Political Propaganda Spread Through Social Bots

Research · December 2017

DOI: 10.13140/RG.2.2.26725.91365

Summer Lightfoot
New York Public Library

Summer Lightfoot

Professor Sean Jacobs

Media, Culture, & Global Politics

18 December 2017

Political Propaganda Spread Through Social Bots

Introduction

The significance of Barack Obama's use of the internet and online technology as a means of gaining support to win the 2012 U.S. presidential election is well documented (Miller 2008). Social bots and cyber security are increasingly important and worrisome in the age of the internet and more recently in the age of Donald Trump. Social bots have become a pervasive presence on social media platforms, and the use of social bots has been documented in a variety of scenarios, including the manipulation of public opinion and for social spam campaigns (Ferrara 2017). Bots have gained an increasing amount of attention in the U.S. media since the 2016 U.S. election, yet the consensus is that the general public does not really understand what bots are or how they are being used. Bots were also used in the 2017 French and German federal government elections, but they had a different effect on those elections than they did on the 2016 U.S. president election. I asked my family and friends what they thought about cyber security and the use of bots on social media. Each person I asked mentioned Russia, North Korea, fake news, and hacking the 2016 U.S. presidential election, but they did not know anything else about the topic or that France and Germany's elections were affected by bots as well. And with the exception of two or three people, everyone I know uses at least one social media platform and received this information from social media. Recently, within the past few months, there have been a large number of research studies studying the effect on the 2016 U.S. election and the 2017 French and German elections. Bots have been already been used for years, especially by Russia, in its cyber warfare tactics. Social bots or automated programs are used on social media and aimed at influencing politics and have become a cyber threat (AFP 2017). In this paper, I'll compare how bots were used in the 2016 U.S. presidential election to how bots were used in the 2017 French and German elections. I will compare which strategies were used, what type of bots were used, and what effects they each had. This paper will not only focus on cyber security and bots in the United States, but on a global level. Social bots have not only had an effect on U.S. politics, they also have had an effect on global politics, specifically those in France and Germany. One common trait among the campaigns is the adoption of automation tools (social media bots) to generate a large volume of social media posts to support or attack candidates (Ferrara 2).

Lit Review: Research on Bots and Social Media in the U.S.

Going back to the early-to-mid-1990s, there have been books and studies on bots. These studies related to bots as internet agents that can help users search the internet more effectively (Williams 1996). In a study done by the University of Washington in 1993, it was discovered that bots (or software bots, as this study refers to them) are “fully implemented AI agents that [use] a UNIX shell and the World-Wide Web to interact with a wide range of internet resources” (Etzoni and Weld 1994). Bots were seen as “the story of [cyberspace’s] first indigenous species”

(Leonard 1997). As of 1997, bots were discovered to be mere strings of code that had yet to have the capability of changing how things are done for people (1997). Bots were supposed to be able to change how people create, find, and look at things by making everything easier. This was before the age of social media, and bots were used to make the internet and its use more efficient and simpler to navigate. Although the internet went public on August 6, 1991, with the publication of the first website by Tim Berners-Lee at the CERN laboratory in Switzerland, the adoption of the internet was not as widespread as it would become in the later half of 1999 and into 2000 (Bryant 2006). The first social media site that "everyone can agree actually was social media" was a website called Six Degrees, and it lasted from 1997 to 2001. Six Degrees allowed users to create a public profile and then friend other users. Six Degrees even allowed those who didn't register as users to confirm friendships and connections from different people, similar to how modern social media sites (Hale 2017) operate. Social media and bots had no true connection to politics, yet bots were always a part of the internet. News outlets did not regularly discuss or talk about bots because there was no need to do so, and bots were there to help the internet function and run, not disrupt it.

Modern-day social media began with the creation of Myspace, which was followed by Facebook, Twitter, Instagram and many other sites that allowed users to interact with each other. A more modern definition of a social bot is a software application that automatically interacts with human users on social media platforms by imitating human behavior (University 2015). Social bots not only mimic human behavior, they gather information on social media users. In a 2015 study done by the Pew Research Center, it was concluded that 65% of adults in the U.S. were using social media in 2015 compared to only 7% of adults in 2005 (Perrin 2015). Does this mean that the number of bots would have increased to meet the growing number of internet and social media users? In a study on bots by Incapsula from 2013, it was found that 61.5% of all traffic to websites actually consists of bots, and when it reconducted the study in 2015, bots only made up 48.5% of online traffic. Some of these bots are good, but the majority are bad. This means that most bots were used for malicious activity, such as scamming, hacking, impersonating and theft (Zeifman 2013 and 2015). These results mean that the number of bots continues to fluctuate (good bots and bad bots), though human traffic continues to grow as internet use grows on a global scale. The good bots of the internet are used to improve and helps sites run more efficiently. Bots help to make sure that sites are healthy, like Googlebots, which search the internet to maintain Google's index. Bad bots are used to contribute to illegal and criminal activities on the internet, such as scamming, stealing and spamming information (Feather 2016). These bad bots are what continue to cause concern regarding social media sites, news, and global politics.

Social media provides a powerful platform for influencers to broadcast content to a large audience of followers, and bots have become a very useful tool in doing so (Harada et al. 2017). In August 2014, Twitter filed a U.S. Securities and Exchange Commission report revealing that over 23 million active user accounts on the company's social networking site were actually social bots — a particular type of automated software agent written to gather information, make decisions, and both interact with and imitate real users online (Zeifman, 2014). Facebook, Twitter, and Youtube are two of the main sources for social bots to feed off of because the large user base and reliability that users will get their news and information from them. There have been many studies done on social media users, and in a study from August 2017 done by the Pew

Research Center, it was found that 67% of American adults “get at least some of their news on social media”, which increased from 62% in 2016 (Wagner 2017). As the number of people who use social media for news increases, it will become easier for social bots to spread propaganda and fake news to their targets. While the study helps to determine how many people get their news from social media, it would be beneficial to know what news they are looking at and what the sources of that news are, both on a professional and nonprofessional level. It would also help further research on bots if studies showed the location and age of these adults. There have been many studies on American use of social media, but not on a global scale. In order to have a substantial amount of data, there need to be a global study on social media and its use for news. In a study on the influence of bots, it was concluded that these bots are trying to convince people that they are human so that they will have more of an effect on people (Murthy 2016). So far, social bots that have had the most impact on manipulating and persuading are almost impossible to study and track.

In an October 2017 report by Newsweek that used data from the Oxford Internet Institute and independent research, it was found that the U.S., Azerbaijan, Israel, China, Russia and the U.K. use social media (including bots) to manipulate social media (Earle 2017). Social media manipulation and social bot use were at an all-time high during the 2016 U.S. election, making them mostly about the drive behind the election of Trump and his scandals instead of the issues that should have been addressed (Sanders 2016). The study shows that bots were also used during the 2016 Brexit referendum to manipulate social media. The governments of Russia, Israel, Azerbaijan, and China used social media as a means of controlling its people and what information is seen using propaganda. In the case of China, there was a study done on social media analysis and it was found that the Chinese government has long been suspected of hiring as many as 2 million people to surreptitiously insert huge numbers of pseudonymous and other deceptive writings into the stream of real social media posts, as if they were the genuine opinions of ordinary people, but there is little evidence to support this, and therefore it is impossible to prove against the government (King et al. 2017). Russia and China are similar cases in which bots were and are used to persuade the public's views and opinions, and it is thought that the United States hired Russia to do the same during the 2016 election. Russia used social bots and fake accounts to spread pro-Trump propaganda on social media. This has had many negative effects, most prevalently the creation of a divide between Trump supporters and non-Trump supporters as well as the spread of fake news, which has been identified as a major global risk. The global media has played a large part in the spread of fake news, which can be hard to differentiate from real news.

Research has been done and continues to be done on other countries and their elections in regard to bots as well. A computer scientist says there are links between Twitter bots that circulated pro-Trump messages ahead of the 2016 election and bots that engaged in a disinformation campaign against French President Emmanuel Macron while he was a candidate. This means that the U.S. election and the French election are tied together by the use of bots. During the U.S. election there were bots used to spread fake news and propaganda about Donald Trump and in France bots were used to spread positive messages about French National Front party leader Marine Le Pen or negative information about Macron. In one way or another these social bots were used to give one side an advantage over the other. But it was observed that the use of bots in the French election was much smaller than their use in the 2016 U.S. election. He detected between 400,000 and half a million Twitter bots engaged in the U.S. political discussion, where most were pro-Trump and only a small amount were pushing for Hillary Clinton (Chalfant 2017). Whoever hired Russia to create the bots was motivated to do so because they wanted Trump to win. It is clear that they also knew how to do this and target a specific audience of people, similar to other cases of social bot use.

In a study by Indiana University in September 2017, "14 million messages spreading 400 thousand claims on Twitter during and following the 2016 U.S. presidential campaign and election" were analyzed. Evidence was found that social bots played a key role in the spread of fake news and accounts that actively spread misinformation are significantly more likely to be bots. Automated accounts are particularly active in the early spreading phases of viral claims, and they tend to target influential users. Humans are vulnerable to this manipulation, retweeting bots that post false news that many believe to be real news stories. Successful sources of false and biased claims are heavily supported by social bots (Shao 2017). There was another similar study on the UK from the University of Maribur where the posting patterns of twitter users was studied to determine whether or not the users were humans or bots. The study showed that there are patterns specific to bots, but it did not go in-depth into these patterns and behaviors. Bots are quickly improving human behaviors, therefore it is important to research which behaviors are unique to bots (Duh 2017). It is very difficult to determine whether or not an account is run by a human or a bot, but one method has been successful as a solution. Botometer has been proven quite accurate in detecting social bots (Ferrara 4). This information is needed because according to another study done on the 2016 U.S. election it was found that the presence of social media bots can negatively affect political discussion rather than improve it, which in turn can potentially alter public opinion and endanger the integrity of the Presidential election (Bessi & Ferrara 2017). The World Economic Forum recently identified the rapid spread of misinformation online as among the top-ten perils to society (Bolsolver et al 1). A conclusion to the study of social bots in the United States, so far is that they have not had any positive effects in politics, but only negative.

What is a social bot and how are they used in 2017?

A social bot, which is short for robot, performs highly repetitive tasks by automatically gathering or posting information through social media based on an algorithm. Social bots are not neutral and always have a motive or intent, whether it be direct or indirect harm, or benefit. They are created by the developer with intended bias, which is what gives them their meaning. New studies have revealed that bots are becoming highly advanced and are able to manipulate situations. The strategy most often used by social bots is to disseminate pro-government or pro-candidate tweets to sway public opinion in their favor (Brachten et al 3). They use automated propaganda, the ability to turn manipulative situations providing real information or misinformation. Social bots can be used to target organizations or individuals and alter public opinion or information. There are many types of social bots such as spam bots, doppelgänger bots, influence bots, infiltration bots, astroturfing bots. Social bots can be used for good, like chatbots, news bots, and recruitment bots (Stieglitz et al. 7). And, for example, outing human rights or social justice abuse is a good use for bots, but the majority of social bots that have been studied have been used negatively.

Many developers have created social bots for analytical use with sorting and understanding big data and unstructured data as well as social media. In order for a bot to be seen as successful, it has to interact with humans without being detected as non-human (Michael 1). Most social bots have social media accounts that look like real people, act like real people and post content like real people. Social bots, like many real people, have personally attacked politicians and supporters, spammed hashtags in order to redirect users, and overinflate user followers in order to cause political disruption. According to the University of California's Information Sciences Institute, up to 15% of Twitter profiles, which equals 50 million users, are bots (Kupferschmidt 1). Earlier versions of social bots were easier to identify because many posted continuously day and night, now they post differently to look like a real person. Today anyone that has social media most likely has friends or followers that are social bots and do not even realize it.

Bots in the 2017 German and French Elections

As previously discussed, bots played a major role in the 2016 U.S. Election, but they also had an effect on the elections in Germany and France. In the last year, there have been numerous studies on social bots in the political sphere that focus on Germany and France. This has been and continues to be an important area of study and research because fake news websites and social bots deliberately publish misleading, deceptive or incorrect information purporting to be real news for political, economic or cultural purposes (Bolsolver et al 1). Much of the spread of misinformation has a political agenda behind it or a motive. When Russian bots were spreading fake news and propaganda through social bots on social media in the U.S., there was a political meaning behind it, and this might be true for France and Germany as well.

2017 French Election

The 2017 French election had two rounds that took place on April 23, 2017 and May 7, 2017. Between April 27 and May 7, 17 million posts occured on Twitter regarding the French election (Ferrara 1). In a May 2017 study on French hashtags used on Twitter during the election, it was found that the conversations about France were not nearly as poisonous in tone as the conversations on the 2016 U.S. Election. French Twitter users shared many high-quality political news articles (Bolsolver et al 2). This is important to point out because in the United States users were more often sharing low-quality political news articles. The same study on Twitter users also revealed that the largest proportion of content being shared came from professional news organizations and the rest came from personal or organizational blogs, portals, junk news, Russian content and religious content, where 10 percent was junk news and Russian content (Bolsolver et al 4). One thing that has not been addressed in this study is where the small amount of junk news and Russian content came from and what it focused on. By the second round of the French election, more fakes news was shared on social media. In the U.S., 25.9 percent of all the links being shared on social media were from professional news content and 3.4 percent were from government agencies, traditional political parties or other experts. In France, 41.7 percent of all shared news were from professional news and 8.8 percent were from government agencies, traditional political parties or other experts (Bolsolver et al 5).

During the election in France, propaganda was spread from within France, not just from the outside. Extremist groups use social media to spread radical ideas and recruit through propaganda, stock market manipulators have created efforts to game financial systems and conspiracy groups have orchestrated campaigns to distribute fake scientific articles (Ferrara 1). It is not difficult to create a Facebook or Twitter account and use it to spread fake news or propaganda because of how widespread social media is. During the election, there was also a leak of information known as “MacronLeaks”. On a message board site, 4chan.org, users coordinated cyber attacks aimed at revealing sensitive information about then-presidential candidate Emmanuel Macron. 4chan’s appeal is that its users remain anonymous and it allowed users to share information without their identities being revealed. Most of the documents that were shared were easily identified as false, but once they were shared on Twitter, there was no way to stop them from spreading. Wikileaks shared the false documents on their Twitter account, which caused them to go viral (Ferrara 2). It was uncovered that accounts used to support Trump before the 2016 U.S. election have been brought back from a period of inactivity in November 2016 to join the MacronLeaks disinformation campaign (3). This points to a possible exchange or sale of social media bot accounts and makes it more difficult to determine where the accounts originated. Since the end of the election, a significant portion of the bot accounts involved in MacronLeaks have been deleted, suspended, or quarantined. Overall, the 2017 French election was not very affected by the leaks and social bots. This is because the majority of the people involved in the information leak and misinformation was of the American alt-right movement rather than French users. They seemed to be able to differentiate the false information from the truth and it did not sway their opinions on Emmanuel Macron nor did it affect how they voted because he won the election against his competition, Marine Le Pene. Overall, the use of social bots and political propaganda did not have as major of an effect in France than they did in the U.S.

2017 German Election

The 2017 German election took place on September 24, 2017, but there was a spread of misinformation in the months leading up to the election. Since the UK's Brexit Referendum and the U.S. Presidential Election of 2016 fake news has been under much scrutiny for degrading public knowledge of important trends. In 2015, the German parliament's network was hacked by Russia, which led to worries about a potential hack. In December 2016, after the Berlin Christmas market attacks, candidate Angela Merkel was bombarded with bots that generated hate speech messages (Howard 1). She was attacked by accounts that were created by the right wing and in relation to the German refugee debate, they sent her xenophobic messages. She warned the German government about the use of social bots and digital misinformation. The government stated that they would not use social bots and that they strongly condemn their use, but it is out of their hands. In Germany, "Facebook was legally classified as a media company in 2016" which means it will be held accountable for the content it publishes, even fake news (Michael 9). Several political leaders have responded and proposed stricter policies towards the use of propaganda and demanded mandatory labeling for bots on social media (Howard 2). There have been outside geopolitical forces working against Germany, like Russia, which have worked at trying to use social media for their own agenda. If Germany were to create a policy to stop the use of social bots and propaganda during elections, it would further prevent any political hacking or digital compromise of information and votes. In March 2017, Germany's Justice Minister Heiko Maas proposed a law that would impose heavy fines on social media sites that would not take down illegal hate speech and junk news content (Howard 2). During the election period, 17,453 Twitter posts included external news content, where 44.9% of the content came from professional news organizations (Howard 3). The amount of fake news and propaganda that appeared on social media in Germany had very little effect on the election, because the majority of German twitter users posted about candidate Steinmeier and he won. This is different from than in the U.S. because there was a large amount of propaganda shared that ultimately had a major impact on the results of the election.

Analysis and Conclusions

Disinformation on the internet is now rife and if the internet has become our primary source of truth, then we might well believe anything (Michael 9). A major strength from previous research and study is that it brought attention to the mishaps of the election and brought social bots to a mainstream audience. Prior to 2015 and 2016, there was a very small amount of research on social bots. The only concrete research that existed was on bots and social bots on the internet when is was created. Research focused on how bots were helping the internet and how users benefited from them. By the mid-2000s, bots had a different meaning altogether because of their use on social media. Prior to the election, the consensus is that the general public did not know what social bots are or that many of their social media friends and/or followers might in fact be social bots used to spread misinformation and collect data. I realized that I cannot always tell the difference between social bots and humans, unless it is spam or nudity. So in order for social media users to protect themselves and their information, there needs to be awareness of social bots. Once people are aware, their judgement will no longer be clouded or changed by fake news or propaganda. This will in turn give people the facts they need to vote by knowing the truth. The media can help improve the amount of real news that is produced; rather than getting a story out as quickly as possible, they could fact check and source check to ensure they are producing factual and credible new stories.

This is especially true in the case of the 2016 U.S. Election and the 2017 French and German elections. A major limitation to previous research and study is that it focuses on a small size of examples of bot use, but further research needs to be done on a larger scale in regard to comparing the different social bots used in different areas of the world. If more research is done, it could be easier to pinpoint which politicians and government officials used which bots and when to target where they came from and when they were created. It would also be beneficial to research where social bot accounts originated and how long they How long ago were the bots that originated from Russia created? Were they created when Trump announced he was going to run for president or earlier? Questions like these are important to answer and research for a more thorough study of social bots and their use in global politics. If there is a way to track where bots come from and who then it needs to be researched. If we were able to see where, when, who and how these social bots got their start, we could pinpoint a source for their use. Researchers need to discover who is funding and creating these social bots and why they become involved in the first place.

Going forward I conclude that it’s important to set up stronger lines of defense and security against social bots and for everyone that uses the internet to familiarize themselves with the signs of bot behavior. Even going through one's Twitter followers or Instagram followers and taking a look at how many of them are bots can be eye-opening. Since bots continue to evolve, we have to keep an open mind and continue to study them. There is no doubt that bots are here to stay and use social media as a form of changing public opinion. The behavior of bots has not been studied thoroughly or collectively. In order to understand the movements and actions of bots, they need to be tracked and traced by security and information technology professionals so that they can analyze the patterns of social bots. Once they recognize a certain behavior with the social bots, I think it will be easier to come up with a solution to understand their behaviors and stopping them before they attack. This will not only help control bots, it will help improve overall cyber defense. Another step is making government officials aware of how important cyber security is for global politics. Cyber warfare is the modern-age weapon of choice and is likely to start more problems on a global level the more bots and other tools are used to manipulate data and information. As a result of social bots, cybersecurity strategy needs to address new threat sources as an increasing factor in terms of risk exposure (Moon). The deep web and Wikileaks are other tools that I think would be useful in understanding bots. The deep web, the hidden part of the internet, has been studied time and time again and there is information on there that is hidden from the rest of the internet. It is possible with further study, that information about social bots and their political use lies hidden on the deep web.

Preventive approach to bots is important for future elections and political relations. This approach has to perform proactive steps to avoid any bots attacks. These steps can include installing host intrusion prevention applications. The second directions are the non-technical direction which is not related to any technical procedure. This direction focus on user's awareness. This direction can be implemented by different steps like attackers deterrence by applying more sanctions and financial penalties on attackers, legal framework for defence mechanism against bots can be a great step for prevent this type of attacks. Finally user education can play a critical role in preventing bot use (Kamal et al. 2016). In order to prevent future hacking and social bot use in political elections, I think that it is up to the state to make it mandatory that these actions are tracked and monitored.

It cannot be left up to the president or other leaders that might have certain biases for who they want to win the election, which in return affect what they let slide by. Working to improve social bot detection methods is another step in preventing bots by using tools such as BotorNot on social media sites (Grimme 2017). The best way to do so would be to compare and analyze human activity and bot activity. I don't think that most social media users can tell the difference between bots and other people, but with the work of a cyber security professional or analyst, it is possible to track them. In order to protect the future of international security and politics, social bots and social media need to be monitored and controlled because without the certainty of online security, I think that we could be on the verge of a cyber war, which puts everyone at risk

(Ferrara 2017). Going further, I think that the global community could learn from the French, German and U.S. elections that took place in 2016 and 2017. The global community needs to take note of Russia, in particular, and the threat that cyber war and propaganda could have. Cyber warfare, political propaganda, and social bots are on the rise as we continue to advance in technologies. If they were involved it might prove that there is a pattern to social bots and where they might strike next and give officials incentive to further investigate. We all need to work on how we look at social media and how seriously we pay attention to the friends, news and posts we see on a daily basis. As a society we have to pay attention to how the media covers politics as well because the media will increasingly be a major influencing factor. NATO recently published a report about World War III, which will be a cyber war, and the countries of concern are Russia, China, and Iran. Political propaganda is a tool of cyber war and something of major concern.

References

AFP. “Social Media 'Bots' From Russia Distorting Global Politics: Study.” *Information Security News, IT Security News & Expert Insights: SecurityWeek.Com*, 22 June 2017.

Andrew Gauntlett on 10 March 2017, et al. “Social media bots endanger democracy, warns Oxford's internet research chief.” *Oxford Today*.

Bessi, Alessandro and Ferrara, Emilio, Social Bots Distort the 2016 US Presidential Election Online Discussion. First Monday, Volume 21, Number 11 - 7 November 2016.

Bolsolver, Gillian and Clementine Desigaud, Philip N. Howard, Samantha Bradshaw, and Bence Kollanyi. “Junk News and Bots during the French Presidential Election: What Are French Voters Sharing Over Twitter in Round Two?”. Oxford, UK: Project on Computational Propaganda. 4 May 2017.

Brachten, Florian, Stefan Stieglitz, Lennart Hofeditz, Katherina Kloppenborg, and Annette Riemann. “Strategies and influence of social bots in a 2017 German state election- A case study on Twitter”. Australasian Conference on Information Systems. 2017.

Bryant, Martin. “20 years ago today, the World Wide Web was born - TNW Insider.” *The Next Web*, 3 Mar. 2016.

Chalfant, Morgan. “Research links pro-Trump, anti-Macron Twitter bots.” *TheHill*, 6 July 2017, thehill.com/policy/cybersecurity/340844-research-links-pro-trump-anti-macron-twitter-bots.

Duh, Andrej, et al. “Collective Behaviour of Social Bots Is Encoded in Their Temporal Twitter Activity.” *University of Maribor, Faculty of Medicine, Institute of Physiology*, 2017.

Earle, Samuel. “How social media is being used by governments to settle scores and silence critics.” *Newsweek*, 14 Oct. 2017.

Etzioni, Oren, and Daniel Weld. “A softbot-Based interface to the Internet.” *Communications of the ACM*, vol. 37, no. 7, Jan. 1994, pp. 72–76.

Feather, Neill. “Bots And Cybersecurity: What's The Risk?” *Forbes*, Forbes Magazine, 31 Aug. 2016.

Ferrara, Emilio. Measuring social spam and the effect of bots on information diffusion in social media. 27 August 2017.

Ferrara, Emilio. Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election. June 2017.

Grimme, Christian & Preuss, Mike & Adam, Lena & Trautmann, Heike. Social Bots: Human-Like by Means of Human Control?. June 2017.

Hale, Benjamin. “The History of Social Media: Social Networking Evolution!” *History Cooperative*, 26 Feb. 2017, historycooperative.org/the-history-of-social-media/.

Harada J. et al. “Prediction of Elevated Activity in Online Social Media Using Aggregated and Individualized Models”. In: Missaoui R., Abdessalem T., Latapy M. (eds) Trends in Social Network Analysis. Lecture Notes in Social Networks. Springer, Cham. 2017.

Howard, Philip N., Lisa-Maria Neudert, Bence Kollanyi. “Junk News and Bots during the German Federal Presidency Election: What Were German Voters Sharing Over Twitter?”. Oxford, UK: Project on Computational Propaganda. 27 March 2017.

Kamal, Saif Uldun Mostfa, et al. “SURVEY AND BRIEF HISTORY ON MALWARE IN NETWORK SECURITY CASE STUDY: VIRUSES, WORMS AND BOTS.” *ARPN Journal of Engineering and Applied Sciences*, vol. 11, no. 1, Jan. 2016.

King et al. How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review, 111*(3), 484-501. 2017.

Kupferschmidt, Kai. “Bot-hunters eye mischief in German election: Fake social media profiles are proliferating, but their potency is unclear”, Science Mag: Vol 357, Issue 6356. 15 September 2017.

Leonard, Andrew. *Bots: the origin of new species*. Hardwired, 1997.

Michael, Katina. “Bots Trending Now: Disinformation and Calculated Manipulation of the Masses”, IEEE Technology and Society Magazine, 8 June 2017.

Miller, Claire Cain. “How Obama's Internet Campaign Changed Politics.” *The New York Times*, The New York Times, 7 Nov. 2008.

Moon, R David. “Social Bots Among Us - is Your Cybersecurity Strategy Prepared?” *LinkedIn*, 31 July 2016.

Murthy, Dhiraj et al.. "Automation, Algorithms, and Politics| Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital." *International Journal of Communication* [Online], 10 (2016): 20. Web.

Perrin, Andrew. "Social Media Usage: 2005-2015." *Pew Research Center: Internet, Science & Tech*, 8 Oct. 2015.

Sanders, Sam. "Did Social Media Ruin Election 2016?" *NPR*, NPR, 8 Nov. 2016.

Shao, Chengcheng , et al. "The spread of fake news by social bots." *Indiana University, Bloomington*, 26 Sept. 2017.

Stieglitz, Stefan, Florian Brachten, Bjorn Ross, and Anna-Katharina Jung. "Do social bots dream of electric sheep? A categorization of social media bot accounts". Australarian Conference on Information Systems. 2017.

UNIVERSITY, SERVERPRONTO. "How to Detect Social Media Bots?" *Serverpronto.com*, 15 Apr. 2015.

Wagner, Kurt. "Two-Thirds of Americans are now getting news from social media." *Recode*, Recode, 7 Sept. 2017.

Williams, Joseph. *BOTS and other Internet beasties*. Sams.net, 1996.

Zeifman, Igal. “Report: Bot traffic is up to 61.5% of all website traffic.” *Incapsula.com*, 9 Dec. 2013.

Zeifman, Igal. “2015 Bot Traffic Report: Humans Take Back the Web, Bad Bots Not Giving Any Ground.” *Incapsula.com*, 9 Dec. 2015.