Computational Propaganda in the United States of America: Manufacturing Consensus Online

Samuel C. Woolley, *University of Oxford*
Douglas R. Guilbeault, *University of Pennsylvania*
A Network Analysis of Twitterbots during the 2016 Election

Table of Figures

Figure 1: Screenshot of Posts from a Pro-Trump Twitter Bot........................................................................... 7
Figure 2: Screenshot of Ruffini’s Twitter Post Detailing an Alleged Botnet ......................................................... 11
Figure 3: A Bot Urging Twitter Users to Report Ted Cruz to the FCC .............................................................. 12
Figure 4: Political Valence of Hashtags ............................................................................................................. 14
Figure 5: Building Blocks of Retweet Networks ................................................................................................ 16
Figure 6: Graphic Illustration of K-Core Decomposition ..................................................................................... 17
Figure 7: K-Core Distribution for Human and Bot Users ..................................................................................... 18
Figure 8: Bots with Top Twenty Betweenness Centrality Scores ........................................................................ 19
Figure 9: Directed Network of Humans Retweeting Bots with Threshold Removing All Users with Only One Connection .................................................................................................................. 20
Figure 10: Comparing the Largest Botnet within the Retweet Networks for Trump vs Clinton Related Hashtags .................................................................................................................. 21
Abstract

Do bots have the capacity to influence the flow of political information over social media? This working paper answers this question through two methodological avenues: A) a qualitative analysis of how political bots were used to support United States presidential candidates and campaigns during the 2016 election, and B) a network analysis of bot influence on Twitter during the same event. Political bots are automated software programs that operate on social media, written to mimic real people in order to manipulate public opinion. The qualitative findings are based upon nine months of fieldwork on the campaign trail, including interviews with bot makers, digital campaign strategists, security consultants, campaign staff, and party officials. During the 2016 campaign, a bipartisan range of domestic and international political actors made use of political bots. The Republican Party, including both self-proclaimed members of the “alt-right” and mainstream members, made particular use of these digital political tools throughout the election. Meanwhile, public conversation from campaigners and government representatives is inconsistent about the political influence of bots. This working paper provides ethnographic evidence that bots affect information flows in two key ways: 1) by “manufacturing consensus,” or giving the illusion of significant online popularity in order to build real political support, and 2) by democratizing propaganda through enabling nearly anyone to amplify online interactions for partisan ends. We supplement these findings with a quantitative network analysis of the influence bots achieved within retweet networks of over 17 million tweets, collected during the 2016 US election. The results of this analysis confirm that bots reached positions of measurable influence during the 2016 US election. Ultimately, therefore, we find that bots did affect the flow of information during this particular event. This mixed methods approach shows that bots are not only emerging as a widely-accepted tool of computational propaganda used by campaigners and citizens, but also that bots can influence political processes of global significance.

Introduction

Political campaigns, candidates, and supporters have made use of bots in attempts to manipulate public opinion in the United States for almost a decade. The role of bots during the 2016 election, as tools for spreading disinformation, attacking users, and amplifying perspectives, has been much discussed in recent news media. This working paper seeks to build an understanding of the role of bots during this pivotal event. It focuses on bots as a tool for the proliferation of computational propaganda, best defined as the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion.

This working paper seeks to fill crucial gaps in our understanding of how political bots, and computational propaganda in general, are shaping the political landscape in the US, with global consequences. It reviews the history of bot interference in US politics, and it focuses on the use of bots to influence the recent 2016 US election. The paper is divided into two parts. Part A reports the results of nine months of ethnographic fieldwork on the campaign trail, including interviews with bot makers, digital campaign strategists, security consultants, campaign staff, and party officials. This on-the-ground investigation revealed that campaigners, citizens, and government representatives tell surprisingly inconsistent stories about the use of bots and their capacity to influence political processes. Part B provides a quantitative response to the question of whether bots were able to influence the flow of political information over Twitter during the election. Using over 17 million tweets, Part B shows how bots were able to reach central positions of measurable influence within retweet networks during the US election. In the final section, we discuss the combined implications of our investigations, with particular concern
for the policy implications surrounding the rising culture of computational propaganda in the US and abroad.

When the political problem of bots is articulated effectively, concrete analyses can be undertaken to enrich qualitative reports about how bots shape the landscape of power and propaganda. In this working paper, we frame the problem of bot influence as a problem of how they influenced the informational dynamics of political discussion over Twitter. The mixed methods approach herein provides a unique perspective on the role of bots in US politics. Ethnographic investigations expose the extent to which bots are nested within a complex system of political institutions and actors, with competing interests and conflicting stories. One of the most important observations to draw from this analysis is that, behind the scenes, bots have become an acceptable tool of campaigners and are a prime example of the new augmented age of computational propaganda. On the other hand, bots hold the promise of democratizing propaganda by taking it out of the hands of the elites and allowing citizens to spread their messages and boost their own voices via the megaphone effect. So far, however, bots have primarily been used to spread extremists’ views in uncritical allegiance to dominant candidates, raising vital concerns about the use of bots to achieve what we call “manufactured consensus”—or the use of bots in creating the illusion of popularity for a candidate who might otherwise be on the political fringes.

While digital strategists and other technically savvy supporters have revealed that they use social media bots in attempts to change people’s perspectives, they often did not know whether or not they actually drove people to consume information differently. The network analysis in this working paper reveals that bots did indeed have an effect over the flow of information among human users. The aim of the network analysis was to observe whether bots infiltrated the core of the discussion network over Twitter and thus the upper echelons of influence. The finding was yes, bots did infiltrate the upper cores of influence and were thus in a position to significantly influence digital communications during the 2016 US election.

An Ethnographic Investigation of Bots and Campaigns in 2016

Halfway through nine months of fieldwork on the 2016 US presidential campaign trail, a light-bulb moment occurred. Cassidy, a digital strategist who did contract work for the Trump campaign, used the language of Communication scholars to explain the unlikely political ascendance of Donald Trump. Cassidy brought up agenda setting, a theory which suggests that the more often something comes up in the media, the more likely the public is to consider it important (McCombs, Shaw, & Weaver, 1997). Agenda setting is generally about power, specifically the power of the media to define the significance of information.

Cassidy said that the Trump campaign turned the concept upon its head. He said, “Trump’s goal from the beginning of his candidacy has been to set the agenda of the media. His strategy is to keep things moving so fast, to talk so loudly—literally and metaphorically—that the media, and the people, can’t keep up” (Cassidy, personal communication, November 2016). Cassidy made it clear that Trump’s campaign wanted to create scenarios wherein the media couldn’t resist covering him. Cassidy said that this was a conscious strategy. Trump inverted, or perhaps
twisted, the typical structure of agenda setting. Cassidy argued that the candidate’s fast-paced rhetoric and willingness to speak “off the cuff” gave an impression of authenticity that demanded attention. By defying expectations for what a presidential candidate should say and do, and doing so constantly, he set the media’s agenda which in turn set the public’s. As a report from the Harvard Shorenstein Center on Media, Politics, and Public Policy put it:

> Overall, Trump received 15 percent more coverage than [Clinton] did. Trump also had more opportunities to define Clinton than she had to define him. When a candidate was seen in the news talking about Clinton, the voice was typically Trump’s and not hers. Yet when the talk was about Trump, he was again more likely to be the voice behind the message. “Lock her up” and “make America great again” were heard more often in the news than “he’s unqualified” and “stronger together”. (Patterson, 2016)

According to Cassidy and other digital strategists, candidates and campaigns are tirelessly working to stay up to date on a variety of evolving digital campaigning tools. Strategists associated with both the Republican and the Democratic campaigns said that interactive advertisements, live-streamed video, memes, and personalized messaging all played a role in the spread of partisan content during the 2016 election. According to the campaign officials, consultants and party employees have the tacit goal of using these tools to affect voter turnout. However, informants said that these tools were also used to achieve other, less conventional, goals: to sow confusion, to give a false impression of online support, to attack and defame the opposition, and to spread illegitimate news reports.

One tool has risen to prominence among those used to achieve these latter aims, that is, to spread propaganda online. That tool is the political bot. Previous research shows that political candidates and campaigns in the United States and abroad have made use of these automated software devices in attempts to manipulate public opinion on social media (Ratkiewicz et al., 2011a; Woolley, 2016). The 2016 US election, however, was a watershed moment for the use of political bots and computational propaganda. Research from several sources suggests that political bot usage was at an all-time high during key moments of this particular election (Bessi & Ferrara, 2016; Howard et al., 2016; Ferrara et al., 2016).

**Campaign Fieldwork**

The goal of this qualitative work is to study the ways in which political parties and their campaigns used digital media, bots, and automation during the 2016 US presidential election. This was achieved using a combination of field research methods. Observation, interview, participation and process tracing were used from the beginning of February 2016, ending in the weeks after the election that November – a total of approximately ten months of material used to build understandings of the campaigns and their digital manoeuvres. Time in the field was motivated by a desire to create a diagnostic, humanized view of the way in which people affiliated with the parties made use of bots.

This project aims to build a comprehensive understanding of digital campaign methods for communicating information. Particular interest is given to communication methods that make use of computational tools (automation, algorithmic design) and attempt, often subtly, to manipulate
public opinion. These efforts are part of spreading computational propaganda. Tools for dissemination and obfuscation, such as political bots, are of central interest to this research. But so are the strategies that these tools helped realize: the spread of false news reports, “shitposts” (highly negative memes), and attacks upon journalists.

In order to understand where these tactics and tools originated, time was spent in several states during the primaries, and also at campaign gatherings, at digital strategy workshops, and at party nominees’ home turf events in New York City. This allowed us to gain a sense of the culture of the campaigns through what Clifford Geertz (1973) called “deep hanging out.” Participant observation formed a portion of this work. It began with spending time meeting people, volunteering, and learning about the structure of the campaign apparatus. This helped to gain access beyond the hordes of volunteers and to get in touch with those in the know about digital strategy who had the ability to make assertions about party and campaign strategy.

One part of this process involved volunteering and interacting with the campaigns: using applications like MiniVan to canvas for Bernie, knocking on doors in NYC’s Chinatown and the Bowery, making calls and sending texts in Detroit for Clinton, and even hanging out with campaign folks at the pre-emptive Michigan primary “victory” party that turned out to be a shocking precursor for the later electoral loss in that state. It meant correspondingly with people working for the Trump campaign, going to their campaign headquarters – and being turned away – twice, and talking to crowds of red-cap-wearing supporters at various rallies. During the New York Republican primary, this also included attending a very sparse meet-up at a Chelsea tech store organized by a relatively unknown digital firm working for Ted Cruz. The company’s chief data scientist and director of sales outlined, in deep detail, the firm’s work in “behavioural analytics.” The firm would turn up later in the campaign, and in many sensational media stories, when it began deploying it’s alleged “psychographic” digital tactics for the Trump campaign – known by the now familiar name Cambridge Analytica.

Other ways of staying up to date involved signing up for every mailer from the campaigns, following the candidates on social media, and religiously scouring digital messages and metadata. This led to familiarity with the regular re-tweeters and likers – especially those that showed signs of automation. Here, data gathering consisted of taking screen shots of public content and writing descriptive memos about what they showed. These, and other field notes, were stored using Zotero and organized with Microsoft Excel. It is worth noting that political bots are often short-lived. They either fulfil their task, and are then taken down by deployers to avoid a trail, or they are deleted by social media platforms because they violate terms of service when they show signs of spam or of being used to harass other users. Several snapshots of these bots are included here to demonstrate particular tactics and types, but also to preserve now non-existent automated accounts.

Important campaign events and important moments that could not be attended were followed online. News reports, community documents, and archived social media material were used to build further understandings of such events. All media reports on bots and US politics were captured using Zotero. Reflective accounts, through one-on-one interview, were gathered from experts who had been in attendance or who had worked with or for the campaigns. Contradictions in stories about how events played out, or about how automation or other social
media tools were used, regularly occurred. This was a highly contested, and strategically ruthless, campaign. Parties and campaigns, and even factions who worked within them, disagreed about how things happened—and about what truth looked like. Cross-referencing and online research allowed for clarity when discrepancies in accounts arose. When possible, these contradictions are preserved rather than simplified, demonstrating the wide range of perspectives about the truth—especially as it relates to the use of bots in politics.

Figure 1: Screenshot of Posts from a Pro-Trump Twitter Bot

Source: Authors’ screenshots, April 2016.

Note: Two screenshots from @DyanNations, one of several hundred accounts that conservative strategist Patrick Ruffini alleged were used to attack Ted Cruz on behalf of Donald Trump. In addition to tweeting pro-Trump messages, the account sent out Russian memes and ads for fake followers. It is still online but hasn’t posted since June 2016.

Agenda Setting and the Campaign

In writing their theory of agenda setting, McCombs and Shaw (1972) wrote specifically about the media’s ability to guide voters through the information provided during the 1968 presidential campaign. The prescient and popular line from Cohen succinctly explains the role of the media in prioritizing information: the press “may not be successful much of the time in telling people what to think, but it is stunningly successful in telling its readers what to think about” (Cohen, 1963). McCombs and Shaw argue that during a heavily contested election, like the ones in 1968 and 2016, the power of the press to shape public attention is significant. They write that “the data suggest a very strong relationship between the emphasis placed on different campaign issues by the media (reflecting to a considerable degree the emphasis by candidates) and the judgment of voters as to the salience and importance of various campaign topics” (p. 181).

The question that arises is: who decides what the media reports on? The traditional answer from the discipline of Communication is gatekeepers, editors, editorial boards, and the like. But during an election like the one in 2016, where the traditional campaign playbook is thrown out by one candidate, thus causing that candidate to draw extraordinary attention, that candidate gains a notable amount of power in driving media coverage.

Traditional media’s willingness to cover Trump for free and to put him at the centre of the presidential conversation was one part of his success. Another major portion, however, can be
attributed to the way in which he and his supporters used social media. Twitter proved a crucial tool for Trump, a soapbox that bypassed gatekeepers and allowed him to circulate content regardless of form. This content was then legitimized by constant coverage by major TV news channels, national radio programmes, and a new media tool—hordes of political bots, automated social media accounts built to look like real users and used to artificially boost content.

Armies of bots allowed campaigns, candidates, and supporters to achieve two key things during the 2016 election: 1) to manufacture consensus and 2) to democratize online propaganda. Social media bots manufacture consensus by artificially amplifying traffic around a political candidate or issue. Armies of bots built to follow, retweet, or like a candidate’s content make that candidate seem more legitimate, more widely supported, than they actually are. This theoretically has the effect of galvanizing political support where this might not previously have happened. To put it simply: the illusion of online support for a candidate can spur actual support through a bandwagon effect. Trump made Twitter centre stage in this election, and voters paid attention. As the New York Times put it, “For election day influence, Twitter ruled social media” (Isaac & Ember, 2016).

Political bots also made it possible for average citizens, people well outside of Washington or the professional campaign apparatuses, to amplify their own viewpoints online. The reach and sheer numerical strength of Twitterbots allowed anyone with some coding knowledge, or connections to groups using automation software, to create their own propaganda network. The question of whether campaigns themselves used political bots to spread “fake news” was, and continues to be, a smoking-gun issue in US politics. However, the democratization of online propaganda is also an especially salient issue. While government departments, academics, and journalists continue to search for evidence that campaigns used these means to manipulate public opinion, they tend to ignore the fact that anyone can launch a bot or spread fake news online. It was these citizen-built bots that probably accounted for the largest spread of propaganda, false information, and political attacks during the 2016 election.

According to many of the people interviewed for this chapter, including political bot makers and campaign personnel, the goals of bot-driven tactics are manifold: to create a bandwagon effect, to build fake social media trends by automatically spreading hashtags, and even to suppress the opinions of the opposition. Bots allow for the democratization of digital propaganda because they make it possible for one person or group to massively enhance their presence online. Open APIs, and laissez-faire approaches to automation on sites such as Twitter, allow regular people to deploy their opinions en masse. As one bot builder stated: if one person operating one profile can automate their profile to tweet every minute, just think what one person running one thousand automated profiles can do.

The Media and the Campaign

In order to understand the success of the Trump campaign’s media strategy, it is useful to look to the early days of the campaign. In January 2016, Trump began gaining traction as a viable Republican candidate for the presidency. In an opinion article for the New York Times written that same month, Peter Wehner, a senior fellow at the conservative Ethics and Public Policy Center and employee of three Republican presidents, said he would never vote for Trump. He
summed up the fears of the growing “Never Trump” movement taking hold within the Republican Party when he said that “no major presidential candidate has ever been quite as disdainful of knowledge, as indifferent to facts, as untroubled by his own benightedness” (Wehner, 2016).

Informants, including people who had done digital work for Republican presidential and senatorial candidates, saw Trump as a “loose cannon” willing to say and do anything. They echoed Wehner’s concerns about his lack of military or government experience. So did key members of the Republican establishment. Mitt Romney, the 2012 Republican presidential candidate, gave a speech in which he said: “Dishonesty is Donald Trump’s hallmark … He’s not of the temperament of the kind of stable, thoughtful, person we need as a leader. His imagination must not be married to real power” (Associated Press, 2016). Romney and his compatriots argued that it was only a matter of time before Trump did something so off-colour that he would be drummed out of the race, but nothing seemed to be able to touch him. Media storms about Trump mimicking a disabled New York Times reporter, impugning Senator John McCain’s war record, and harassing women did not stick. Any one of these stories might have undone another candidate. Suddenly, however, Trump would say or do something else and a misstep would be forgotten in the next day’s media cycle.

Then, of course, Trump won the presidency.

Experts from every quarter have since weighed in on what caused the Trump win. Communication scholars have suggested it has to do with the fact that, despite his disregard for traditional advertising and what his supporters have derisively deemed “the mainstream media,” he received far more media attention than any other candidate. According to MediaQuant, a firm that tracks media coverage of candidates, Trump received nearly five billion dollars’ worth of free media attention compared to Clinton’s three million (Harris, 2016). Scholars have also noted that the Trump campaign was innovative in its use of social media (Albright, 2016; Beckett, 2016). An article in Wired magazine went as far as to say that sites like Facebook and Twitter won Trump the presidency (Lapowsky, 2016). The same article noted that “social media was Trump’s primary communication channel.” In a conversation with CBS’s 60 Minutes (2016), Trump himself said that Twitter and Facebook were key to his victory.

The numbers from the Wesleyan Media Project’s (Franklin Fowler et al., 2017) report on campaign spending suggest that, as with the polls, the metrics by which advertising agencies seek insight into political wins proved to be misleading when it came to an actual outcome. Television advertising seemed to have very little bearing on success: Clinton spent $258 million to Trump’s $100 million. On local cable, Trump had less than a 1 percent market share. Clinton even dominated digital ads (desktop, display, pre-roll) and had a 73 percent share of nationally focused digital ads, with Trump at only 27 percent.

Social media’s affordances for democratizing communication and organization have long been discussed by scholars concerned with politics and the media (Benkler, 2006; Howard & Hussain, 2013; Owen, 2015). More recently, there has been a normalizing pattern on sites like Facebook and Twitter. That is, political elites have figured out how to harness social media to exert power and control (Karpf, 2012). Donald Trump used one digital tool in particular to circumvent the need for traditional political advertising. That tool was Twitter.
As one informant, a conservative social media expert named Clint, put it: “Trump used Twitter as a megaphone, as a tool to get his campaign message heard above all others” (Clint, personal communication, April 2016). However, suggesting that the Trump campaign’s success in harnessing social media, an emergent version of political normalization or the elite use of technology to manipulate public online, won him the presidency is off the mark. In fact, a somewhat oppositional phenomenon, the democratization of propaganda, was also key to his success. Together, the campaign’s creative use of social media and supporters’ use of large-scale social automation allowed the agenda of the media to be set in favour of Trump.

The Megaphone Effect

Discussions about the Trump campaign’s attempts to speak over all other news – what Clint called “megaphoning” – became a clear theme in interviews. For instance, another research informant, Al, echoed Clint’s claims of this amplified communication tactic. Al was and is a high-ranking member of the Republican Party apparatus. Al explained that the campaigns he had worked on treated “digital” (online marketing) like the “Wild West.” He said, “Anything goes as long as your candidate is getting the most attention.”

Generally speaking, social media bots play a fairly heavy-handed role in amplifying political messages. The idea behind political botnets is one of numbers: if one account makes a splash with a message then 1,000 bot-driven accounts make a flood. Armies of bots pretending to be human, what some call “sock-puppet accounts,” computationally and automatically extend the ability of the deploying party to spread messages on sites like Twitter. Political botnets, large networked collections of bots, are no exception. During the 2016 election, numerous occurrences of bots were catalogued as being used to drive up traffic around a particular event or idea.

For instance, at the height of Pizzagate, the conspiracy that linked the Clinton campaign to an alleged human trafficking and child abuse ring, automated shell accounts rampantly spread memes putting Clinton campaign Chair John Podesta and the candidate herself at the centre of the fabricated controversy. A disproportionate number of the accounts generating traffic on Pizzagate appeared to originate in Cyprus, the Czech Republic, and Vietnam (Albright, 2016b). According to the Washington Post, “[A]s the bots joined ordinary Twitter users in pushing out Pizzagate-related rumors, the notion spread like wildfire” (Fisher et al., 2017). Pro-Clinton bots also spread attacks on Donald Trump, though they were about 1/5 as active as the pro-Trump bots during key election events (Howard et al., 2016).

One example of bots amplifying political messages during the campaign stands out. In April 2016, conservative political strategist Patrick Ruffini, webmaster of the 2004 Bush/Cheney campaign and former eCampaign Director of the RNC, sent out a series of tweets suggesting that bots were being used to attack Ted Cruz. Figure 1 is an example of one of the bots Ruffini identified. The Daily Caller and the National Review quickly picked up the story, both suggesting that the bots were potentially part of a broader network of “fake” Trump Twitter traffic. Ruffini made a spreadsheet of nearly 500 allegedly automated accounts, many of which were deleted or became inactive just after he publicly shared the list. Figure 2 shows a tweet of this spreadsheet. Most of the accounts in the document had no followers, copied one another’s messages, and sent out advertisements alongside political content. Ruffini found that they were
also being used to support the Trump campaign. The strategist noted that the bots sent out 400,000 messages about Trump, and nearly 2 million tweets in total, over the course of a month. The same accounts retweeted Dan Scavino, Trump’s social media director, nearly 15,000 times.

Figure 2: Screenshot of Ruffini’s Twitter Post Detailing an Alleged Botnet

Source: Authors’ screenshot, April 2016.

Note: Ruffini sent out several messages on Twitter about the accounts in question. He also compiled a spreadsheet of accounts, complete with metrics and links, and shared this on the platform.

Ruffini’s main issue with the accounts was that they were urging those who had received Ted Cruz campaign robocalls to report him to the Federal Communications Commission for violating political media regulations. In a twist of irony, a group of automated Twitter accounts were being deployed to mobilize voters against automated campaign phone calls. The novel tactic of using bots to make assertions about campaign law had not been seen in two previous years of research about political bot use in other countries. Also interesting was the fact that this was a group of pro-Trump Republican bots being used to attack Ted Cruz, another Republican. In an interview with Politico, Ruffini said, “A lot of these unsavory tactics that you would see in international elections are being imported to the US.” He also noted that “there is very clearly now a very conscious strategy to try to delegitimize opposition to Trump” (Schreckinger, 2016).
Ruffini’s allegations, and his efforts to catalogue information about the accounts in question, provided a reason for further examination of party-focused or candidate-focused bots. There is evidence that US political actors have previously used bots in attempts to manipulate public opinion (Ratkiewicz et al., 2011a; Metaxas & Mustafaraj, 2012). During the 2012 election cycle, Mitt Romney’s campaign was accused of buying thousands of followers on Twitter in a bid to seem more popular (Coldewey, 2012). In 2010, researchers discovered a botnet purpose built to attack Martha Coakley, the former Massachusetts attorney general, by alleging she was anti-Catholic (Mustafaraj & Metaxas, 2010). At the time, Coakley was in a tight race with Scott Brown in the special election to fill Ted Kennedy’s senate seat. Brown eventually won the race. In these cases, bots were used to support US political candidates, and even to attack the opposition. Was this a common campaign tactic, however?

The same week that the anti-Cruz botnet was launched, contact was made with a well-placed member of the Republican Party. The informant, Jane, had worked on several high profile political campaigns and was, at the time, employed by the Republican National Committee. When asked if she had seen campaigns use social media bots before, she answered bluntly, “Yes, absolutely. It’s a common tactic, in both presidential campaigns and lower down the ladder” (Jane, personal communication, May 2016). She was, however, sceptical that using bots to boost candidates was actually effective. In fact, Jane said that doing so was, in her opinion, a waste of money and more a distraction than a benefit. She said, “[L]ikes and retweets don’t equal votes.” That said, she claimed that in her experience digital teams treated online strategy in a fairly ad hoc way. “We will throw anything against the wall and see what sticks,” Jane said. “Bots are one tactic among many, and they aren’t illegal.”

There are two clear take-away points from the interview with Jane. The first is that, despite her own ambivalence about the efficacy of political bots, she openly admitted that bots were regularly used in Republican campaigns at all levels of governance. Second, she was emphatic that digital campaign teams, again at all levels, commonly made use of a variety of tactics and treated the online space as a frontier for testing new marketing methods. This picture, one of experimentation and spontaneity, stands in stark contrast to the one painted later in the campaign by groups like Cambridge Analytica. Jane was not alone in this assessment; several other informants who worked in digital campaign contracting echoed her scepticism. Some went further, saying that claims of psychographic or psychometric targeting were largely
exaggerated and that it was clear campaign messages and boots on the ground that led to votes, not fancy computational tactics.

However, it is a straw-man argument to denounce the political influence of digital tactics simply because a direct line cannot be drawn between social media activity and votes. First of all, some researchers have indeed made an effort to draw this line, and the results are increasingly exposing the influence of social media, and bots in particular (Bessi & Ferrara, 2016; Howard et al 2016). Social media and automated agents of propaganda are part of much broader socio-political systems. These systems contain a vast diversity of actors, interests, techniques, and mechanisms of power. A more suitable question regarding the importance of bots is do they have the capacity to influence the flow of political information over social media? The answer is important because this type of influence can make downstream contributions to a slew of political behaviours, including voting. Framed with this in mind, bots are a growing threat to American democracy, especially given that more than 60 percent of Americans now rely on social media for their political discussion (Mitchell et al. 2014; Gottfried & Shearer 2016). If it can be shown that bots influence political discussion online, it becomes tenuous to view social media websites as neutral public spheres for the democratic marketplace of ideas.

Modelling the influence of bots on real political processes has been a challenge. There have been efforts to use experimental methods to show how bots can influence Twitter discourse. For example, Messias et al. (2013) show that designing Twitterbots on the basis of simple feedback principles can enable them to reach positions of measurable influence. However, Messias et al. (2013) base their measures of influence on ready-made software packages such as Klout and Twitalyzer, which do not publicly reveal their methods for calculating influence. Mønsted et al. (2017) further demonstrate that networks of Twitterbots can be used to seed the spread of norms and misinformation, which spread in a complex, contagious fashion. Such methods establish the potential for bots to influence political discussion online. To understand how bots influenced specific political events of interest – in this case, the recent 2016 US election – it is important to focus analyses on data from this time period.

In order to study bots in actual Twitter networks, there have been efforts to automate bot detection. Some detection software can classify bots that deviate strongly from normal users in terms of click rate, message frequency, and time of operation (Ratkiewicz et al., 2011; Wang, Konolige, et al., 2013). Other software systems use network structure to detect bots (Alvisi, Clement, Epasto, Lattanzi, & Panconesi, 2013; Fire, Goldschmidt, & Elovici, 2014; Wald, Khoshgoftaar, Napolitano, & Sumner, 2013). The Truthy team combined these detection methods into a machine-learning ensemble they recently made accessible as a public API (Davis et al 2016). Using this classifier, Bessi and Ferrara (2016) found that almost one-fifth of Twitter discussion during the election was likely to come from bots. While these studies use network structures to distinguish human and bot accounts, they have yet to undertake detailed analysis of the network influence that bots achieve within specific political events of interest, such as the recent US election.

Using the public API designed by Truthy, the second part of this working paper provides a transparent network analysis of the role of Twitterbots during the 2016 US election. As such, the
goal of Part B is to provide a clear answer to the question of whether bots were capable of influencing the political discussion during the US election. The answer, as our results reveal, is yes.

A Network Analysis of Twitterbots during the 2016 Election

Sampling the Twittersphere
The data consists of approximately 17 million unique tweets and 1,798,127 unique users, collected from 1 November to 11 November 2016. The election was on 8 November 2016. The data was collected using the Twitter streaming API which provides access to 1 percent of the Twittersphere, tailored to the hashtags used to collect the data. Figure 4 is a display of the hashtags used during data collection. Hashtags highlighted in blue represent those associated with Clinton; red hashtags are those associated with Trump; and black hashtags are neutral:

Figure 4: Political Valence of Hashtags

Bot or Not?
The analysis procedure deployed in this working paper relies on three steps. First, we collected data from the Twitter streaming API. Then, to classify bots, we ran this data through the BotOrNot API, which is a machine-learning ensemble for classifying bots that the Truthy team designed (Davis et al, 2016). Once our sample was classified, we constructed networks of retweeting among users to assess whether bots achieved influence over the flow of information during the 2016 US election. Each of these steps is discussed in detail below.
Classifying Users
To classify accounts as human or bot, we ran the profile data and 200 most recent tweets associated with each account through the BotOrNot API. Using the BotOrNot service begins with querying the BotOrNot system with a specific Twitter handle (a screen name). The BotOrNot website and API use Twitter’s REST API to obtain the account’s recent history, including recent tweets from that account as well as mentions of that screen name. Once the requested data is received from Twitter’s API, the BotOrNot website or API forwards it to the BotOrNot server. The server processes the bot-likelihood score using the classification algorithm described below. This description is based directly on the writing of Davis et al. (2016). We encourage readers to visit the original paper for more technical introductions.

BotOrNot’s classification system recruits more than 1,000 statistical features using available meta-data and information extracted from the social interactions and linguistic content generated by accounts. It groups its classification features into six main classes. Network features capture various dimensions of information diffusion patterns. It builds networks based on retweets, mentions, and hashtag co-occurrence, and it pulls out their statistical features, such as degree distribution, clustering coefficient, and centrality measures. User features are based on Twitter meta-data related to an account, including language, geographic locations, and account creation time.

Friend-based features include descriptive statistics relative to an account’s social contacts, including their number of followers, who they follow, and posts. Temporal features capture the average tweet rate and the burstiness of tweet activity. Content features are based on linguistic cues computed through natural language processing, especially part-of-speech tagging. Sentiment features are built using general-purpose and Twitter-specific sentiment analysis algorithms, including happiness, arousal-dominance-valence, and emoticon scores. To classify an account as either bot or human, the model is trained with instances of both classes. BotOrNot’s classifier uses Random Forest, an ensemble supervised learning method. The features described above are used to train seven different classifiers: one for each subclass of features and one for the overall score (Davis et al., 2016).

Using the BotOrNot classification system, we considered an account to be a bot if it was scored as more likely to be a bot than a human. Any account given a score of over 0.5 was labelled as a bot (or at the very least, bot-like). It should be noted that there are several limitations to this classification method. First, because it relies on the rest API, it can only classify users whose accounts still exist and are open to public data mining. Bots are most affected by these limitations, because bot accounts are more likely to be removed or deleted after the sampling period. A decently large number of participants also block their accounts from the rest API, further restricting analysis. The BotOrNot ensemble also often categorizes organizational accounts, like @BarackObama, as bot accounts. Lastly, the BotOrNot classifier was trained on mostly English-language tweets, so it is best suited to detecting bots that tweet in English. Since our data analysis was concerned with English tweets during the election, this bias was not an issue for this working paper.
A Brief Primer on Network Analysis

A network consists of a set of nodes (otherwise called vertices) and connections (otherwise called edges). The nodes and connections are defined with respect to the kind of network being built. In this working paper, we model the retweet network between users, where users represent the nodes and connections represent retweeting. Networks can be either directed or undirected. In the case of retweet networks, directed networks draw an edge between two users (nodes) – $A$ and $B$ – if $A$ retweets $B$. In this working paper, undirected networks draw a connection between users if they have both retweeted each other. For a visualization, see Figure 5.

*Figure 5: Building Blocks of Retweet Networks*

![Directed and Undirected Retweet Networks](image)

*Source: Authors’ construction.*

Network analysis consists of mathematical and statistical tools for examining the geometry and dynamics of connections within a network. One key measure concerns the degree of a node, which refers to the number of connections possessed by that node. For directed networks, it is possible to examine indegree (number of incoming connections) and outdegree (number of outgoing connections) separately. In the case of retweeting, indegree captures the number of people who retweeted a given user, and outdegree captures the number of people whom a given user retweeted. Network analysis also supplies methods for analysing network influence, where influential nodes are more important for connecting others and controlling the flow of information. We deploy two methods for characterizing bot influence: k-core decomposition and betweenness centrality. We also examine the largest botnets associated with Trump-related and Clinton-related hashtags, and we apply a range of measures to characterize the differences between these botnets. As is standard in network analysis, all retweet networks in this working paper are built by extracting the largest connected component, which refers to the largest continuous web of connections among users where every user has at least one connection in the network. Many of the measures we deploy require the object of analysis to be a single connected component.

**K-core Decomposition**

K-core decomposition breaks a network down into separate layers where each layer (also known as a shell) consists of nodes that have the same number of connections or higher (see Figure 6). The k-core decomposition is a recursive approach that trims the least-connected nodes in a network, that is, those with a lower degree, in order to identify its core. At the base of the decomposition procedure lie the most peripheral nodes. At the highest shells, we uncover nodes that are cohesively most central with respect to the number of connections they wield.
The output of k-core decomposition depends on the density and the degree distribution of networks. The relative size of the core and periphery, and the communication dynamics that are created between the two, are important for understanding political influence. Network cores represent segments of the network that integrate the most information and disseminate this information most widely. In this sense, the upper cores of the network represent structural positions that are most likely to set the agenda for the rest of the network, given their ability to reach many people and thereby achieve a megaphone effect. For example, it has been shown that the core of political networks online is capable of triggering cascades of recruitment during political protest, where a cascade in this case refers to a chain of users who not only cause their network neighbours to join a protest, but also to encourage their own peers to do so as well (González-Bailón et al., 2011). In this working paper, we aim to observe whether bots infiltrated the higher cores of the network and thus the upper echelons of influence. If bots are in the core of the network, this means that they dwell alongside the most influential humans in our sample, with the capacity to disseminate propaganda and potentially initiate global cascades of politically relevant behaviour, in terms of information exchange and action.

**Betweenness Centrality**

Betweenness centrality represents the extent to which nodes “stand between” each other in a network, as gatekeepers of information (Freeman, 1979; Newman, 2010). A node has high betweenness centrality if it is necessary for linking many other nodes. As such, betweenness centrality is a robust measure of influence in a network, because nodes with high betweenness centrality have more control over the flow of information between other nodes. In terms of graph theory, betweenness centrality is based on measures of shortest paths, where a path refers to the number of people a message must travel through to get from person A to person B. For every pair of nodes in a single connected component, there exists at least one shortest path...
between nodes. The betweenness centrality for each node is the number of these shortest paths that pass through the node. See Newman (2010) for mathematical descriptions of this measure.

Comparing the Complexity of Botnets with Global Transitivity
We were also concerned with comparing how bots influenced content associated with Trump and Clinton, as an indicator of differences in the sophistication of computational propaganda strategies associated with each candidate. We built separate retweet networks for the hashtags associated with Trump and Clinton. We found the largest botnet by extracting the portion of the undirected retweet network including only bots and then by identifying the largest connected component. To compare the sophistication of botnets, we calculated global network transitivity, (also termed clustering coefficient), which measures how densely interconnected the nodes are in a network. High transitivity scores can be used as a proxy for the complexity of community organization. In our specific case, it provides a measure of the complexity with which bots retweeted each other, thus indicating the possibility of coordinated propaganda strategies and megaphone effects. Again, see Newman (2010) for mathematical descriptions of this measure.

Evidence of Influence
Using BotOrNot, we were able to classify a sample of 157,504 unique users. The remaining users were not classified either because their profiles were not publicly accessible or their accounts had been deleted since the data was collected. Of this sample of classified users, 15,805 accounts were identified as bots, representing over 10 percent of users.

Figure 7: K-Core Distribution for Human and Bot Users

Source: Authors’ construction.

Note: This figure shows what percentage of the overall population for each type of user is located within a given k-shell. For example, this figure shows that, of the 34,922 humans, 50 percent (17,461) of these humans fell within the first k-shell. So this does not mean that the first k-shell included 50 percent humans. This approach allows us to compare how the populations of humans and bots were distributed across the shells.

To measure whether bots reached positions of structural influence, we undertook k-core decomposition analysis of the largest connected component of retweets within our network. We
built an undirected network, where a link was formed between user A and user B if they had reciprocally retweeted one other. The largest connected component contained 38,306 users and 102,623 connections (retweet relationships). Within this largest connected component, we identified 3,517 potential bots (roughly 10 percent of the sample). As Figure 7 displays, our k-core decomposition analysis reveals that bots are distributed throughout both the periphery and the core of the largest connected component. In fact, nearly a third of the bots were in k-cores with a degree of at least 10. These results indicate that bots infiltrated the core discussion network of our sample, suggesting that they had the capacity to influence political discourse over Twitter.

Figure 8: Bots with Top Twenty Betweenness Centrality Scores

Next, we examined which bots achieved positions of high centrality within the retweet network, as evidence of their capacity to control the flow of information during the election. We focus our analysis on a directed model of the largest connected component in the retweet network. The directed network allows us to measure whether bots played a role in mediating the flow of information between users, where bots with high betweenness centrality are those that were potentially necessary for exposing users to tweets within the retweet network. By transforming betweenness centrality measures into z-scores, which indicate the number of standard deviations a score is from the mean, we find that 204 bots have a betweenness centrality score that is above the average score of all users, including humans. Figure 8 displays the top 20 potential bots with the highest betweenness centrality scores, as revealed by the first column indicating z-scores for betweenness centrality. We also found that 487 bots were above average in terms of their indegree (the number of users retweeting them) and 800 bots were above average in terms of their outdegree (the number of users they were retweeting). Bots thus reached positions

<table>
<thead>
<tr>
<th>User</th>
<th>Betweenness Centrality</th>
<th>In-degree</th>
<th>Out-degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>098James</td>
<td>73.0</td>
<td>16.8</td>
<td>15.5</td>
</tr>
<tr>
<td>DeplorableBride</td>
<td>32.3</td>
<td>13.9</td>
<td>6.3</td>
</tr>
<tr>
<td>Miami4Trump</td>
<td>29.9</td>
<td>66.2</td>
<td>4.0</td>
</tr>
<tr>
<td>RedNationRising</td>
<td>23.1</td>
<td>28.8</td>
<td>0.3</td>
</tr>
<tr>
<td>AMITrump4PRES</td>
<td>22.0</td>
<td>18.6</td>
<td>1.5</td>
</tr>
<tr>
<td>FreedomChild3</td>
<td>20.0</td>
<td>7.2</td>
<td>5.8</td>
</tr>
<tr>
<td>UnPoliticalPrtty</td>
<td>19.5</td>
<td>8.1</td>
<td>4.4</td>
</tr>
<tr>
<td>GaetaSusan</td>
<td>15.7</td>
<td>4.4</td>
<td>4.2</td>
</tr>
<tr>
<td>winegirl73</td>
<td>12.6</td>
<td>6.9</td>
<td>4.9</td>
</tr>
<tr>
<td>MynerStuff</td>
<td>11.8</td>
<td>5.6</td>
<td>4.9</td>
</tr>
<tr>
<td>ResistTyranny</td>
<td>10.7</td>
<td>14.4</td>
<td>1.2</td>
</tr>
<tr>
<td>RNRFloida</td>
<td>10.3</td>
<td>1.8</td>
<td>1.5</td>
</tr>
<tr>
<td>NgullenR</td>
<td>9.8</td>
<td>0.3</td>
<td>0.3</td>
</tr>
<tr>
<td>THETXEMBASSY</td>
<td>9.5</td>
<td>4.0</td>
<td>0.5</td>
</tr>
<tr>
<td>EverySavage</td>
<td>8.9</td>
<td>0.6</td>
<td>0.1</td>
</tr>
<tr>
<td>FredZeppelin12</td>
<td>8.3</td>
<td>16.1</td>
<td>1.0</td>
</tr>
<tr>
<td>Indians4Trump</td>
<td>8.3</td>
<td>0.2</td>
<td>5.1</td>
</tr>
<tr>
<td>Dhargen</td>
<td>7.8</td>
<td>13.6</td>
<td>0.5</td>
</tr>
<tr>
<td>masg66</td>
<td>6.8</td>
<td>0.0</td>
<td>4.9</td>
</tr>
<tr>
<td>LEPTH00K</td>
<td>6.0</td>
<td>0.6</td>
<td>8.1</td>
</tr>
</tbody>
</table>

Source: Authors’ construction.

Note: This table represents the authors’ calculations of the z-scores for each measure, where z-scores refer to the number of standard deviations a given user is from the mean measure for a given distribution. Negative values are standard deviations below the average, and positive values are above the average.
of centrality because they were retweeting others and being retweeted. This raised the question of whether bots and humans were retweeting bots.

Figure 9: Directed Network of Humans Retweeting Bots with Threshold Removing All Users with Only One Connection

Source: Authors’ construction.

Note: In this figure, the bots are coloured green and the humans are coloured black. A connection is drawn between a human and a bot only if the human retweeted that bot. The boldness of an edge is weighted by the number of times that the human user retweeted the bot. The bots with the highest number of humans retweeting them are labelled, with the number of connections beside their name. We removed all bots that were retweeted by only one human, along with all their connections, for the purposes of visualization. This is why thousands of connections are not displayed for the bots with the highest indegree.

To model whether humans retweeted bots, we constructed a version of the retweeting network that only included connections where a human user retweeted a bot. The result was a directed retweet network, where a connection represented a human retweeting a bot. Overall, this network consisted of 15,904 humans and 695 bots. The average number of times that a given person retweeted a bot was 5 times. The average in-degree of bots in this network was 2, meaning that bots were retweeted by approximately 2 people on average. When examining only the bots who were retweeted by humans more than once, we discovered 122 bots (see figure 9). These bots were retweeted 63 times on average, with connections to 40 different humans on average. These results confirm that bots won a significant amount of attention and interaction from humans users. As figure 8 displays, 4 out of the 5 most retweeted bots had
explicitly pro-Trump in their twitter handle: @TeamTrump, @Miami4Trump, @Bikers4Trump, and @RedNationRising.

Figure 10: Comparing the Largest Botnet within the Retweet Networks for Trump vs Clinton Related Hashtags.

We were also interested in comparing the largest botnets associated with Trump-related hashtag networks and Clinton-related hashtag networks. We constructed botnets by extracting the largest undirected, connected component of retweets among bot users within the set of either Trump-related or Clinton-related hashtags. As Figure 10 displays, we found that the largest botnet in the Trump network was almost 4 times larger than the largest botnet associated with the Clinton network. The Trump botnet consisted of 944 bots in total, whereas the Clinton botnet consisted of only 264 bots. To compare the sophistication of botnets, we computed the global transitivity for each botnet, where transitivity captures the number of shared neighbours among bots (in some sense, the number of potential mutual conspirators). The global transitivity of the Trump botnet was 0.01, which had a substantially higher transitivity score than randomly generated networks with the same number of nodes and edges, in each of 1000 simulations (the average transitivity of these random networks was 0.004). By contrast, the global transitivity of the Clinton botnet was 0.009, which was less than the transitivity found in random benchmark networks in over half of 1000 simulations. What this means is that while the organization among bots in the Clinton network may be an accident, this is far less likely to be the case within the Trump retweet network. The results show how bots obtained a much greater presence when retweeting with Trump-focused hashtags. The results also reveal more sophistication in the mutual retweeting connections among bots retweeting with Trump-focused hashtags. Altogether, these results suggest that bots played a much more prominent role in boosting the salience of Trump
related content over Twitter, with signs of more coordination and strategic organization among Trump-related bot activity.

The Rise of Bots: Implications for Politics, Policy, and Method
The results of our quantitative analysis confirm that bots reached positions of measurable influence during the 2016 US election. Our k-core decomposition reveals that bots occupied both the periphery and the core of political discussion over Twitter. As members of the core, bots are in a position where they are capable of diffusing information that sets the agenda over Twitter (González-Bailón et al., 2011). Betweenness centrality measures indicate that bots also reached positions where they were able to control the flow of information between users. We then showed how bots were, in fact, retweeted by humans, adding further evidence to the finding that bots influenced meaningful political discussion over Twitter, where pro-Trump bots garnered the most attention and influence among human users. Lastly, we provide preliminary evidence that bots were more actively involved in influencing the uptake of Trump-related hashtags than Clinton-related hashtags, with the potential to augment the megaphone effect, previously defined. Altogether, these results deepen our qualitative perspective on the political power bots can enact during major political processes of global significance. It is the task of future studies to explore in greater depth the downstream consequences of bot influence over social media on actual on-the-ground political behaviour.

Most concerning is the fact that companies and campaigners continue to conveniently undersell the effects of bots. The quantitative analysis of this working paper aims to partially settle the question of bot influence so that we can begin to address the realities of bot manipulation more directly. Bots infiltrated the core of the political discussion over Twitter, where they were capable of disseminating propaganda at mass-scale. Bots also reached positions of high betweenness centrality, where they played a powerful role in determining the flow of information among users. Several independent analyses show that bots supported Trump much more than Clinton, enabling him to more effectively set the agenda. Our qualitative report provides strong reasons to believe that Twitter was critical for Trump’s success. Taken altogether, our mixed methods approach points to the possibility that bots were a key player in allowing social media activity to influence the election in Trump’s favour. Our qualitative analysis situates these results in their broader political context, where it is unknown exactly who is responsible for bot manipulation – Russian hackers, rogue campaigners, everyday citizens, or some complex conspiracy among these potential actors.

Despite growing evidence concerning bot manipulation, the Federal Election Commission in the US showed no signs of recognizing that bots existed during the election. There needs to be, as a minimum, a conversation about developing policy regulations for bots, especially since a major reason why bots are able to thrive is because of laissez-faire API access to websites like Twitter. The only gesture towards bot policy in the US to date is the US Anti-Bot Code of Conduct (ABCC), in relation to which a large number of representatives from major ISPs, and a noticeably smaller number of representatives from the US government, gathered to discuss concerns regarding bots of all kinds (Bot Remediation Working Group, 2013).

The report exposes one of the possible reasons why we have not seen greater action taken towards bots on behalf of companies: it puts their bottom line at risk. Several company
representatives fear that notifying users of bot threats will deter people from using their services, given the growing ubiquity of bot threats and the nuisance such alerts would cause. The conclusion of the report is that, for the time being, bot attacks should be viewed as the responsibility of the individual user. The problem is, research abounds showing that people are inherently and incurably poor at detecting bots online (Edwards et al., 2014; Guilbeault, 2016). Most curious of all is the ABCC’s claim that one of the leading obstacles to bot policy is the fact that, in their words, “[Y]ou can’t manage what you can’t measure.” We hope that the empirical evidence in this working paper – provided through both qualitative and quantitative investigation – can help to raise awareness and support the expanding body of evidence needed to begin managing political bots and the rising culture of computational propaganda.
References


About the Authors

Samuel C. Woolley is the Director of Research of the Computational Propaganda Project at the Oxford Internet Institute, University of Oxford and a doctoral candidate (ABD) at the University of Washington. He is a research fellow at Google Jigsaw, the Institute for the Future, the TechPolicy Lab at the University of Washington and a former fellow at the Center for Media, Data and Society at Central European University. He researches automation and propaganda.

Douglas R. Guilbeault is an Affiliate Researcher on the Computational Propaganda Project at the University of Oxford. He is a Research Assistant in the Network Dynamics Group and PhD Student at the Annenberg School for Communication at the University of Pennsylvania. Doug is a computational social scientist who studies social bots and conducts online experiments; his writing on bots has appeared in IJOC, the Atlantic, and Quartz.
Citation

Series Acknowledgements
The authors gratefully acknowledge the support of the European Research Council, Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe,” Proposal 648311, 2015-2020, Philip N. Howard, Principal Investigator. Additional support has been provided by the Ford Foundation and Google-Jigsaw. Project activities were approved by the University of Oxford’s Research Ethics Committee. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funders or the University.