literal meaning (of a word or phrase) stems from an area of sensoric or cultural experience (source area)." As computers and the internet have continued to permeate every aspect of society, cybersecurity and threats associated with it have equally became more ingrained in societal consciousness. At its most literal meaning, hacking can be defined as unauthorized entry into a computer system or network for nefarious purposes. Although there have been many high-profile hacking incidents (e.g., Stuxnet, the Mirari Botnet, Heartbleed, among others) that could be considered a shared cultural experience, the Russian hacking allegations are arguably the most publicized cybersecurity incident, and thus the largest share cultural experience from which we can derive literal meaning. Thus, as cultural experience shapes the literal perception of hacking in the minds of the general population, it should be able to stand as meeting Schmitt's second qualification.

Finally, Schmitt's third qualification states "which, however, is transferred to a second, often abstract, area (target area)." I would argue the "target area" of this metaphor can be the terminal interpretation of technology-as-magic. As previously stated, ordinary individuals apply the term "hacking" to actions that are not unauthorized compromise of a computer system or network. Non-technical individuals—the majority of the population—often jump to the conclusion that they have been "hacked" when faced with computer errors they do not understand. Popular media refers to self-improvement tips as "life-hacks." Individuals simply create a false correlation between vaguely scientific or technological concepts that they deem to be beyond their understanding as some sort of "nefarious trick" to overcome the cognitive dissonance of their own lack of understanding. Simply put, writing-off concepts as hacking creates an easy explanation for acts that would require a large amount of cognition to explain. Ultimately, I would argue that hacking easily fulfills Schmitt's third qualification.

After examining the term "hacking" through Schmitt's method, it is abundantly clear that we can classify "hacking" as a metaphor in and of itself.

But what exactly is this metaphor? Hacking can be a metaphor for technology-as-magic. In the context of #russianhacking, applying the hacking metaphor to the entire incident beyond the literal hacking action allows one to come to an easy explanation for something as complex as the result of a United States presidential election. In the aftermath of Donald Trump's election to the presidency, many individuals felt as though the result was inexplicable. Returning to the Russian hacking incident, utilizing the term "hacking" as a metaphor for technology-as-magic allows individuals to explain the confluence of a multitude of factors that contributed to the outcome of the election. However, simply attributing an unexpected outcome to some computer wizard casting his hacking spells to influence something as important as an election takes far less cognitive work than sorting through factors like Clinton's email scandal, Trump's ability to motivate voter turnout, or the fact that mainstream media had pushed a narrative that pre-ordained Clinton as the next president, which arguably colored perceptions about how close the presidential race truly was.

What exactly do I mean when I use the phrase "technology-as-magic"? First, allow me to refer to one accepted definition of magic in religious scholarship and anthropology. Magic "consists of a control worked by humans over nature by use of spiritual forces, so that the end result is expected to lie within the will of the person or persons working the spell or the ritual. In theory anybody ought to be able to carry out either, but in practice most societies have produced specialist practitioners in both" (Hutton, 1993). In our modern, technology-driven society we have replaced control over spiritual forces with control over electronic forces. Much like the mages of ancient lore, "hackers" and those who are technologically skilled appear to have otherworldly abilities far beyond the reach of the common person. In reality, the skills required to perform these actions are able to be learned by almost anyone, but like Hutton says, most societies produce specialists in these fields. I use the term "magic" here to make a connection to pre-technological phenomenon. Often society attempts to position the issues and cultural concepts surrounding technology to be some sort of new frontier. In reality, it's simply another medium for the reflection of human nature. While it may be easy to think that computer technology represents some new powerful threat to society, it truly only replicates previous cultural issues.

Now that it has been established that hacking can be viewed as a metaphor, I will discuss the implications of this metaphor through the lens of the Fear Appeals Model. Although the original model was specific to the user adoption of organizational security controls, I believe it has relevance to the implications of the hacking metaphor. Allow me to first examine the impact this would have on perceived threat risk and severity. As previously discussed, the hacking metaphor functions as a label for unexplainable technical phenomena, and the inexplicable nature of the literal meaning of hacking exponentially increases the perceived threat risk. When individuals are fed this metaphor on a societal level, they become socialized to feel at risk of a threat. Specifically, in the context of the Russian Hacking, an individual's overall perceived threat susceptibility and response efficacy are affected by the use of the hacking metaphor to portray this incident. Consider this: If an outside sovereign government could "hack" an election, a cornerstone of United States democracy, what hope does an average person have for warding off cyberattacks? This is the power of the metaphor. Due to the inexplicable nature of these "hacking" incidents and the continued reliance upon technology in society, it is easy to see how it seems like the threat could be existential. In fact, the threat has been argued to be nuclear. In 2009, Jason Fritz argued that due to the inherent flaws in most nuclear command systems, it is not outside of the realm of possibility that hackers could provoke a nuclear war by confusing early detection systems. As this attack could be performed against multiple nuclear powers simultaneously, one could see the realization of the most destructive cold-war scenarios. Although this scenario seems far-fetched, it is not unreasonable that one could logically draw a path from election hacking to nuclear cyberattacks. However, this is exactly what the framing of hacking as a metaphor would criticize. It is undeniable that there are cyber threats. However, as we continue to misuse the term as a metaphor for the inexplicable, we give rise to paralyzing fears of fantastical doomsday scenarios.

These fantastical scenarios influence perceived response efficacy and self-efficacy. Frankly, when society wantonly uses terms like hacking, with all of the fearful connotations that word implies, to describe incidents from political email leaks to someone guessing a weak password, we create a fear complex that inspires feelings of helplessness in the general population, who see the technical explanations of these issues as beyond their grasp. If anything, many individuals will feel that there is no response, much less an effective response. That's the ultimate problem with hacking becoming a metaphor: it becomes applied to inappropriate scenarios that have real consequences. Specifically, as we misuse hacking as a metaphor for technology-as-magic, we further multiply the perceived difficulty of acquiring the skills necessary to have a modicum of self-responsiveness to cyber threats. Technology, although capable of amazing things, is not magic; it's all based on a series of logic that individuals can learn. The inappropriate use of the hacking metaphor is directly responsible for societal justifications of technical illiteracy. If non-technical individuals view computers as scary in part because there are hackers on the internet, it may lead these individuals to question whether they should bother to learn how to avoid risks while using the internet.

In a world where we have to worry about other governments hacking our election, it becomes easy to fall into a trap of this thinking.

If one feels that they are going to be the victim of a cyberattack anyway, what motivation do they have to engage in time-consuming effective cyber behavior? Truthfully, they have none. They generally believe their best protection is the hope that a hacker will have little interest in their data. On the other extreme, some individuals shun certain technologies due to security concerns. Although this response is less common, these individuals have such low perceived self-efficacy that the only way to protect themselves is to give up certain technologies, like social media websites. Sometimes, certain cyber risks promote a fad of shunning certain technology. For example, in 2016, when FBI director James Comey said that individuals should take precautions to protect their webcams from intrusion, millions of people began taping over their webcams, or even physically breaking them to ensure privacy (Hattem, 2016). However, the far more common response is to engage in risky cyber behavior without pursuing behavioral change. This can lead to a number of consequences, including a higher rate of cyberattacks, especially if these individuals are pursuing risky cyber behaviors in situations where they have access to valuable information like their workplace.

Even if one does not pinpoint the metaphor as the primary input to the Fear Appeals Model, the phenomena discussed above culminates in factors that affect the social influence characteristic of the model. Thus, even while examining other concepts as the beginning input for the model, hacking as a metaphor ultimately still affects the terminal behavior in the ways previously described. It's this concept that allows the analysis of the hacking metaphor within the Fear Appeals Model to serve a dual purpose. It first can serve to explain the implications of the use of the metaphor and create a logical path from the use of the metaphor to individual behavior. Second, when the hacking metaphor is applied through a lens of acting as a social influence, it allows one to use the model in future analysis of influences on cyber behavior with macro-social influence already accounted for. In this way, I hope my analysis can contribute to future research.

## Quantitative Results and Conclusions

The quantitative results are intended to supplement the qualitative analysis. I hypothesized that applying the hacking metaphor to the Russian interference colored perceptions of cybersecurity. While only 24.67% of tweets expressed a positive sentiment, those that were identified as positive were of stronger conviction, possessing both a large average polarity score and a higher media polarity (see Figure 3). This would indicate that

**FIGURE 3: TOTAL DISTRIBUTION, AVERAGE POLARITY & MEDIAN POLARITY**

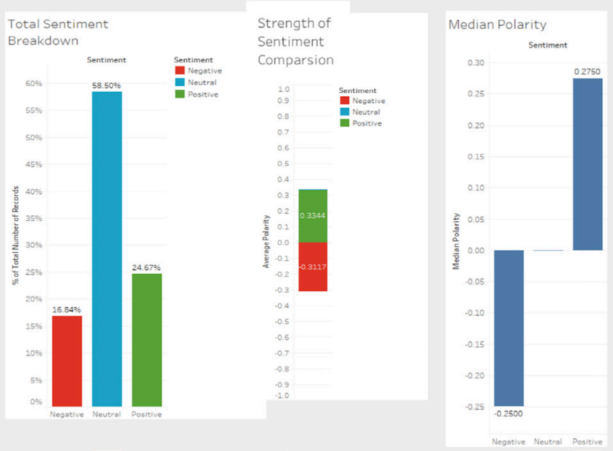
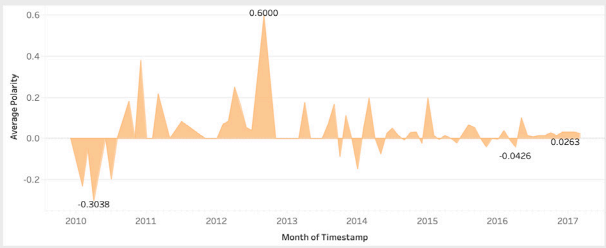


FIGURE 4: TOTAL SENTIMENT OVER TIME



while sentiments of positivity are the minority of responses, those who expressed a positive sentiment felt stronger than those who expressed a negative sentiment. However, the fact that 75.33% of tweets were either negative or neutral indicates that overall response to #russianhacking can be considered negative. Considering the size of the dataset analyzed (300,000 tweets), I would argue that these results justify a supporting analysis.

We can also see the change in sentiment over time (see Figure 4). For the purposes of this analysis, we can disregard tweets prior to May of 2015, though it is interesting that there were such strong swings in polarity prior to media coverage of the Russian incident. It is ultimately telling that the change between months becomes far narrower when we analyze tweets from around the time #russianhacking was first publicized. In April 2016, we can see the lowest monthly polarity within the past year, as the average polarity score of all tweets in that month was -.0426. Conversely, in March of 2017—when I acquired my data set—it had spiked back into the positive range with a score of .0263. To explain this change of sentiment, one can look to the changing media narrative surrounding the Russian Hacking. In March, FBI director James Comey announced that the FBI was investigating connections between the Trump campaign and the Russian government (Rosenberg & Huetteman, 2017). It seems likely that individuals who were previously tweeting negative sentiments about #russianhacking were pleased with the announcement and thus began tweeting positive sentiments. However, as I removed Personally Identifiable Information from my dataset, I am unable to analyze where there are any repeat Twitter user in my data.

Luckily, it is easy to "drill-down" to acquire examples of specific tweets. Take for example, one tweet that scored a polarity score of -0.637. This tweet read "The evil of the #russianhacking is palpable. I can feel it building. Everything about this feels very bad." When analyzed through the qualitative methods I utilized for my previous analysis, this tweet largely reflects that individual's perceived threat risk. This reference to the Russian incident as "evil" conveys great fear of hacking, but it also sits within the framing of technology-as-magic. Many definitions of evil frame it within supernatural forces. ("Evil," 2017) Thus, to call this event "evil" can imply the concept of technology-as-magic.

As another example, allow me to examine a tweet that possesses a polarity score of -1. This tweet reads "But this is the 1st time the CIA and FBI don't seem to care - that's a terrifying difference! #russianhacking." If we once again look to the Fear Appeals Model, we can determine that this tweet expresses a low perceived response efficacy. If an individual is feeling scared about the potential scenario of an outside power hacking their democratic elections, and they also in turn feel that the agencies entrusted with protecting the nation from these sort of incidents are unable to successfully respond, it is only logical to assume they will be engaging in riskier cyber behavior due to a low perceived response efficacy. In the same vein, if an individual is looking only toward these government agencies to protect themselves, this would demonstrate a low perceived self-efficacy. Ultimately, I don't intend for this section to replicate the qualitative analysis; however, these examples serve as a demonstration of the accuracy of the sentiment analysis.

## Conclusion

After the media circus surrounding the 2016 presidential election and the Russian hacking allegations, it seems necessary to re-evaluate how we utilize cybersecurity rhetoric in societal discourse. In order to examine this, I have first argued that the term "hacking" has become a metaphor on its own. In this analysis, I defined "hacking" as a metaphor for technology-as-magic and drew a comparison to medieval conceptions of magic to further illustrate this notion. Next, to evaluate the implications of the use of this metaphor, I utilized Johnston and

Warkentin's Fear Appeals Model to argue that the use of the hacking metaphor amplifies individuals' perceived susceptibility to cyber threats while diminishing both their perceived response efficacy and perceived self-efficacy. Ultimately, I argue that this macro level discourse influences individual cyber behavior in ways that lead to riskier cyber behaviors. Finally, in order to offer empirical support for my analysis, I scraped Twitter to acquire a dataset of 300,000 tweets and then performed a sentiment analysis using a Naïve Bayes classifier in order to examine sentiment trends in response to #russiahacking and #russiagate.

As Lakoff argues that most metaphors have already been discovered, I argue that my research justifies the entry of "hacking" into the metaphor lexicon. Additionally, as it appears that the social influence factor of the Fear Appeals Model seems to be underexamined, I hope that the hacking metaphor can offer a point of praxis for future use of the model. As I have published the software I created for the quantitative portion of my research under an open source MIT license, I also hope that other researchers can find what I have created over the course of this study useful.

For future research, it could be worthwhile to repeat my quantitative analysis with the usernames of individuals who composed the tweets. One could then analyze the change in sentiment of their tweets over time as an indication of evolving perspective. Additionally, although the Naïve Bayes classifier I utilized boasts a high accuracy rate, further research should be done into this classification to further account for lingual phenomena like sarcasm or modified syntax. In regard to the qualitative portion of my research, behavioral scholars could attempt to determine if the hacking metaphor has more of an impact on the Fear Appeals Model as a primary input or as an independent social influence variable. This would shed more light on how the metaphor functionally creates certain implications.

**References**

Bird, S., Klein, E., & Loper, E. (2009). *Natural language processing with Python: Analyzing text with the natural language toolkit* (1st ed.). Cambridge, MA: O'Reilly Media.

Cummins, J. (2016, February 17). This is the dirtiest presidential race since '72. *Politico Magazine.* Retrieved from https://www.politico.com/magazine/story/2016/02/2016-elections-nastiest-presidential-election-since-1972-213644

Deyasi, A., Mukherjee, S., Debnath, P., & Bhattacharjee, A. K. (2016). *Computational Science and Engineering: Proceedings of the International Conference on Computational Science and Engineering.* Beliaghata, Kolkata, India: CRC Press.

Fritz, J. (2009). Hacking nuclear command and control. *International Commission on Nuclear Non-Proliferation and Disarmament.* Retrieved from https://works.bepress.com/jason_fritz/4/

Hattem, J. (2016, September 14). FBI director: Cover up your webcam [Text]. *The Hill.* Retrieved from http://thehill.com/policy/national-security/295933-fbi-director-cover-up-your-webcam

Hutton, R. (1993). *The pagan religions of the ancient British Isles: Their nature and legacy* (Reprint ed.). Oxford: Wiley-Blackwell.

Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Management Information Systems Quarterly, 34*(3), 549–566.

Lakoff, G. (1993). The contemporary theory of metaphor. In A. Ortony (Ed.), *Metaphor and thought* (pp. 202–251). Cambridge University Press.

Lakoff, G. (2016, July 24). Understanding Trump. Retrieved from https://georgelakoff.com/2016/07/23/understanding-trump-2/

Lakoff, G. (2017, March 7). George Lakoff. Retrieved April 17, 2017, from https://georgelakoff.com/blog/

Lakoff, G., Dean, H., & Hazen, D. (2004). *Don't think of an elephant!: Know your values and frame the debate--The essential guide for progressives* (1st ed.). White River Junction, Vt: Chelsea Green Publishing.

Nussbaum, M. (2017, March 3). The definitive Trump-Russia timeline of events. *Politico*. Retrieved from http://politi.co/2mkSJO2

Evil. (2017). In *Oxford Dictionaries*. Oxford University Press. Retrieved from https://en.oxforddictionaries.com/definition/evil

Rosenberg, M. A., Matthew, & Huetteman, E. (2017, March 20). F.B.I. is investigating Trump's Russia ties, Comey confirms. *The New York Times*. Retrieved from https://www.nytimes.com/2017/03/20/us/politics/fbi-investigation-trump-russia-comey.html

Sanger, E. L., David E., & Shane, S. (2016, December 13). The perfect weapon: How Russian cyberpower invaded the U.S. *The New York Times*. Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Schmitt, R. (2005). Systematic metaphor analysis as a method of qualitative research. *The Qualitative Report, 10*(2), 358–394.

Troussas, C., Virvou, M., Espinosa, K. J., Llaguno, K., & Caro, J. (2013). Sentiment analysis of Facebook statuses using Naive Bayes Classifier for language learning. *Information, Intelligence, Systems and Applications (IISA) Conference, 4*, 1-6.