Bots and Computational Propaganda: Automation for Communication and Control

Samuel C. Woolley

INTRODUCTION

Public awareness surrounding the threat of political bots, of international fears about armies of automated accounts taking over civic conversations on social media, reached a peak in the spring of 2017. On May 8 of that year, former Acting US Attorney General Sally Yates and former US Director of National Intelligence James R. Clapper Jr. sat before Congress to testify on what they called “the Russian toolbox” used in online efforts to manipulate the 2016 US election (Washington Post Staff 2017). In response to their testimony and a larger US intelligence community (IC) report on the subject Senator Sheldon Whitehouse said, “I went through the list [of tools used by the Russians] … it looked like propaganda, fake news, trolls, and bots. We can all agree from the IC report that those were in fact used in the 2016 election” (Washington Post Staff 2017).

Yates and Clapper argued that the Russian government and its commercial proxy – the Internet Research Agency (IRA) – made substantive use of bots to spread disinformation and inflame polarization during the 2016 US presidential election. These comments mirrored concurrent allegations made by other public officials, but also by academic researchers and investigative journalists, around the globe. Eight months earlier, during a speech before her country’s parliament German Chancellor Angela Merkel raised concerns that bots would affect the outcome of their upcoming election (Copley 2016). Shortly thereafter, the New York Times described the rise of “a battle among political bots” on Twitter.

Around the same time, research from the University of Southern California’s Information Sciences Institute concretized the ways that social media bots were being used to manipulate public opinion:

The presence [of] social bots in online political discussion can create three tangible issues: first, influence can be redistributed across suspicious accounts that may be operated with malicious purposes; second, the political conversation can become further polarized; third, the spreading of misinformation and unverified information can be enhanced. (Bessi and Ferrara 2016)
These findings were backed up by several other prominent studies that both preceded this work and have vindicated it since. Metaxas and Mustafaraj (2012) discussed findings in Science illuminating a similar distribution of influence across suspicious Twitter bot accounts used to defame a Massachusetts Senate candidate in 2010. Kramer, Guillory, and Hancock (2015), in the Proceedings of the National Academy of Sciences of the United States of America (PNAS), found that exposure to Twitter bots with oppositional views increased political polarization among participants in an experimental study. Woolley and Howard (2018), in a book of country-specific case studies entitled Computational Propaganda, argued that bots are often used during events around the world to spread and bolster misinformative and disinformative stories online.

This chapter explores these, and other, core arguments surrounding the political use of bots. It details the brief history of their use online. It accesses the academic literature to highlight key themes on the subject of what some researchers call computational propaganda and others simultaneously call “information operations,” “information warfare,” “influence operations,” “online astroturfing,” “cybertufing,” and many other terms. Computational propaganda, and each of these other concepts to one degree or another, focuses on the ways in which the use of algorithms, automation (most often in the form of political bots), and human curation are used over social media to purposefully distribute misleading information over social media networks (Woolley and Howard 2016a).

This literature review details empirical work on how the bot as an internet-based tool, and computational propaganda as a political communication strategy, function in relationship to social media and democracy. As Luceri et al. (2019) argue, “the presence of social bots does not show any sign of decline despite the attempts from social network providers to suspend suspected, malicious accounts.” With this argument in mind, this chapter discusses the implications of the continued use of political bots and computational propaganda for social media and democracy.

The following discussion is broken into five parts: The first section explores bots in the context of their general use online and then unpacks research that examines their social use. The second looks into their political use and discusses research on how to detect such use. The third details arguments on how bots can and have been deployed over social media as tools used in the interest of democracy. The fourth outlines key arguments and research more broadly focused on computational propaganda, information operations, and the like. The fifth, and final, section illuminates gaps in the literature. It outlines ongoing and new research into how bots and computational propaganda are used over social media to effect democracy and summarizes the core ideas of this piece.

To begin, it is important to examine perspectives on exactly why bots have become a particular topic of concern for scholars who study the online world. How are they used technically? What are their social uses?
In part due to the political concerns detailed in the Introduction to this chapter, but also because of broader interest in artificial intelligence (AI) and automation, scholars and publics have begun to shine a light on the automated internet software technology known as the bot. Socially oriented versions of bots, which can be programmed to look and act like real people on sites like Facebook or Twitter, are often key tools for spreading computational propaganda. When this is the case, these programs have been referred to as digital “astro turf content” or as “political bots” (Ratkiewicz et al. 2011; Woolley 2016).

The word “bot” is an umbrella term that encapsulates many different kinds of automated online software programs or scripts. In fact, what counts as a bot is the topic of conjecture and debate within the technology community (Martineau 2018). Leonard (1998) called bots “the web’s first indigenous species” and set out to discuss and historicize the wide array of automated online actors that could be considered to exist in the category of “bot.” Both bots and social bots (sometimes called chat bots), as the narrower category of front-facing, communication-enabled, online bots are often known, do have a broad array of uses online outside of the political sphere, however (Wagner et al. 2012). They were, and are, crucial applications for automating spam messaging over email (Zhuang et al. 2008). The earliest bots were designed for network maintenance by the computer engineers who faced infrastructural challenges and a need for human coders to take on tasks requiring more critical oversight (Leonard 1998). Researchers, however, were quick to see their potential as “intelligent software” that could help people better navigate, and even communicate, via the Internet (Weld and Etzioni 1995).

In their most simple iteration as online programs that run automated tasks (while not directly interacting with other web users) bots have long been infrastructural tools used for activities relating to early iterations of online indexing and internet search (Middlebrook and Muller 2000; Seymour, Frantsvog, and Kumar 2011). Both simple strings of code intended to back up or update personal computers and socially oriented, automated, imposter accounts on Twitter can be referred to as bots. These automated programs have a seriously large presence online. In fact, in 2015 the cybersecurity firm Incapsula (now known as Imperva Incapsula) found that bot usage made up around 50 percent of all online traffic (Incapsula 2015). In 2014, as many as 20 million accounts on Twitter were identified as bots (Motti 2014). The number of bots functioning on Facebook and other prominent platforms is less clear, in part due to firms’ close hold on user data and metrics. In 2018, however, Facebook self-reported to the US Securities and Exchange Commission (SEC) that an estimated 3–4 percent of, or around 50 million, accounts on the site were “fake” (Facebook 2017). It is clear that a significant
amount of bots function online today, but it is also true that social bots have existed on the Internet for several decades.

The use of bots in online social settings dates back to before their integral use over Internet Relay Chat (IRC) – a precursor to contemporary social media (Mutton 2004). Social bots also appeared even earlier, in experiments with what programmers then called “chat bots” on the public web’s precursor, the Advanced Research Projects Agency Network (ARPANET) (Garber 2014). The automated, perpetual nature of bots, combined with modern computational power, means that bots, whether social or not, are hugely important in scaling work online (Leonard 1998). Bots can achieve discrete, repetitive tasks in a fraction of the time it would take a human counterpart. Because of this, they have been integral to the endless organizational work central to maintaining sites such as Wikipedia and Reddit (Geiger 2014; Long et al. 2017). As bot technology progresses and social media becomes more ubiquitous worldwide, these automatons continue to become more and more useful as political amplification and suppression tools online (Shao et al. 2018).

Advances in machine learning allow social bots to more readily learn from their environment and to use what they find in their interactions on gaming platforms or in their conversations on social media platforms (Baumgarten, Colton, and Morris 2009; Ferrara et al. 2016). For instance, Tay – now known mostly as Microsoft’s failed Twitter chat bot experiment – was first seen as unique because it was built to learn from other users on the platform (Vincent 2016). As Suárez-Gonzalo, Mas-Manchón, and Guerrero-Solé (2019) point out, however, Tay was still a product of its human designers. This is an important distinction because, as they argue, people often see bots as independent actors due to the fact bots work autonomously. Yet, ultimately, the identity and agency of bots are complicated by way of their symbiotic relationship with the people who build and use them (Neff and Nagy 2016).

Because this usage extends to the social – where bots have real-time conversations with humans on sites like Facebook and Twitter – the engineers who build them often view them as more than a tool but less than human, a proxy for the creator (Woolley, Shorey, and Howard 2018). Social bots play a key role in generating content and are often used to mimic real users on Twitter and many other social media sites and online discussion communities (Kumar et al. 2017). Researchers have developed ways, but still face challenges, in detecting whether a given online account is a human, bot, or cyborg (Chu et al. 2010; Gorwa and Guilbeault 2018). Though machine learning capabilities used for social bot development are progressing, it is still true that sophisticated propagandists make use of both human and bot communication and work in order to most effectively manipulate public opinion (Paavola et al. 2016). Even the most sophisticated machine learning or deep learning–enabled social bots have trouble parsing human emotion, humor, and sarcasm and as such can be identified more readily than bot-human hybrids that harness human intelligence (Davis et al. 2016; Chatterjee et al. 2019).

Samuel C. Woolley
Because bots are useful in scaling communication online – and because they provide an additional layer of anonymity over social media – they have become popular tools for spreading political propaganda over social media (Woolley 2016). The next section details research on the various uses – and ramifications – of political bots. It situates the political bot as a global phenomenon, as tools now used in efforts to manipulate public opinion on numerous websites and social media platforms in a variety of languages and countries.

**Political Bots**

Political bots – sometimes known as fake followers, astroturf accounts or sock puppets – are automated social media accounts, often built to look and act like real people, in order to manipulate public opinion (Ratkiewicz et al. 2011; Woolley and Howard 2016b). Political bots can be used to amplify the spread of particularly partisan, or completely false, information. They have, for instance, been used by far-right groups on Twitter to spread content and by anti-vaccine activists to boost false messaging on health communication (Marwick and Lewis 2017; Broniatowski et al. 2018). They can drive up the number of likes, re-messages, or comments associated with a person or idea. Researchers have catalogued political bot use in massively bolstering the social media metrics of politicians and political candidates from Donald Trump to Rodrigo Duterte (Zhang et al. 2018; Uyheng and Carley 2019). They can be used to harass journalists, activists, and political opposition in state-sponsored trolling campaigns (Monaco and Nyss 2018). They are even used in attempts to prioritize, and subsequently harness, online views for particular traditional news sources over others (Sanovich, Stukal, and Tucker 2018).

While events including the 2016 US election and the UK Brexit referendum may have catapulted these ideas to the forefront of the Western zeitgeist, political bots and computational propaganda are global in use and continue to play a role in international political communication at present. Bots have been used over Twitter and other applications to harass journalists and attack dissidents in Mexico, for instance, since at least 2012 (Orcutt 2012; Treré 2016). Automated accounts have been estimated to account for up to 50 percent of traffic among accounts tweeting about Russian politics (Stukal et al. 2017). In Syria, bots have been used to spread messages in favor of Bashir al-Assad and to confuse and attack opposition (Abokhodair, Yoo, and McDonald 2015). So-called spambots have been used in conversations about Italian politics online to generate civic noise (Cresci et al. 2017). Canadian researchers found that “identification, evidence, attribution, and enforcement” were among the chief problems associated with bots “disrupting” that country’s democratic process (Dubois and McKelvey 2019). During Chile’s 2017 presidential race, bots were deployed to spread Twitter messages related to numerous candidates, including a suspiciously large amount
of automated traffic for the eventual third-place progressive candidate Marco Enríquez-Ominami (Castillo et al. 2019).

Though country-specific cases of political bot usage are useful in studying particular ways these tools are used in particular places, the same groups of bots are often used in efforts to manipulate public opinion across borders, during different types of situations and in different languages. Studies have revealed that bot accounts used to spread political communication during one country’s election have then been used in another separate country and contest (Ferrara 2017). Similarly, researchers have found that the same bot accounts used in one event or crisis in the same country have then been reused in another (Starbird et al. 2014). Still others have found bot networks that switch between multiple languages or written versions of the same language (i.e., simplified versus traditional Mandarin) and argued that this can be both a useful feature in bot detection and indicative of outside efforts to influence digital political conversation in other countries (Monaco 2017; Varol et al. 2017). Owing to the complexity of how networks of political bots operate – with the same collections of accounts switching focus between state borders and across multiple tongues – they are often difficult to detect and manage (Morstatter et al. 2016). This has not, however, stopped governments and technology firms from attempting to curb their use.

There has recently been a spate of policies, both in the United States and elsewhere, attempting to deal with the malicious use of political bots on social media. Many of these policies fall short due to a lack of institutional clarity – in both technology and political circles – about what actually constitutes bot traffic and, indeed, whether all automated traffic is problematic. Researchers have argued “that multiple forms of ambiguity are responsible for much of the complexity underlying contemporary bot-related policy” (Gorwa and Guilbeault 2018). Moreover, Gorwa and Guilbeault suggest that “before successful policy interventions can be formulated, a more comprehensive understanding of bots – especially how they are defined and measured – will be needed.” Indeed, recent US policy has been criticized for taking an overly censorial, broad, and technologically unsophisticated approach to combating and regulating the political use of bots during elections and other events (West 2017; Bromwich 2018). Maréchal (2016) has argued for a normative framework for bots across social media sites in response to such ambiguity about how online platforms define automated accounts and how the public understands them. Yet the quest for a normative framework for understanding bots is challenged not least by the sheer difference in the ways that different categories of political bots are used, despite recent authorship of several articles that attempt to define and categorize social bots (Grimme et al. 2017; Stieglitz et al. 2017; Gorwa and Guilbeault 2018).

In an early discussion of malicious bot software, Holz (2005) discussed “the zoo” of bot types: from those harnessed in distributed denial-of-service
DDoS) attacks to those deployed for mass identity theft. There are a similar range of varieties of political bots. Listener bots can monitor social media sites and databases for key information but also track and communicate what they find (Woolley 2016). Spambots, conversely, are built to generate noise (Cresci et al. 2017). Wikiedits bots can be created to monitor politicians’ edits to Wikipedia pages, but they are also often programmed to tweet about alleged changes to Twitter in efforts to name and shame — potentially stymying governmental use of Wikipedia (Ford, Dubois, and Puschmann 2016). Sleeper bots are social media accounts that sit on a site like Twitter all but unused for years, in order to generate a more realistic online presence, and are then activated during key political events (Howard, Kollanyi, and Woolley 2016). Troll bots, built to harass, have been used to demobilize activists trying to organize and communicate on Twitter but can also be used to drive traffic from one cause, product, or idea to another (Llewellyn et al. 2019). Finally, honeypot bots are built to attract particular users or even other bots (Lee, Caverlee, and Webb 2010).

It is clear that the collection of academic research into the rise in usage of political bots — and of broader online tactics relating to the promotion of disinformation and polarizing content — has grown since Metaxas, Mustafaraj, and Gayo-Avello’s (2011) early work on suspicious political campaigns on Twitter. Despite this, social scientific research demonstrating large-scale offline sociopolitical effects related to online bot usage remains slim (Tucker et al. 2018). Though many of the aforementioned researchers have demonstrated that social media bots have an active role in political communication around the world, fewer have had success in relating this automated communication directly to electoral outcomes. There has been more success, however, in drawing connections between the types of human users who spread bot content — or disinformative or polarizing content — and why.

Badawy, Lerman, and Ferrara (2018) examine users who spread Russian content during the 2016 US election and determine “that political ideology, bot likelihood scores, and some activity-related account meta data are the most predictive features of whether a user spreads trolls’ content or not.” Woolley and Guilbeault (2017) find that those in positions of power — including politicians, pundits, and journalists — often share Twitter bot-related content when it reflects their own views. The work of Stella, Ferrara, and De Domenico (2018), using data from the 2017 Catalan referendum, builds on this idea. They argue that, in this case, bots — despite often existing on the peripheries of social systems — were successful in exposing influential people to inflammatory and extreme views. Still other studies, however, suggest that digital disinformation, automated or otherwise, has little effect on people’s understanding of politics or that social media use has an insignificant correlation to polarization (Allcott and Gentzkow 2017; Castillo et al. 2019).
The debate about the influence of political bots, and surrounding the larger effects of computational propaganda, continues. The literature makes it clear, though, that political bots have become an important new tool for political communication online. Importantly, not all political uses of social bots are malicious or focused on control. There are a variety of examples, and a growing body of research, on the democratically positive uses of bots.

**BOTS FOR DEMOCRATIC GOOD**

Journalists, activists, commentators, and civic society groups have built chatbots aimed at openly engendering general political conversation over sites like Wikipedia and over modern social media precursors since the Net went public (Mutton 2004; Tsvetkova et al. 2017). Recently, there has been a rise in those producing public-facing social bots aimed at engendering conversation on pressing social issues, revealing political malfeasance and calling attention to protests (Sample 2015; Følstad et al. 2018). Bots have even been used to generate stories and to report on pending and real-time natural disasters or public health concerns (Lokot and Diakopoulos 2016; Lemelshtrich 2018). Because bots are able to automatically function at a computationally enhanced rate, they are particularly useful for journalists facing the very real demands of traditional story generation in that they can facilitate connections with readers to both spread and retrieve news (Gonzales and González 2017). Gonzalez and Gonzalez, exploring the case of a service known PolitiBot, which operated during the 2016 Spanish election over Telegram, write that the true journalistic potential of the program was to share relevant news (with more than 70 percent user satisfaction) with readers through that platform.

Hwang, Pearce, and Nanis (2012) explore the ways that bots can be used as a social prosthesis or scaffolding for connecting networks of people that might not otherwise communicate. They argue, citing natural bot-driven experiments on social media, that bots can be effectively used to parse information on a social network, pay particular attention to what people have in common, and connect users based on these interests. They make the point that bots can be used to mitigate the burden of troublesome conversations online. It is important to note that, while the connective use of bots has certain benefits for democracy, it can also be being harnessed for control (Woolley and Guilbeault 2017).

While some researchers have examined journalism bots’ capacities to search for information and communicate with readers, others have used these automated digital tools to problematize the idea that communication necessarily exists between two or more people, arguing instead that tools like bots play a key nonhuman role in news sharing online (Larsson and Hallvard 2015). Lokot and Diakopoulos (2016) propose a typology of “news bots” in order to guide intent, utility, and functionality of bots constructed by future
designers and reporting teams. They note the limits of robot journalists – especially in the areas of automated commentary, opinion writing, algorithmic transparency, and general accountability.

The analysis of Lokot and Diakopoulos (2016) primarily focuses on design elements of a sample of extant news bots on Twitter. They examine the various journalistic functions of these accounts and make it clear that news bots could change the modern media environment. In particular, their exploration of journalism bot accounts is concerned with their function in generating articles and reporting. They discuss problems associated with the opacity of algorithms that drive news bots but leave room for a larger discussion about the people who construct those algorithms, what cultural values they encode into that software, and the function and of the resultant bots during political crises and elections.

Lokot and Diakopoulous (2016), as well as other researchers, have explored the idea that bots could feasibly replace human journalists in some instances. Indeed, tools like the LA Times’s Quake Bot can automatically generate and post stories (Walker 2014). Harvard University’s Nieman Journalism Lab has argued that there will be a large-scale shift toward the “botification” of the news in coming years (Barot 2016). Others, with more unease about automated reporting, have suggested that journalism may be the latest industry to be under threat by automation – because of article writing bots – or that algorithms may “kill” journalism (Goichman 2017; Keohane 2017). In a case study of three newsrooms, however, Linden (2017) finds that the use of automated software has actually benefited reporters in that bots do the repetitive tasks journalists would otherwise have to do – thus freeing people up for other work. Latar (2018) provides a balanced view of both perspectives, what he terms the pessimistic and optimistic stances on robot journalists. He explores several case studies, including the LA Times, that exemplify both stances.

Democratically beneficial bots provide hopeful foils to their political bot counterparts. In his 2018 hearings before the US Congress (Harwell 2018), which took place because of political misuse of Facebook in 2016, Facebook CEO Mark Zuckerberg spoke of automation and AI as necessary tools to combat the rise of disinformation and misinformation. He pointed out that the sheer informational scale of social media makes it so that human labor alone cannot address the problems at hand. Some researchers have taken up this logic, suggesting that automation may have a role to play in preventing misuse of bots (Wang 2010). Indeed, many bot-detection systems rely on sophisticated algorithms and machine learning (Ratkiewicz et al. 2011; McKelvey and Menczer 2013; Klyueva 2019).

In order to prevent the political misuse of bots over social media, it is crucial to understand the complex ways in which bots facilitate and amplify the flow of misinformation, disinformation, trolling, and propaganda. The next section provides an overview of literature on computational propaganda – one of the umbrella terms and strains of research from the social sciences that attempts to grapple with the problem of political bots.
Understanding Computational Propaganda

Computational propaganda is specifically defined as “the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion” (Woolley and Howard 2016a). Research on computational propaganda spans the social sciences and computer sciences. Although the Computational Propaganda Project at the University of Oxford’s Oxford Internet Institute defined the term and carried out early social scientific work on the topic, the research from Ferrara et al. (2016), Metaxas and Mustafaraj (2012), Ratkiewicz et al. (2011), and others was foundational in building the preliminary understandings of how social bots effected the informational and computational systems that make social media possible.

Early research on computational propaganda was focused primarily on how powerful political actors leveraged social media bots for control. A great deal of this work looked at how governments, militaries, political campaigns, corporations, and other well-resourced entities launched such offensives online (Murthy et al. 2016). Now, however, it is clear that many types of groups – including regular citizens and activists – use the tools and tactics of computational propaganda to spread their own perspectives and communicate politically (Woolley 2018).

Indeed, computational propaganda has been propelled by a broader scale normalization of social media as a means for control by those focused on digital political communication (Karpf 2012). As Chadwick (2013) points out, “even the most radical changes to communications systems must be channeled through structural constraints in order to impact traditional political outcomes” (p. 10). Many old guard members of the political elite remain the same worldwide, and newly powerful individuals and groups have ascended and now make use of digital tools in efforts to gain and retain power (Howard 2015). As Karpf (2012) points out, these actors have adjusted to, and made use of, the altered state of political communication tools as they exist online. In some ways, digital democracy has not played out as cyber-optimists had hoped. The elite on the Internet are still elite and thus “online speech follows winner-take-all patterns” (Hindman 2008).

Sociotechnical innovation has led to ever-changing organizational affordances of the multimedia landscape encompassed by social media, both for the elite and for regular people (Treem and Leonardi 2013). The rise of hybridized technology and “networked society” has not only affected the way political conversations occur; it has also altered the ways campaigns are organized, elections function, and power is exerted (Benkler 2006). New political organizations have been birthed, political systems have changed, and politicians have risen and fallen. Some aspects of political communication, however, remain constant. Computational propaganda is a novel mechanism and strategy for enabling control among well-resourced and powerful groups,
though the means to build and launch bots over social media is becoming more widespread – and available to regular citizens – everyday (Woolley 2018).

Nimmo and the Digital Forensic Research (DFR) team at the Atlantic Council point out three core features of political bots and computational propaganda, which he claims separate it from traditional propaganda: activity, amplification, and anonymity (Nimmo and DFR Lab 2016). He writes that:

Many of these bot and cyborg accounts do conform to a recognizable pattern: activity, amplification, anonymity. An anonymous account which is inhumanly active and which obsessively amplifies one point of view is likely to be a political bot, rather than a human. Identifying such bots is the first step towards defeating them. (n.p.)

In order to “defeat” political bots, or broader manipulations that occur by way of algorithms and automation online, researchers have argued that social media firms must accept greater responsibility for the social and political outcomes of the tools they build and design – the algorithms, but also the very concept of platforms, have politics (Gillespie 2010; Gillespie 2014).

Indeed, prominent scholars of political communication argue that social media platforms such as Twitter and Facebook are now crucial transnational communication mechanisms for political communication (Segerberg and Bennett 2011; Tufekci and Wilson 2012). That is, their use in this regard – at least in most country cases worldwide – is not necessarily restricted by state borders. As such, people from around the globe use them to communicate about political issues with one another. As the research detailed in this chapter reveals, computational propaganda itself is also transnational. It is not confined to only one social media site but stretches across them in a tangled web (Council on Foreign Relations 2018). Revelations from Facebook, Twitter, and Google reveal, for instance, that government-sponsored Russian citizens used multiple social media sites to spread propagandistic content during the US presidential election (Allcott and Gentzkow 2017).

Research from several sources suggests that computational propaganda and political bot usage was at an all-time high during key moments of this particular election (Bessi and Ferrara 2016; Ferrara et al. 2016; Howard et al. 2016). Bessi and Ferrara (2016) found that “about 400,000 bots [were] engaged in the political discussion about the [US] Presidential election, responsible for roughly 3.8 million tweets, about one-fifth of the entire conversation.” Kollanyi et al. (2016) found that the thousands of Twitter bots supporting Trump outnumbered those supporting Clinton in the days preceding the election at a rate of five to one. Supporters of both candidates used these social automatons to give voters the impression that the campaigns had large-scale online grassroots support, to plant ideas in the news cycle, and to effect trends on digital platforms. At times during the 2016 US contest, regular people were convinced and even tricked by fringe partisans into using bots,
coordinated hashtag bombing and other tools to bolster trending topics that benefited candidates and campaigns (Schreckinger 2016).

The concept of “manufacturing consensus” is a central tactic of those who use computational propaganda (Woolley 2018). It occurs not only when bots boost social media metrics but also when the media reinforces illusory notions of candidate popularity because of this same automated inflation of the numbers. The concept of manufacturing consensus is drawn not just from the ways bots and computational propaganda were used during the 2016 US election but also from a range of parallel uses in multiple countries dating back as early as 2007 (Robb 2007; Gorwa 2017, p. 38). In the Americas, political actors in Mexico (Verkamp and Gupta 2013), Ecuador (Woolley 2015), Venezuela (Forelle et al. 2015), and Brazil (Arnaudo 2017) have pioneered the deployment of related techniques in attempts to boost the credibility of candidates and campaigns through increased metrics: follows, likes, retweets, shares, comments, and so on.

State-sponsored trolling, another novel online political manipulation strategy, is specifically concerned with governmentally driven computational propaganda campaigns aimed at attacking political opposition over social media (Monaco and Nyss 2018; Zannettou et al. 2019). Analysis from Monaco and Nyss on this phenomenon notes that the now global trend of “disinformation is often only one element of a broader politically motivated attack on the credibility and courage of dissenting voices: journalists, opposition politicians and activists” (Monaco and Nyss 2018, p. 4). According to their study, informed by more than two years of research and interviews and fieldwork spanning more than eight countries, the use of computational propaganda and astroturf political communication is not only propagated by organizations tangentially associated with governments, such as the IRA in Russia. Politically motivated trolling teams, in some cases outfitted with armies of political bots, are housed within the official governmental infrastructure of some countries. A recent report on cyber-troops by Bradshaw and Howard (2017) corroborates these findings and details the ways in which multiple governments now use the tools of computational propaganda.

Increasingly, computational propaganda and the tactic of using political bots to influence online conversation are moving from the political sphere to other topical areas. In healthcare, Twitter bots have been used to amplify anti-vaccine content (Shao et al. 2017; Allem and Ferrara 2018). In fact, coordinated Russian bots and human trolls have been used to manipulate the vaccine debate online (Broniatowski et al. 2018). Social media bots, alongside groups of people, have also played a role in distributing information and, worryingly, misinformation and rumors during natural disasters and terrorist attacks (Gupta et al. 2013; Starbird et al. 2014; Khaund et al. 2018; Vosoughi et al. 2018). Twitter bots are also used to create a significant amount of tweets linking to scientific articles, creating serious implications for using raw counts of such
messages for the evaluation or assessment of the reach or successful uptake of research over that platform (Haustein et al. 2016).

Computational propaganda shows no signs of abating, and there is a great deal of research to be done in order to build thorough understandings of the topic. The next section identifies gaps in the current research and suggestions for future work.

CONCLUSION AND GAPS

Computational propaganda is still propaganda. What has changed about this new form of an old strategy of control and coercion is that it now happens at scale. This new political communication strategy is scaled not just in terms of the number of people in places around the world that can and do access computational propaganda but also by the computational power and constantly advancing software – including political bots but also data analytics technology including machine learning and sentiment analysis – that facilitate it.

Several areas are at the forefront of innovation, and future problems, associated with political bot and computational propaganda usage. The first, both in the United States and globally, is policy and the law. How will these political domains be affected by the rise in political manipulation over social media? What laws are needed to regulate firms where disinformation is spread? The academy must aid policymakers by undertaking more empirical research to inform policy recommendations to be delivered to key US politicians, policy experts, civil society groups, and journalists. Campaign finance, election law, voting rights, privacy, and several other areas of the law are currently being affected in both unforeseen and complex ways by the spread of political disinformation over social media. Solid research into the ways computational propaganda contravenes the law is a crucial step in addressing the policy gap at the intersection of information dissemination, automation, social media, and politics.

We need better software, informed by both social and computer science research, to help researchers, journalists, and activists keep up with the challenges posed by the modern disinformation threat. Tools could include high-powered data intelligence platforms, that make use of bots in parsing large sets of relevant data, usable by these groups worldwide. They ought to exploit recent advances in graph databases and machine learning and cheap, massive computation to dramatically accelerate investigations. The target should be to accelerate civil society in identifying patterns of activity that would help to root out entities backing disinformation campaigns, in addition to uncovering a great deal about when and where these campaigns are occurring.

Longitudinal work can help establish more solid metrics for tracking information flows – but also effects – related to the use of political bots,
computational propaganda, and, correspondingly, disinformation and online polarization. Quantitative insight into the roles of automation, network structure, temporal markers, and message semantics over social media can allow experienced researchers to effectively create ways of measuring the flow of political manipulation over social media over sustained periods. The results of longitudinal research on this phenomenon will be crucial to building evolving long-term public and governmental understandings of computational propaganda.

There is potential for the continued use of bots as technologies for democratic engagement. There are also ongoing efforts in the academy to develop software to detect malicious bots and disinformation. Research-grounded tools to detect bots on social media, led by the team at Indiana University that developed Botometer (previously BotOrNot), are on the rise and are becoming more effective (Varol et al. 2018). Other groups are developing tools to study how disinformation, or fake news, is spread and whether or not a tweet is credible (Gupta et al. 2014; Shao et al. 2016). Start-ups including RoBhat Labs are simultaneously creating browser plug-ins and apps that track both bots and propaganda (Smiley 2017). As Varol and Uluturk (2018) aptly point out, however, “we should also be aware of the limitations of human-mediated systems as well as algorithmic approaches and employ them wisely and appropriately to tackle weaknesses of existing communication systems.” Software solutions, no matter how sophisticated the technology, can only mitigate a portion of the problems intrinsic to computational propaganda. Social solutions must be implemented as well.

REFERENCES


