

Deception Strategies and Threats for Online Discussions

Onur Varol^{a,*} and Ismail Uluturk^b

^aCenter for Complex Network Research, Northeastern University

^bUniversity of South Florida

*Correspondence to: ovarol@northeastern.edu

Abstract

Communication plays a major role in social systems. Effective communications, which requires transmission of the messages between individuals without disruptions or noise, can be a powerful tool to deliver intended impact. Language and style of the content can be leveraged to deceive and manipulate recipients. These deception and persuasion strategies can be applied to exert power and amass capital in politics and business. In this work, we provide a modest review of how such deception and persuasion strategies were applied to different communication channels over the years. We provide examples of campaigns that has occurred in different periods over the last 100 years, together with their corresponding dissemination mediums. In the Internet age, we enjoy

access to the vast amount of information and the ability to communicate without borders. However, malicious actors work toward abusing online systems to disseminate disinformation, disrupt communication, and manipulate people by the means of automated tools, such as social bots. It is important to study the old practices of persuasion to be able to investigate modern practices and tools. Here we provide a discussion of current threats against society while drawing parallels with the historical practices and the recent research efforts on systems of detection and prevention.

1 Introduction

Communication is a central part of the society and crucial for human evolution (Kirchner, 1997). All forms of living organisms develop or inherit ways to interact with each other (Wiley, 1983). Shannon's ground-breaking work formally defines the components of efficient communication systems and introduces concepts about information, noise, and transmission bandwidth (Shannon, 1949). Through human history, we see many forms of communication: verbal, written, artistic expressions, etc. Even one of the simplest forms of communication, drawing, serves as a tangible record that facilitates communication with future generations. Formation of signals and invention of languages are inevitable for evolving groups and systems to transfer information (Skyrms, 2010). Over the centuries, technology has helped us develop more efficient models of communication. Early use of paper and printing technologies have ensured the longevity of the records. Invention of the telegraph and the telephone overcame the difficulty of transmitting information over vast distances. These peer-to-peer communication systems mirror our natural interactions. We have also

invented different mechanisms to transmit information to larger audiences, instantaneously. The Internet became an archive for *virtually all knowledge* by organizing and storing petabytes of data daily. Recent collections surpass any conventional records of notable events and human narratives in history. Additionally, recent integrated systems have been storing streams of environmental sensory information and mobility of individuals, creating extensive archives that were not possible before.

Independent from the underlying technology and modes of communication, every communication system consists of three main components: sender, receiver, and the medium for dissemination. In most cases, transmission between the sender and the receiver is not perfect, and this can be attributed to the interference of noise within the medium or how information is encoded and decoded by the sender and the receiver, respectively. People have developed strategies that can convey information effectively by mimicking the receiver, adjusting their message, and trying to use different properties of the dissemination medium to be able to bridge the communication gap between two ends.

Cybernetics literature describes the systematic processes of meme diffusion. Heylighen shows the factors that contribute to the success of memes and the process that underlies its spread (Heylighen, 1998). He points to a 4-stage process: assimilation, retention, expression and transmission. Note that the first three steps are about how individuals adopt, process, and embody new information. Only the last stage describes the process of dissemination, however, fitness of memes relies on sender, receiver, and group properties along with the intrinsic qualities of memes.

In social psychology, there is a large body of work on persuasion and social influence (Chaiken et al., 1996; Cialdini, 1993; Wood, 2000) that talks about various cog-

nitive theories and psychological processes behind how people deceive and influence each other. Guadagno and Cialdini discuss persuasion and compliance in the context of Internet-mediated communications, especially textual messages (Guadagno and Cialdini, 2005). Examples of language and style matching can be seen in the language mimicry observed in the context of power differentials between discussants (Danescu-Niculescu-Mizil et al., 2012; Das et al., 2016; Bagrow et al., 2017) and the prediction of message popularity (Tan et al., 2014).

As the information within our reach grows exponentially, attention becomes the limiting factor in its consumption. Communication between humans is limited due to the evolutionary pressure applied by the finite amount of attention and favors efficiency over clarity (Dunbar, 1992). Herbert Simon introduced the term *attention economy* to explain human attention as a scarce commodity and the economic theory behind the various information processing strategies (Simon, 1971). Imperfect communication channels, as described by Shannon, are also relevant to human communications. Noise introduced to the communication channel might lead to imperfect transmission or misinterpretation by the receiver. We have invented different modes of communication to overcome these attention and noise limitations. When popularity and influence of the content is an important consideration, information producers should adopt a variety of strategies to convey their messages or use a medium that supports broader dissemination. Large-scale broadcasting of information introduces new channels for information dissemination. Radio, television, and newspapers are some examples of one-to-many communication tools.

The unprecedented increase in social media use may be the result of our limited attention and desire to reach information fast. Platforms like Twitter mainly serve

as information networks where people follow others to access the content they are sharing. Social connectivity on information networks deviates from offline social network structure, where connections between individuals is less likely to reflect their social relations (Kwak et al., 2010). Facebook and other similar social networks, on the other hand, reflect offline social network structure better where people tend to connect with their friends and colleagues. However, information networks promote formation of connections to maximize our need to access information. To save time when sharing the same content with larger audiences, we *broadcast*. To acquire relevant information, we *filter* and *prioritize* content to be able process it within our attention span. Long term information storage also addresses the limited attention issue by providing an opportunity to go back and access the necessary information when desired. Researchers emphasize the importance of the Internet in the study of mass communication and how theories about communication can be applied to this new medium (Morris and Ogan, 1996). Research by Philip Howard points to the important distinction between traditional and modern campaigning, produced by the shifting political culture (Howard, 2003).

Every communication system has a certain level of noise and disruptions that impacts the efficiency of the overall system. Temporal durability of the messages and limited attention of the receivers may be some of the more significant challenges for earlier communication systems. Recently, we have been facing more serious problems: deception, censorship, and abuse. Depending on the platform, malicious actors have several mechanisms available to them that can exploit the social trust between individuals and abuse the limited attention of users. Platforms like Facebook rely on personal connections, and we tend to believe what our friends share and this ten-

dency can be exploited. Information networks like Twitter, where the connections are built by the information need, on the other hand, are more prone to attacks by social bots and misleading content. The volume of available online data enables improved success for manipulation strategies through more accurate micro-targeting models, as social media platforms provide the tools to directly interact with users. While each interaction recorded online can be harnessed to develop better systems, adversaries can also use them to test and measure the performance of their malicious strategies just as easily. Researchers study these problems and develop systems that can prevent manipulation and gaming of the system for power and profit. Efforts to educate Internet users are also very important in the endeavor to prevent the dissemination of unreliable and misleading news.

In this work, we make a modest attempt to discuss the use of different communication channels and adoption of persuasion strategies. We aim to point out the different facets of deception on communication systems. We focus our attention to highlight the problems that we have been facing in the Internet age.

2 Interplay between politics and communication

Politics, in broad terms, can be defined as the process of making decisions that apply to all members of a group governed by the same entity. Alternatively, politics can represent the ideologies of a person who tries to influence the way a country is governed. To obtain such power and influence, politicians work towards obtaining trust of citizens and persuading their opposition to influence their attitudes. They are required to have strong communication skills and the ability to use available

technologies efficiently to reach their goals.

In the political system, we have been observing the impact of different communication media and how politicians adapt their strategies to influence and persuade voters and citizens (Castells, 2007; Krueger, 2006). We depict a timeline representation of technological development and how politicians adopted these trends in Fig. 1.

In the early days, newspapers and telegraph were important tools to diffuse news (Even and Monien, 1989; Blondheim, 1994). These technologies accelerated the information diffusion rate from days to hours. Mobilizing larger crowds for public speeches in parks and squares became easier, thanks to advertisements which made informing a broad audience more convenient. They also made sharing important policy decisions and public affairs more efficient.

The invention of the telephone and the radio, in 1870s and 1920s respectively, created opportunities for politicians to reach out to even larger groups. Television, for instance, changed political campaigns significantly (Simon and Ostrom, 1989; Behr and Iyengar, 1985; West, 2017). Only ten years after the first news program aired on the BBC, in 1947, President Truman gave his presidential speech live on TV. This trend was followed by the first TV advertisement placed by Eisenhower in 1952 and the first presidential debate between Kennedy and Nixon in 1960. One estimate of President Truman's campaign indicates that he was able to travel more than 31k miles and meet 500k voters in person. Only four years later, Eisenhower was able to reach millions through television advertisements (Diamond and Bates, 1992). It is also important to note that the nature of these political contacts during campaigns have also changed, as studied to learn more about voter behavior and carefully engineered to steer political discourse.

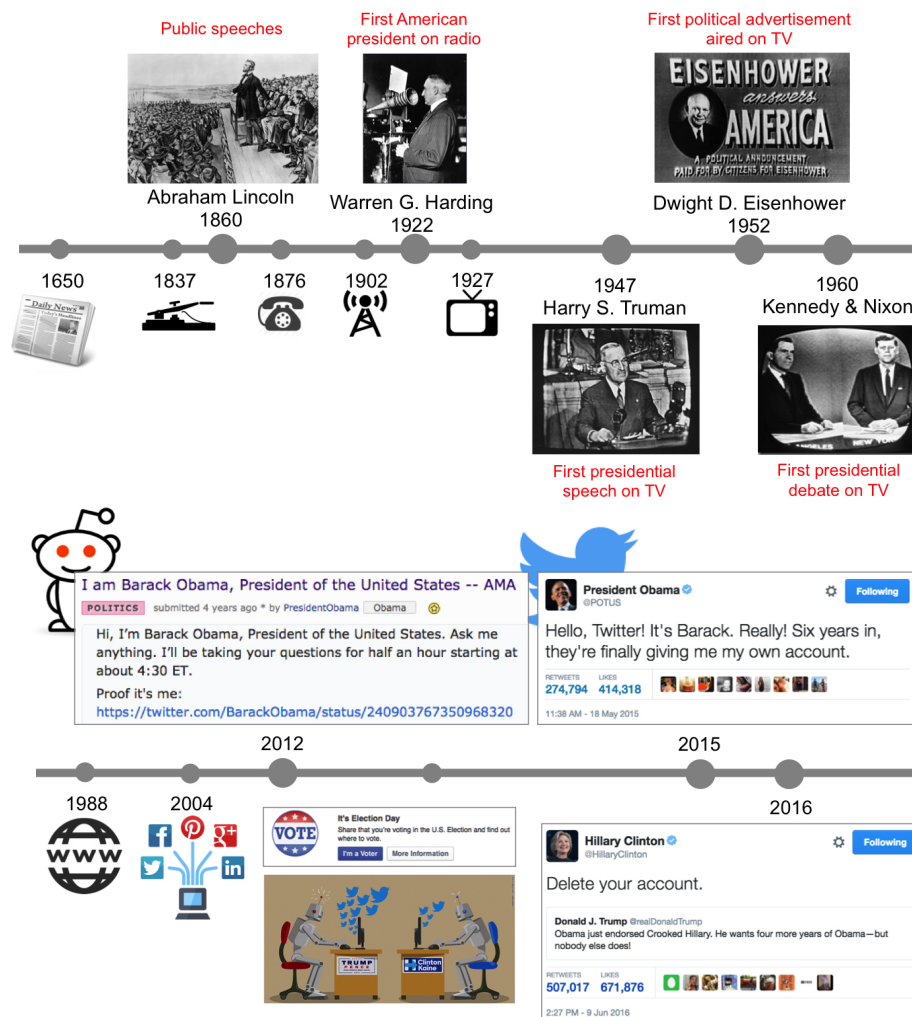


Figure 1: Timeline of US politics and its relation with the technological developments. Some of the leading events are selected. Top panel presents the influence of traditional communication mediums such as newspaper, radio and television. Bottom panel starts with the invention of the Internet and presents examples of US political presence on the internet.

The information age has transformed our experience in various ways. According to an analysis by Pew research center, 65 percent of US adults are actively using social media (Perrin, 2015). The Internet turns out to be a significant resource to study and answer valuable questions about communication in general (Morris and Ogan, 1996). Politicians have also become active users of the social media. They are able to engage with their constituents and campaign on social networks. Research on online mobilization shows that it is very effective to directly influence political expression, information seeking and real-world voting behaviour of millions of people (Bond et al., 2012).

In the last presidential election of the United States, we have observed an active role of social media. Researchers have been focusing on analyzing disinformation and social bots to better understand their impact on the election process in many elections around the world, especially the 2016 presidential election of the United States (Bessi and Ferrara, 2016; Ferrara, 2017; Howard et al., 2016; Howard and Kollanyi, 2016). We will discuss more on these subjects in the following sections.

3 Propaganda and campaigns on traditional media

Traditional communication channels like newspapers, radio, and TV have changed how political campaigns were organized and campaign funds were allocated, so these platforms can be used more efficiently. We provide examples from US politics, however, these observations are applicable to most countries. Here, we will delve into campaign strategies adopted on traditional media channels.

Advertisement has a significant role in reaching voters, and the goal of a successful campaign is to choose the right approach to ultimately win the election. Successful campaigns are often the ones with the most memorable themes and visuals that help sway the public opinion.

Since ancient Greek times, rhetoric and elocution have been recognized as the highest standard for a successful politician. Aristotle's rhetoric describes three main mechanisms for persuasion: *ethos*, *pathos*, and *logos* (Aristotle and Kennedy, 1992). *Ethos* is an appeal to authority, or the credibility of the presenter. If a presenter has credibility and possesses certain moral values, these moral values can be utilized to support a message. Examples of such campaigns were common among cigarette advertisements, showing actors dressed as doctors to mislead audiences. *Pathos* is another important component, which appeals to the emotions of the audience. *Pathos* might not only appeal to positive emotions like hope and gratitude, but also to negative emotions such as fear and feeling threatened. Lastly, *logos* is the logical appeal, or the simulation of it. It is commonly used by presenting facts and figures to support claims made by the presenter. It is often used together with *ethos*.

Persuasion and propaganda are the main tools in a traditional campaign. All forms of campaign media, such as posters, TV ads., etc., are the products of carefully engineered themes and messages. How public opinion is created and shaped in advertisement campaigns is explained by Edward Bernays in his seminal work "Crystallizing public opinion" together with various examples (Bernays, 2015).

In many cases, persuasion campaigns on politics take the form of propaganda, where persuaders work to achieve a desired response from the targeted audience by following a predefined agenda (Cunningham, 2002; Jowett and O'donnell, 2014). Pro-



Figure 2: Some of the notable examples of propaganda posters: “Uncle Sam” (Flagg, 1917), “Daddy, what did YOU do in the Great War?” (Committee, 1915), “We Can Do It!” (Miller, 1943), and a propaganda poster from the USA against Nazis and Japanese during the WWII (for Emergency Management. Office of War Information. Domestic Operations Branch. Bureau of Special Services, 1941).

paganda have been used in the past to recruit people for a cause, manipulate opinions of groups, and create conflicts between two parties. Earlier engineered propaganda campaigns used printed media, such as posters and newspaper advertisements, to reach their targeted audiences.

Common themes in propaganda posters are depicting an enemy as evil, or portraying yourself to look righteous (Mahaney, 2002). Some of the most memorable posters target various other personal traits and moral foundations as well (see Fig. 2). For instance, the “I Want You” poster presents Uncle Sam as a way to manifest patriotic emotion, which was used to recruit soldiers for both the first and the second world wars. A similar example of recruitment propaganda was released by the British government during WWI, which depicts a daughter posing a question to her father,

“Daddy, what did YOU do in the Great War?”. This poster is trying to manipulate an able man with the guilt associated with not volunteering for wartime service. “We Can Do It!” is another propaganda poster that was used to encourage involvement of women in the wartime economy during WWII. It later became popular for promotion of feminism and other political issues (Shover, 1975; Honey, 1985). An example of a poster that demonizes the enemy is also presented in Fig. 2. During war, stereotyping of the citizens of hostile countries and their values can often be seen in propaganda posters.

Perhaps not surprisingly, we observe an increase in comic book sales during international conflicts as well (Murray, 2000). Comic books are used as propaganda tools predominantly by employing visual cues to present cultural ideas embodied in flesh-and-blood characters. Ideas about nationalism, societal stability, and struggles over femininity were best presented by Superman, Batman, and Wonderwoman respectively (Chambliss, 2012). These depictions of ideas also create a state of psychological warfare between nations as well. They aim to gain leverage on their opponents without military intervention (Linebarger, 2015). The purpose of these propaganda campaigns is to affect the morale of their opponents, while making the current situation more appealing to their own citizens.

Another interesting example where media helped influence the social psyche is the original Godzilla movie from 1954 (Honda et al., 1954). The movie depicts the terrible destruction of Tokyo and its citizens, by an unstoppable radioactive monster whose signature attack is an atomic breath. It has provided the Japanese public, who were the only firsthand witnesses to the terrible powers of atomic weapons, a chance of cathartic relief. It has also allowed wider world audiences to face the devastation

that has been brought to Japan, while depicting the nation as an innocent bystander assaulted by forces beyond its control (Kalat, 2017).

Themes and motives used in political television advertisements show common parallels with the propaganda posters used during the Second World War. An analysis of over 800 TV advertising spots between 1960 and 1988 shows that *negativity* in the advertisements is mostly appealing to voters' fears (Kaid and Johnston, 1991). We observe shared components such as triggering fear and emotions, nationalism, and demonizing the enemy. Tony Schwartz, a media consultant, has created one of the most memorable election advertisements in US politics. "Daisy" spot was aired only once in 1964, but was later replayed several times in other news outlets because of its emotional impact. In this short clip, the association between a countdown for the atomic bomb and a young girl counting daisy petals is utilized to trigger emotional response and fear.

Power of television was widely used by politicians for reaching out to larger crowds, and increasing awareness of selected topics they deemed significant (Diamond and Bates, 1992; Benoit, 1999; Hermida, 2010; Dimitrova et al., 2014). Advertisements play the important role of putting the "typical citizen" on the spot and setting the norms and important questions. Politicians employ advertisements by either supporting their own campaigns, or attacking the policies of their opponents (Simon and Ostrom, 1989; Behr and Iyengar, 1985). One of the first examples of this effort was known as the "Eisenhower answers America" campaign, where the President answered questions recorded in a studio that contained important messages for his campaign.

Associating admired celebrities with certain ideologies is another strategy used

in political campaigns. McAllister discusses the personalization of politicians, and how political priming works through television (McAllister et al., 2007).

Persuasion is a broad term that covers different types of influence, including deceptive strategies. We have talked about how advertising is used to influence political beliefs. However, influence through advertisement is not the only type that affects and changes belief systems (Cialdini, 2001). Fake news and conspiracy theories are some examples of such deceptive strategies.

Most deception campaigns use strategies that present content along with conflicted facts and distorted claims by authorities (Clarke, 2002; Young and Nathanson, 2010). Conspiracy theories are one of the most extreme but persistent examples of disinformation. They appeal to the psychological urge to explain that mysterious things happen for a reason (Goertzel, 1994; Sunstein and Vermeule, 2009). Successful conspiracy theories emerge from a group of supporters, who believe in the sinister aims of higher entities such as governments, religious groups or even extraterrestrial life forms (Goodnight and Poulakos, 1981).

Censorship is the practice of repressing the dissemination of the truth, or opinions of opposing parties. Historically, practices such as collecting printed media, preventing the release of movies, or manipulating pictures or news to hide facts have been observed. Nazi Germany and USSR government under Joseph Stalin are both known to have collected books and other printed media and burned them during political repressions (Goldberg, 2006). Such practices have inspired dystopian novels like *Fahrenheit 451* (Bradbury, 2012) and *1984* (Orwell, 2009).

Censorship demands on various newspapers were protested by printing the censored content blank (Collins, 1996). Examples of such counter-censorship tactics



Figure 3: Example of news censorship in Poland (Wrocławia, 1981) on the top. Twitter withheld messages can be seen in the bottom for tweet and user censorship.

can be seen in French, Australian, and Palestinian media. In Fig. 3, we present an example of a censored newspaper from Poland dating back to 1981. In response to censorship, the newspaper decided to print the censored section with just the headlines and blank space instead of the text substituted by the censor. Recently, Twitter has introduced a similar precaution towards governmental censorship requests with the *withheld tweets* feature. Withheld tweets are censored only in the country that made the request to Twitter through official channels like governments and law enforcement. Twitter determines the user locations based on the IP addresses to apply the content censorship selectively. Users accessing Twitter from a censored country

are notified by the template tweets in Fig. 3. Therefore, users are notified that the tweets they are trying to access are being censored, serving a similar purpose as the historical examples of white spaces placed by newspaper editors.

We would also like to note that, censorship can also be applied by disrupting the communication channels and making them nonfunctional for the users, for example, by the excess activity of social bots. An example of such communication disruption through bots was observed in Mexico (Suárez-Serrato et al., 2016).

4 Deception in the age of the Internet

Technologically mediated communication systems, like social media platforms and social networks, support the production of information cascades and connect millions of individuals (Goel et al., 2015; boyd and Ellison, 2010; Vespignani, 2009). Our society has been going through profound changes about how we consume and produce information (Aral and Walker, 2012; Bond et al., 2012), how we interact with our peers (Centola, 2010, 2011), and how we seek information about societal events surrounding us (Metaxas and Mustafaraj, 2013, 2012).

We are exposed to a tremendous amount of information through social media platforms. Social networks help us organize at least a part of this information, through what our friends share. However, some of the information we share with our network may be inaccurate, and that means we are unintentionally helping the dissemination of misinformation. We may be helping malicious entities, and promoting a disinformation campaign by naively sharing content we find appealing. Our friends in the network are also likely to have similar interests and tendencies as we

do, which leads to the spread of misinformation content due to homophily (McPherson et al., 2001). The echo chambers that we live in also help the amplification of this misinformation (Adamic and Glance, 2005; Conover et al., 2011).

Integrating social media as a dissemination medium provides opportunities for everyone to share their stories and experiences. Some governments take this as a threat to their established system and try to mitigate online activity around certain subjects. One mechanism commonly employed by governments around the world is using Internet censorship, or blocking service providers. These practices terminate the users right to access information.

Malicious actors on social media can also employ typical misinformation and deception campaigns. *Astroturf*, for instance, is a peculiar form of deception, often observed on social media in the context of politics and social mobilization (Ratkiewicz et al., 2011b). It aims to emulate a grassroots conversation through an orchestrated effort. Although the history of astroturfing and lobbying is older than social networks, these platforms provide a more visible stage for the interactions between online presences of front groups and the promoted accounts (Howard, 2003; Murphy, 2012). Actors who attempt to generate such orchestrated campaigns generally exploit fake accounts or social bots (Hwang et al., 2012; Wagner et al., 2012; Ferrara et al., 2016a). These artificial means allow the generation of a large volume of content, and emulate the online activity of real users. Cases of massive astroturf campaigns have been observed during political races such as the US senate (Mustafaraj and Metaxas, 2010) and presidential elections (Metaxas and Mustafaraj, 2012; Bessi and Ferrara, 2016).

In this section, we have provided examples and mechanisms of campaigns that

operate using social bots, disseminate fake news, and apply censorship to restrain the reach of credible information sources. These practices have become very powerful, and the consequences of their involvement remains to be an important research question.

4.1 Social bots

Increasing evidence suggests that a growing amount of social media content is generated by autonomous entities known as social bots (Varol et al., 2017a; Howard et al., 2017; Ferrara et al., 2016a; Aiello et al., 2012). As opposed to social media accounts controlled by humans, bots are controlled by software, algorithmically generating content and establishing interactions. While not all social bots are harmful, there is a growing record of malicious applications of social bots. Some emulate human behavior to manufacture fake grassroots political support (Ratkiewicz et al., 2011a), promote terrorist propaganda and recruitment (Berger and Morgan, 2015; Ferrara et al., 2016c; Bessi and Ferrara, 2016; Woolley, 2016), manipulate the stock market or advertisements (Clark et al., 2015; Ferrara, 2015), and disseminate rumors and conspiracy theories (Bessi et al., 2015a).

Discussion of social bot activity, their broader implications on social networks, and the detection of these accounts are becoming central research avenues (Lee et al., 2011; Boshmaf et al., 2011; Ferrara et al., 2016a; Ferrara, 2015). Magnitude of the problem is underscored by a social bot detection challenge, recently organized by DARPA to study the information dissemination mediated by automated accounts, and to detect malicious activities carried out by these bots (Subrahmanian et al., 2016). A recent study on social bots reports that 9 to 15 percent of all active

users among English-speaking population exhibits bot-likely behaviors (Varol et al., 2017a). Researchers are also working on identifying social bots with different behavioral patterns and interaction styles. Analysis of social bots during US presidential election points out that more than 20 percent of the accounts were exhibiting social bot behavior (Bessi and Ferrara, 2016). Another analysis points that one third of the total volume of tweets and shared online news articles supporting the political candidates during 2016 election were consisted of fake or extremely biased news (Bovet and Makse, 2018). Influence of external factors on the US presidential election in 2016 is a source of controversy. Recent research shows evidence supporting the involvement of social bots in political discourse (Bessi and Ferrara, 2016).

Participation of social bots on political conversations are not necessarily needed to be sophisticated. Simple interactions such as retweeting can still be powerful, considering the visibility it might lead to. Purchasing fake followers is also common among politicians that wish to create a false impression of popularity (Woolley, 2016). Recent research shows evidence that social bots played a key role in the spread of fake news during the 2016 US presidential election (Shao et al., 2017) and most of the central actors in the diffusion network consisted of bots (Shao et al., 2018). Social bots are also known to disrupt conversations by flooding a particular conversation channel with content. Pollution of conversations on social media makes it intractable for individuals looking for useful information.

Social bots can also be used for coordinated activities where large collections of social bots, also known as botnets, are controlled by botmasters. Examples of such botnets have been identified for advertisements (Echeverra and Zhou, 2017) and influencing Syrian civil war (Abokhodair et al., 2015). The orchestrated behavior

of thousands of bots is worrisome, since they can be used to pollute conversation channels, boost the popularity of disinformation content, and target individuals to deceive them on certain subjects. Social bots also vary greatly in terms of their behavior, intent, and vulnerabilities, as described by Mitter *et al.* (Mitter et al., 2013).

4.2 Fake news

The term *fake news* is not new (Lippmann, 2004), yet the prevalence of the online disinformation come in different forms and properties: hoaxes, rumors, conspiracy theories, etc. Fake news websites deliberately publish hoaxes, propaganda, and disinformation pretending to be a legitimate news source. They often aim to mislead readers, unlike the satirical news websites that may appear similar, in exchange for political and financial gain.

A large amount of disinformation spreads online, and their prevalence and persuasiveness can affect serious decisions around important topics such as vaccination (Kata, 2012; Nyhan et al., 2013; Buttenheim et al., 2015), elections (Allcott and Gentzkow, 2017; Mustafaraj and Metaxas, 2017; Giglietto et al., 2016; Rojecki and Meraz, 2016) and stock market behavior (Carvalho et al., 2011; Lauricella et al., 2013) among other issues. A recent study suggests that misinformation is just as likely to go viral as reliable information (Shao et al., 2016; Qiu et al., 2017). One of the mechanisms promoting the persistence of fake news is the copycat websites. Copycat websites operate by duplicating the original content with only trivial changes. If the original article contains misinformation, copycat websites replicate this misinformation as well. Corrections or removal of the original source are no longer relevant or

useful, since many other media outlets are already affected and have already disseminated false information. We can make an analogy between the dissemination of fake news through multiple media outlets and a disease spreading in groups, vaccination or treatment of a single individual will not stop an epidemic by itself. In some cases, even reliable sources can publish misinformation, simply because of the competition introduced by online journalism. The rush to break the news first has lead news agencies to employ automation tools in their workflows, from tools that write complete articles like the Automated Insights used by Associated Press,¹ to news discovery tools like the Reuters Tracer by Reuters. Reuters Tracer parses through millions of tweets every day and reportedly gives Reuters a 8 to 60 minutes of a headstart on news pieces against its competitors (Liu et al., 2017). While automated tools like the Reuters Tracer are being employed to help verify stories in a timely manner as well (Liu et al., 2017), the continuously narrowing window to break a story may lead to articles lacking deliberate investigation which will then be picked up and disseminated by copycat sites before any corrections can be made. It is almost impossible to propagate corrections to all other copycat articles that are based on the original piece. (Janowitz, 1975)

Recent research efforts have also focused on modeling the diffusion of misinformation (Del Vicario et al., 2016; Bessi et al., 2015a,b; Friggeri et al., 2014; Jin et al., 2013). Algorithmic efforts on detecting rumors and misinformation are also crucial to prevent the spread of campaigns with malicious intents (Varol et al., 2017b; Ferrara et al., 2016b; Resnick et al., 2014; Metaxas et al., 2015; Qazvinian et al., 2011).

Journalists and readers both have important roles and responsibilities to hinder

¹<https://automatedinsights.com/case-studies/associated-press>

the dissemination of fake news. Online websites like *FactCheck*,² *PolitiFact*,³ and *Snopes*⁴ provide fact-checking services to debunk fake news. Fact-checking provided by online services influences the opinions of voters, and provides politicians a guide in judging what news might be fake before disseminating it (Fridkin et al., 2015; Nyhan and Reifler, 2015). Researchers are working on designing systems that can evaluate the credibility and truthfulness of claims in order to automate the fact-checking process (Ciampaglia et al., 2015; Wu et al., 2014).

The problem with fake news can be partially resolved by educating Internet users. *News literacy* is important, and everyone should at least make an effort to learn how they can identify fake news. Recently, we have been observing a growing community of fact-checkers. *Poynter* is one of these organizations, which has released “International Fact-Checking Network fact-checkers’ code of principles”⁵ to promote excellence in fact-checking. Another noteworthy example is *First draft*.⁶ These organizations not only provide fact-checked information about popular claims, but they also monitor political campaigns and elections. Collaboration between different fact-checking organizations is promoted by proposing an integrated system to share fact-checking information by implementing *ClaimReview* schema.⁷

²factcheck.org

³politifact.com

⁴snopes.com

⁵poynter.org/fact-checkers-code-of-principles/

⁶firstdraftnews.com

⁷schema.org/ClaimReview

4.3 Censorship

Preventing censorship and supporting the freedom of speech is crucial in continuing services like social networks, where people can freely express their opinion as long as they avoid disruptive behavior such as abuse and harassment. According to a report by the watchdog organization Freedom House, out of 65 countries tracked, 49 of them have received a rating of “Not Free” or “Partly Free” on internet freedom within the observation period of June 2016 to May 2017. This means less than a quarter of the users are living in countries where internet has received “Free” designation. While the report also states that the internet is still more free from censorship compared to traditional press, it points out that internet freedom has declined in 32 countries while making mostly minor gains in only 13, showing a downward trend (Kelly et al., 2017).

In some societies, governments have responded to the political mobilizations by either terminating the access to online services, or developing laws to restrict the exchange of information (Zhang, 2006). China, Iran, North Korea, and Turkey are examples of countries applying internet censorship widely. These countries are monitoring social media and news with the intention of controlling the online discourse. If discussions steer into sensitive topics, concerned governments intervene and attempt to control information dissemination (King et al., 2013; Ali and Fahmy, 2013).

Platforms like Facebook and Twitter have been censored in the past by limiting the internet access at the country level. Social media companies have recently created specialized legal departments to address requests from governments, with hopes to provide continuous service for their users in countries that employ censorship regularly. Periodically, transparency reports are released by technology companies like

Facebook,⁸ Twitter,⁹ Microsoft,¹⁰ and Google.¹¹ These reports contain the statistics of requests received from different governments, including requests for disclosure of information. The increasing trend in government requests for disclosure of user information and censorship requests are worrisome.

Many censorship regulations are developed to control or limit dissemination of political discussions. A recent study highlights a significant rate of content removal on Weibo (Bamman et al., 2012). They estimated that 16 percent of the posts compared to overall activity are deleted by authorities on Weibo due to their political content. The content analysis of the censorship on Weibo points out that, content that is aiming to create oppositional awareness towards the Chinese Communist Party are censored more frequently (Vuori and Paltemaa, 2015). The political impact of micro-blogging platforms was analyzed by comparing Twitter and Weibo use in China (Sullivan, 2012).

In another analysis of Weibo, researchers have studied the mechanism of Weibo's trending topic detection system to track sensitive viral discussions (Zhu et al., 2012). Authors have also showed the mechanism behind content filtering by tracking sensitive users (Zhu et al., 2013). They have found that the trend of a sensitive viral topic is short-lived, which points to the effectiveness of Weibo's censorship on sensitive topics.

Twitter requires legal documents to censor content on their platform, unlike the Chinese social media that has centralized control over censorship with no regulatory

⁸govtrequests.facebook.com

⁹transparency.twitter.com

¹⁰microsoft.com/en-us/about/corporate-responsibility/reports-hub

¹¹google.com/transparencyreport

oversight. Twitter announced their “withheld tweet” mechanisms to abide by governmental requests in 2012 after the Internet service provider (ISP) level blockages by various governments. If removal requests are submitted properly by authorized entities, Twitter grants censorship to these requests. Other than content removal, Twitter can limit access to a particular tweet or user when requested by governments. Previous analysis of Twitter withheld content shows that the topical groups that get censored are emerging around politically sensitive topics (Tanash et al., 2015). There has also been an increasing trend in the amount of censored content on Twitter over the years (Varol, 2016).

Historically, censorship implies hindering peoples access to content. An alternative mechanism of censorship is the manipulation of the source directly. A well-known example of such manipulation is the edited photographs from USSR under Joseph Stalin’s government, where members of the party that fell out of favor were removed from the pictures. Editorial censorship of newspapers and books are additional examples of such manipulation. These strategies have become much more difficult in the current online systems, where records of a source are replicated and stored in a distributed manner. However, it is also possible censor content by polluting the communication medium. Finding reliable information within low signal to information ratio channels is becoming a new challenge. It is possible to use social bots to create bursts of posts to distract users and pollute communication channels. An example of such channel disruptions were observed in Mexico recently (Suárez-Serrato et al., 2016), when different hashtags were flooded by social bots, forcing people to move the discussion to alternative channels.

Technical developments like VPN services or the TOR project¹² can provide resilience against censorship attempts. Researchers have also built services to quantitatively measure the censorship problem (Burnett and Feamster, 2013) and analyze the examples of country-wide Internet outages (Dainotti et al., 2011; Verkamp and Gupta, 2012).

So far, we have briefly described the strategies and mechanisms of deception for traditional media and online platforms. We have also presented recent research efforts for detecting malicious intentions and building platforms to improve the existing situation.

5 Discussion

We have shown the mechanisms of traditional campaigns and modern persuasion techniques so far. Here, we will discuss how we can benefit from the lessons provided by historical evidence and prepare to engage malicious actors proactively. We will present modern threats for the online echo-chambers and introduce research directions for prevention mechanisms.

Current campaigns have been adapting their tactics from the historical examples we have presented to the developments in technology. Tools for dissemination and manipulation have also been evolving and developing alongside campaign tactics to address the new demands of advancements. In terms of human behavior, we are still vulnerable to the similar cognitive biases, which can be used to manipulate opinions of and trigger certain behaviors from individuals and groups. Taking similarities and

¹²torproject.org

differences between modern and historical campaigns into consideration, we have the chance to turn the technological and research efforts into our advantage.

Efforts in designing viral online campaigns have yielded the development of modern marketing tools and strategies. Unfortunately, malicious actors are also able to benefit from such developments and adopt them to achieve their ends. Successful campaigns often rely on carefully designed messages and punctual timing. Experts in social psychology can identify possible concepts to frame their campaigns to target specific groups. Nowadays, the volume and velocity of the data are significantly increased, and thanks to that, evaluating different strategies for manipulation and framing messages have become virtually effortless. The abundance of digital data and developments on personalization might result in building targeted campaigns and the ability to rapidly evaluate the effects of different campaign components. We are living in a data-rich world that helps with accurate estimates of demographics and personal characteristics (Kosinski et al., 2013).

Researchers demonstrated the predictive power of Facebook data in a 2013 article by predicting various personality traits, demographic information, sexual orientation, and political leaning (Kosinski et al., 2013). Facebook has also published results of their experiment on randomized controlled trial of political mobilization messages during 2010 US congressional elections, in which they delivered messages to 61 Million users (Bond et al., 2012). Facebook demonstrated how minor interventions to the content they deliver can influence real-world voting behavior. Emotional contagion phenomenon is also demonstrated on Facebook by manipulating the content of the posts Kramer et al. (2014). This work shows experimental evidence on emotional contagion without direct interaction between individuals.

The recent example of a controversy about a British political consulting firm called *Cambridge Analytica* demonstrates how a social media platform can become an instrument for political manipulation. The company claims that they have capabilities to build *psychographics* models to predict the propensities of user behavior towards different stimuli such as social media posts with different sentiment and content. Their data collection methods raise serious concerns about privacy and breach of institutional review board (IRB) protocols. Researchers from Cambridge University have created a Facebook application called *thisisyourdigitallife* to collect the information of users and their friends for a research project, however this data later got shared with Cambridge Analytica to build models that company has claimed to be effective for micro-targeting.¹³ Although effectiveness of Cambridge Analytica's methodologies is still not clear, it is important to make our points on data privacy and use of technology for political manipulation.

Another past case, a UCLA mathematician who has employed *social bots*, *user profiling* and *targeting* on an online dating platform, may serve as a concrete example to help understand how these methods can be employed to achieve real-world results. He has used *social bots*, that were programmed to mimic human users to circumvent safety measures, to mine OKCupid, a popular dating site, for the data from thousands of users. He then used this data to *profile* users and found out that the users fell within one of seven distinct clusters. He analyzed these clusters and decided that he was only interested in users within two out of the seven. Finally, he has used a machine-learning algorithm to *target* these users and help maximize his match

¹³niemanlab.org/2018/03/this-is-how-cambridge-analyticas-facebook-targeting-model-really-worked-according-to-the-person-who-built-it

percentage with them, resulting in a very large number of users with unusually high match percentages (Poulsen, 2014). It demonstrates that, with the necessary know-how, even a single person with limited resources can achieve meaningful real-world impact.

Social bots have been getting increasingly better fake persona generation (Li et al., 2016a; Bhatia et al., 2017) and conversation models thanks to the advancements in deep-learning technologies (Sordoni et al., 2015; Li et al., 2016b). Such technologies make detection of social bots more difficult and provide an advantage to the bot creators in this arms race. Targeted attacks are made possible through the anonymous use of social media, by orchestrating a large army of social bots, trolls (McCosker, 2014; Aro, 2016), sock puppets, and bullies (Bellmore et al., 2015; Resnik et al., 2016). Examples of extremist activities on social media have been increasing at an alarming rate, and many platforms have started taking precautions for early-detection and prevention of such activities. Recent studies have also pointed to the use of social media for the recruitment efforts of terrorist organizations (Berger and Morgan, 2015; Ferrara et al., 2016c; Magdy et al., 2015).

Increasing online participation on websites and social media is creating new avenues for and enabling new forms of deception and manipulation (Phillips and Milner, 2018). We have been particularly observing the societal impact of disinformation manufactured with the intent of drawing an extreme reaction, disseminated by cloaked websites and accounts (Daniels, 2009; Farkas et al., 2017). It is important and valuable to understand the roots of the problem before setting out to propose solutions. Confirmation bias is considered one of the contributing factors (Nickerson, 1998). According to this hypothesis, people tend to believe and seek information

supporting their initial opinions. An alternative explanation considers the attention paid to judge the credibility of the source. Herbert Simon's work on attention economy might help explain some of our mental shortcuts; we tend to believe a content based on our opinions about the friend who had shared it with us. Researchers have studied when readers pay attention to the source of the content (Kang et al., 2011). They have found that users tend to believe the content based solely on the source they obtained it from, unless the subject is really important to them. Trust towards personal contacts also makes individuals more vulnerable to attacks such as phishing (Jagatic et al., 2007). These problems can be alleviated by focusing on news literacy. It is possible to restrain the prevalence of fake news when educated online users are combined with appropriate fact-checking tools. A recent review on fake news lays out a future agenda and invites interdisciplinary research efforts to study the spread of fake news and its underlying mechanisms (Lazer et al., 2018).

Throughout the 20th century, people living in a number of developed countries had access to credible information through accountable sources, where the content was monitored by editorial boards for accuracy prior to publishing. However, in the age of Internet, the mechanisms for information production by journalists and news websites have been changing (Giglietto et al., 2016). These changes are also effecting how we access and consume information. Most of the content of an article is created by an original source where many other websites can copy it from, and various services can propagate the content even further. The role of social media in this process is crucial, since users can share those links through their network. These cascades of dissemination can cause problems if the original content has erroneous claims. Correcting the original source after the fact in this process is not likely to

fix copycat content and misinformation already disseminated by social media users.

We should also raise our concerns about the third-party applications connected to social media accounts with user permissions. If these applications are breached by malicious entities, they can be employed to disturb communication channels and disseminate misinformation. A recent example of such an attack have targeted hundreds of Twitter accounts, including popular news organizations and celebrities, when a third-party analytics application was compromised (Kharpal, 2017). These accounts have posted tweets, written in Turkish, that contained the swastika symbol and hashtags which, when translated, mean “Nazi Germany” and “Nazi Holland”. Accounts compromised by this attack, such as Forbes (@forbes), Germany soccer club Borussia Dortmund (@BVB), and Justin Bieber’s Japanese account (@bieber_japan) have the combined follower count of several millions. Considering the wide reach of such a compromise in a 3rd party application is worrisome.

Another concern on third-party applications is their ability to change social ties. Applications with necessary permissions can follow and unfollow accounts through APIs. This can lead to long-term manipulation of how people access information by selectively filtering content or providing exposure to certain users. Segregation and filter bubbles are foreseeable threats that can utilize untrustworthy or compromised applications. Similarly, adversaries can benefit from the changing attitudes towards fake followers to discredit influential accounts by contaminating their followers with social bots. It is important to develop methodologies that can be employed by the platforms to identify these attacks, build preventive strategies, and prevent data breaches.

Sir Tim Berners-Lee published a post on the 29th birthday of World Wide Web

to share some concerns and challenge our community to make WWW a safer, more accessible, and transparent place for everyone.¹⁴ There are significant efforts to preserve the social ecosystem. Researchers are developing tools like Botometer¹⁵ (Davis et al., 2016; Varol et al., 2017a) to detect social bots on Twitter, Hoaxy¹⁶ (Shao et al., 2016) to study dissemination of fake news, and TweetCred¹⁷ (Gupta et al., 2014) to evaluate the credibility of tweet contents. The Jigsaw lab of Google also has significant efforts to tackle some of the global security challenges, working on systems and tools to prevent censorship and online harassment.¹⁸ Considering the impact of technology on the dissemination of misinformation, we share a great responsibility to work together. 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 the weaknesses of existing communication systems. Computer scientists, social scientists, journalists, and other industry partners must collaborate in the effort to implement policies and systems against online threats for an effective resistance.

Acknowledgement

I want to thank our anonymous reviewers, Christine Ogan, and Filippo Menczer for their insightful discussions and feedback.

¹⁴webfoundation.org/2018/03/web-birthday-29

¹⁵botometer.iuni.iu.edu

¹⁶hoaxy.iuni.iu.edu

¹⁷twitdigest.iiitd.edu.in/TweetCred

¹⁸jigsaw.google.com

References

- Abokhodair, N., Yoo, D., and McDonald, D. W. (2015). Dissecting a social botnet: Growth, content and influence in twitter. In *Proc. of the 18th ACM Conf. on Computer Supported Cooperative Work & Social Computing*, pages 839–851. ACM.
- Adamic, L. A. and Glance, N. (2005). The political blogosphere and the 2004 us election: divided they blog. In *Proceedings of the 3rd international workshop on Link discovery*, pages 36–43. ACM.
- Aiello, L. M., Deplano, M., Schifanella, R., and Ruffo, G. (2012). People are strange when you’re a stranger: Impact and influence of bots on social networks. In *Proc. 6th Intl. AAAI Conf. on Weblogs and Social Media (ICWSM)*.
- Ali, S. R. and Fahmy, S. (2013). Gatekeeping and citizen journalism: The use of social media during the recent uprisings in iran, egypt, and libya. *Media, War & Conflict*, 6(1):55–69.
- Allcott, H. and Gentzkow, M. (2017). Social media and fake news in the 2016 election. Technical report, National Bureau of Economic Research.
- Aral, S. and Walker, D. (2012). Identifying influential and susceptible members of social networks. *Science*, 337(6092):337–341.
- Aristotle and Kennedy, G. A. (1992). *Rhetoric*. JSTOR.
- Aro, J. (2016). The cyberspace war: propaganda and trolling as warfare tools. *European View*, 15(1):121–132.
- Bagrow, J. P., Liu, X., and Mitchell, L. (2017). Information flow reveals prediction limits in online social activity. *arXiv preprint arXiv:1708.04575*.
- Bamman, D., O’Connor, B., and Smith, N. (2012). Censorship and deletion practices in chinese social media. *First Monday*, 17(3).

- Behr, R. L. and Iyengar, S. (1985). Television news, real-world cues, and changes in the public agenda. *Public Opinion Quarterly*, 49(1):38–57.
- Bellmore, A., Calvin, A. J., Xu, J.-M., and Zhu, X. (2015). The five ws of bullying on twitter: who, what, why, where, and when. *Computers in human behavior*, 44:305–314.
- Benoit, W. L. (1999). *Seeing spots: A functional analysis of presidential television advertisements, 1952-1996*. Greenwood Publishing Group.
- Berger, J. and Morgan, J. (2015). The isis twitter census: Defining and describing the population of isis supporters on twitter. *The Brookings Project on US Relations with the Islamic World*, 3:20.
- Bernays, E. L. (2015). *Crystallizing public opinion*. Open Road Media.
- Bessi, A., Coletto, M., Davidescu, G. A., Scala, A., Caldarelli, G., and Quattrociocchi, W. (2015a). Science vs conspiracy: Collective narratives in the age of misinformation. *PLoS ONE*, 10(2):e0118093.
- Bessi, A. and Ferrara, E. (2016). Social bots distort the 2016 us presidential election online discussion. *First Monday*, 21(11).
- Bessi, A., Petroni, F., Del Vicario, M., Zollo, F., Anagnostopoulos, A., Scala, A., Caldarelli, G., and Quattrociocchi, W. (2015b). Viral misinformation: The role of homophily and polarization. In *Proceedings of the 24th International Conference on World Wide Web*, pages 355–356. ACM.
- Bhatia, P., Gavalda, M., and Einolghozati, A. (2017). soc2seq: Social embedding meets conversation model. *arXiv preprint arXiv:1702.05512*.
- Blondheim, M. (1994). *News over the wires: The telegraph and the flow of public information in America, 1844-1897*. Number 42. Harvard University Press.
- Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D., Marlow, C., Settle, J. E., and Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature*, 489(7415):295–298.

- Boshmaf, Y., Muslukhov, I., Beznosov, K., and Ripeanu, M. (2011). The socialbot network: when bots socialize for fame and money. In *Proc. 27th Annual Computer Security Applications Conf.*
- Bovet, A. and Makse, H. A. (2018). Influence of fake news in twitter during the 2016 us presidential election. *arXiv preprint arXiv:1803.08491*.
- boyd, d. and Ellison, N. B. (2010). Social network sites: Definition, history, and scholarship. 2007. *Journal of Computer-Mediated Communication*, 13(1).
- Bradbury, R. (2012). *Fahrenheit 451: A Novel*. Simon and Schuster.
- Burnett, S. and Feamster, N. (2013). Making sense of internet censorship: a new frontier for internet measurement. *ACM SIGCOMM Computer Communication Review*, 43(3):84–89.
- Buttenheim, A. M., Sethuraman, K., Omer, S. B., Hanlon, A. L., Levy, M. Z., and Salmon, D. (2015). Mmr vaccination status of children exempted from school-entry immunization mandates. *Vaccine*, 33(46):6250–6256.
- Carvalho, C., Klagge, N., and Moench, E. (2011). The persistent effects of a false news shock. *Journal of Empirical Finance*, 18(4):597–615.
- Castells, M. (2007). Communication, power and counter-power in the network society. *International journal of communication*, 1(1):29.
- Centola, D. (2010). The spread of behavior in an online social network experiment. *Science*, 329:1194–1197.
- Centola, D. (2011). An experimental study of homophily in the adoption of health behavior. *Science*, 334(6060):1269–1272.
- Chaiken, S., Wood, W., and Eagly, A. H. (1996). Principles of persuasion.
- Chambliss, J. C. (2012). Superhero comics: Artifacts of the us experience. *Juniata Voices*, 12:149.
- Cialdini, R. B. (1993). Influence: The psychology of persuasion.

- Cialdini, R. B. (2001). Science and practice.
- Ciampaglia, G. L., Shiralkar, P., Rocha, L. M., Bollen, J., Menczer, F., and Flammini, A. (2015). Computational fact checking from knowledge networks. *PLoS ONE*, 10(6):e0128193.
- Clark, E. M., Jones, C. A., Williams, J. R., Kurti, A. N., Nortotsky, M. C., Danforth, C. M., and Dodds, P. S. (2015). Vaporous marketing: Uncovering pervasive electronic cigarette advertisements on twitter. *arXiv preprint arXiv:1508.01843*.
- Clarke, S. (2002). Conspiracy theories and conspiracy theorizing. *Philosophy of the Social Sciences*, 32(2):131–150.
- Collins, R. F. (1996). A battle for humor: satire and censorship in le bayard. *Journalism & Mass Communication Quarterly*, 73(3):645–656.
- Committee, B. P. R. (1915). Daddy, what did you do in the great war? [Online; accessed February 27, 2017].
- Conover, M., Ratkiewicz, J., Francisco, M., Gonçalves, B., Flammini, A., and Menczer, F. (2011). Political polarization on Twitter. *Proceedings of the 5th International AAAI Conference on Weblogs and Social Media*.
- Cunningham, S. B. (2002). *The idea of propaganda: A reconstruction*. Greenwood Publishing Group.
- Dainotti, A., Squarcella, C., Aben, E., Claffy, K. C., Chiesa, M., Russo, M., and Pescapé, A. (2011). Analysis of country-wide internet outages caused by censorship. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pages 1–18. ACM.
- Danescu-Niculescu-Mizil, C., Lee, L., Pang, B., and Kleinberg, J. (2012). Echoes of power: Language effects and power differences in social interaction. In *Proceedings of the 21st international conference on World Wide Web*, pages 699–708. ACM.

- Daniels, J. (2009). Cloaked websites: propaganda, cyber-racism and epistemology in the digital era. *New Media & Society*, 11(5):659–683.
- Das, A., Gollapudi, S., Kıcıman, E., and Varol, O. (2016). Information dissemination in heterogeneous-intent networks. In *Proceedings of the 8th ACM Conference on Web Science*, pages 259–268. ACM.
- Davis, C. A., Varol, O., Ferrara, E., Flammini, A., and Menczer, F. (2016). Botornot: A system to evaluate social bots. In *Proceedings of the 25th International Conference Companion on World Wide Web*, pages 273–274. International World Wide Web Conferences Steering Committee.
- Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Stanley, H. E., and Quattrociocchi, W. (2016). The spreading of misinformation online. *Proceedings of the National Academy of Sciences*, 113(3):554–559.
- Diamond, E. and Bates, S. (1992). *The spot: The rise of political advertising on television*. Mit Press.
- Dimitrova, D. V., Shehata, A., Strömbäck, J., and Nord, L. W. (2014). The effects of digital media on political knowledge and participation in election campaigns: Evidence from panel data. *Communication Research*, 41(1):95–118.
- Dunbar, R. I. (1992). Neocortex size as a constraint on group size in primates. *Journal of Human Evolution*, 22(6):469–493.
- Echeverra, J. and Zhou, S. (2017). The ‘star wars’ botnet with 350k twitter bots. *arXiv preprint arXiv:1701.02405*.
- Even, S. and Monien, B. (1989). On the number of rounds necessary to disseminate information. In *Proceedings of the first annual ACM symposium on Parallel algorithms and architectures*, pages 318–327. ACM.
- Farkas, J., Schou, J., and Neumayer, C. (2017). Cloaked facebook pages: Exploring fake islamist propaganda in social media. *New Media & Society*, page 1461444817707759.

- Ferrara, E. (2015). Manipulation and abuse on social media. *SIGWEB Newsletter*, Spring(4):1–9.
- Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 french presidential election. *First Monday*.
- Ferrara, E., Varol, O., Davis, C., Menczer, F., and Flammini, A. (2016a). The rise of social bots. *Communications of the ACM*, 59(7):96–104.
- Ferrara, E., Varol, O., Menczer, F., and Flammini, A. (2016b). Detection of promoted social media campaigns. In *Tenth International AAAI Conference on Web and Social Media*.
- Ferrara, E., Wang, W.-Q., Varol, O., Flammini, A., and Galstyan, A. (2016c). Predicting online extremism, content adopters, and interaction reciprocity. In *International Conference on Social Informatics*, pages 22–39. Springer.
- Flagg, J. M. (1917). Uncle sam. [Online; accessed February 27, 2017].
- for Emergency Management. Office of War Information. Domestic Operations Branch. Bureau of Special Services, O. (1941). Stop this monster that stops at nothing. produce to the limit. this is your war. [Online; accessed February 27, 2017].
- Fridkin, K., Kenney, P. J., and Wintersieck, A. (2015). Liar, liar, pants on fire: How fact-checking influences citizens reactions to negative advertising. *Political Communication*, 32(1):127–151.
- Friggeri, A., Adamic, L. A., Eckles, D., and Cheng, J. (2014). Rumor cascades. In *ICWSM*.
- Giglietto, F., Iannelli, L., Rossi, L., and Valeriani, A. (2016). Fakes, news and the election: A new taxonomy for the study of misleading information within the hybrid media system.
- Goel, S., Anderson, A., Hofman, J., and Watts, D. J. (2015). The structural virality of online diffusion. *Management Science*, 62(1):180–196.
- Goertzel, T. (1994). Belief in conspiracy theories. *Political Psychology*, pages 731–742.

- Goldberg, A. (2006). Reading and writing across the borders of dictatorship: Self-censorship and emigrant experience in nazi and stalinist europe. In *Letters across Borders*, pages 158–172. Springer.
- Goodnight, G. T. and Poulakos, J. (1981). Conspiracy rhetoric: From pragmatism to fantasy in public discourse. *Western Journal of Speech Communication*, 45(4):299–316.
- Guadagno, R. and Cialdini, R. (2005). Online persuasion and compliance: Social influence on the internet and beyond. *The social net: Human behavior in cyberspace*, pages 91–113.
- Gupta, A., Kumaraguru, P., Castillo, C., and Meier, P. (2014). Tweetcred: Real-time credibility assessment of content on twitter. In *International Conference on Social Informatics*, pages 228–243. Springer.
- Hermida, A. (2010). From tv to twitter: How ambient news became ambient journalism.
- Heylighen, F. (1998). What makes a meme successful? selection criteria for cultural evolution.
- Honda, I., Tanaka, T., Murata, T., Kayama, S., and Tamai, M. (1954). *Gojira*.
- Honey, M. (1985). *Creating Rosie the Riveter: class, gender, and propaganda during World War II*. Univ of Massachusetts Press.
- Howard, P. N. (2003). Digitizing the social contract: Producing american political culture in the age of new media. *The Communication Review*, 6(3):213–245.
- Howard, P. N., Bolsover, G., Kollanyi, B., Bradshaw, S., and Neudert, L.-M. (2017). Junk news and bots during the us election: What were michigan voters sharing over twitter. Technical report, Data Memo 2017.1. Oxford, UK: Project on Computational Propaganda. Retrieved from <http://comprop.ox.ac.uk/2017/03/26/junk-news-and-bots-during-the-uselection-what-were-michigan-voters-sharing-over-twitter>.
- Howard, P. N. and Kollanyi, B. (2016). Bots, #strongerin, and #brexit: Computational propaganda during the uk-eu referendum. *Browser Download This Paper*.

- Howard, P. N., Kollanyi, B., and Woolley, S. (2016). Bots and automation over twitter during the us election. *Computational Propaganda Project: Working Paper Series*.
- Hwang, T., Pearce, I., and Nanis, M. (2012). Socialbots: Voices from the fronts. *Interactions*, 19(2):38–45.
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10):94–100.
- Janowitz, M. (1975). Professional models in journalism: The gatekeeper and the advocate. *Journalism Quarterly*, 52(4):618–626.
- Jin, F., Dougherty, E., Saraf, P., Cao, Y., and Ramakrishnan, N. (2013). Epidemiological modeling of news and rumors on twitter. In *Proceedings of the 7th Workshop on Social Network Mining and Analysis*, page 8. ACM.
- Jowett, G. S. and O’donnell, V. (2014). *Propaganda & persuasion*. Sage.
- Kaid, L. L. and Johnston, A. (1991). Negative versus positive television advertising in us presidential campaigns, 1960–1988. *Journal of communication*, 41(3):53–64.
- Kalat, D. (2017). *A critical history and filmography of Tohos Godzilla series*. McFarland.
- Kang, H., Bae, K., Zhang, S., and Sundar, S. S. (2011). Source cues in online news: Is the proximate source more powerful than distal sources? *Journalism & Mass Communication Quarterly*, 88(4):719–736.
- Kata, A. (2012). Anti-vaccine activists, web 2.0, and the postmodern paradigm—an overview of tactics and tropes used online by the anti-vaccination movement. *Vaccine*, 30(25):3778–3789.
- Kelly, S., Truong, M., Shahbaz, A., Earp, M., and White, J. (2017). Freedom on the Net 2017. Technical report, Freedom House.
- Kharpal, A. (2017). Hundreds of twitter accounts including bieber and forbes hacked, calling germany, netherlands ’nazi’.

- King, G., Pan, J., and Roberts, M. E. (2013). How censorship in china allows government criticism but silences collective expression. *American Political Science Review*, 107(02):326–343.
- Kirchner, W. H. (1997). The evolution of communication. *Trends in Cognitive Sciences*, 1(9):353–353.
- Kosinski, M., Stillwell, D., and Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 110(15):5802–5805.
- Kramer, A. D., Guillory, J. E., and Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, 111(24):8788–8790.
- Krueger, B. S. (2006). A comparison of conventional and internet political mobilization. *American Politics Research*, 34(6):759–776.
- Kwak, H., Lee, C., Park, H., and Moon, S. (2010). What is Twitter, a social network or a news media? In *Proceedings of the 19th international conference on World wide web*, pages 591–600. ACM.
- Lauricella, T., Stewart, C. S., and Ovide, S. (2013). Twitter hoax sparks swift stock swoon. *The Wall Street Journal*, 23.
- Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., et al. (2018). The science of fake news. *Science*, 359(6380):1094–1096.
- Lee, K., Eoff, B. D., and Caverlee, J. (2011). Seven months with the devils: A long-term study of content polluters on twitter. In *Proc. 5th AAAI Intl. Conf. on Web and Social Media*.
- Li, J., Galley, M., Brockett, C., Spithourakis, G. P., Gao, J., and Dolan, B. (2016a). A persona-based neural conversation model. *arXiv preprint arXiv:1603.06155*.

- Li, J., Monroe, W., Ritter, A., Galley, M., Gao, J., and Jurafsky, D. (2016b). Deep reinforcement learning for dialogue generation. *arXiv preprint arXiv:1606.01541*.
- Linebarger, P. M. (2015). *Psychological warfare*. Pickle Partners Publishing.
- Lippmann, W. (2004). *Public opinion*. Courier Corporation.
- Liu, X., Nourbakhsh, A., Li, Q., Shah, S., Martin, R., and Duprey, J. (2017). Reuters tracer: Toward automated news production using large scale social media data. *arXiv preprint arXiv:1711.04068*.
- Magdy, W., Darwish, K., and Weber, I. (2015). # failedrevolutions: Using twitter to study the antecedents of isis support. *arXiv preprint arXiv:1503.02401*.
- Mahaney, D. C. (2002). Propaganda posters. *OA Magazine of History*, 16(3):41–46.
- McAllister, I. et al. (2007). The personalization of politics. *The Oxford handbook of political behavior*, pages 571–588.
- McCosker, A. (2014). Trolling as provocation youtubes agonistic publics. *Convergence: The International Journal of Research into New Media Technologies*, 20(2):201–217.
- McPherson, M., Smith-Lovin, L., and Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual review of sociology*, 27(1):415–444.
- Metaxas, P. and Mustafaraj, E. (2013). The rise and the fall of a citizen reporter. In *Proceedings of the 5th Annual ACM Web Science Conference*, pages 248–257. ACM.
- Metaxas, P. T., Finn, S., and Mustafaraj, E. (2015). Using twittertrails. com to investigate rumor propagation. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing*, pages 69–72. ACM.
- Metaxas, P. T. and Mustafaraj, E. (2012). Social media and the elections. *Science*, 338(6106):472–473.
- Miller, J. H. (1943). We can do it! [Online; accessed February 27, 2017].

- Mitter, S., Wagner, C., and Strohmaier, M. (2013). A categorization scheme for socialbot attacks in online social networks. In *Proc. of the 3rd ACM Web Science Conference*.
- Morris, M. and Ogan, C. (1996). The internet as mass medium. *Journal of Computer-Mediated Communication*, 1(4):0–0.
- Murphy, R. D. (2012). Tea party constitutionalism: does the astroturf have roots in the history of the constitution. *Hastings Const. LQ*, 40:187.
- Murray, C. (2000). *Popaganda: superhero comics and propaganda in World War Two*. Copenhagen: University of Copenhagen Press.
- Mustafaraj, E. and Metaxas, P. T. (2010). From obscurity to prominence in minutes: Political speech and real-time search. In *WebSci10: Extending the Frontiers of Society On-Line*, pages 317–323.
- Mustafaraj, E. and Metaxas, P. T. (2017). The fake news spreading plague: Was it preventable? *arXiv preprint arXiv:1703.06988*.
- Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of general psychology*, 2(2):175.
- Nyhan, B. and Reifler, J. (2015). The effect of fact-checking on elites: A field experiment on us state legislators. *American Journal of Political Science*, 59(3):628–640.
- Nyhan, B., Reifler, J., and Ubel, P. A. (2013). The hazards of correcting myths about health care reform. *Medical care*, 51(2):127–132.
- Orwell, G. (2009). *Nineteen eighty-four*. Everyman’s Library.
- Perrin, A. (2015). Social media usage. *Pew Research Center*.
- Phillips, W. and Milner, R. M. (2018). *The ambivalent internet: Mischief, oddity, and antagonism online*. John Wiley & Sons.

- Poulsen, K. (2014). How a math genius hacked okcupid to find true love.
- Qazvinian, V., Rosengren, E., Radev, D. R., and Mei, Q. (2011). Rumor has it: Identifying misinformation in microblogs. In *Proceedings of the Conference on Empirical Methods in Natural Language Processing*, pages 1589–1599. Association for Computational Linguistics.
- Qiu, X., Oliveira, D. F., Shirazi, A. S., Flammini, A., and Menczer, F. (2017). Limited individual attention and online virality of low-quality information. *Nature Human Behavior*, 1:0132.
- Ratkiewicz, J., Conover, M., Meiss, M., Goncalves, B., Flammini, A., and Menczer, F. (2011a). Detecting and tracking political abuse in social media. In *Proc. 5th Intl. AAAI Conf. on Weblogs and Social Media (ICWSM)*, pages 297–304.
- Ratkiewicz, J., Conover, M., Meiss, M., Gonçalves, B., Patil, S., Flammini, A., and Menczer, F. (2011b). Truthy: mapping the spread of astroturf in microblog streams. In *Proc. 20th Intl. ACM Conf. on World Wide Web (WWW)*, pages 249–252.
- Resnick, P., Carton, S., Park, S., Shen, Y., and Zeffer, N. (2014). Rumorlens: A system for analyzing the impact of rumors and corrections in social media. In *Proc. Computational Journalism Conference*.
- Resnik, F., Bellmore, A., Xu, J.-M., and Zhu, X. (2016). Celebrities emerge as advocates in tweets about bullying. *Translational Issues in Psychological Science*, 2(3):323.
- Rojecki, A. and Meraz, S. (2016). Rumors and factitious informational blends: The role of the web in speculative politics. *New Media & Society*, 18(1):25–43.
- Shannon, C. E. (1949). Communication in the presence of noise. *Proceedings of the IRE*, 37(1):10–21.
- Shao, C., Ciampaglia, G. L., Flammini, A., and Menczer, F. (2016). Hoaxy: A platform for tracking online misinformation. In *Proceedings of the 25th International Conference Companion on World Wide Web*, pages 745–750. International World Wide Web Conferences Steering Committee.

- Shao, C., Ciampaglia, G. L., Varol, O., Flammini, A., and Menczer, F. (2017). The spread of fake news by social bots. *arXiv preprint arXiv:1707.07592*.
- Shao, C., Hui, P.-M., Wang, L., Jiang, X., Flammini, A., Menczer, F., and Ciampaglia, G. L. (2018). Anatomy of an online misinformation network. *arXiv preprint arXiv:1801.06122*.
- Shover, M. J. (1975). Roles and images of women in world war i propaganda. *Politics & Society*, 5(4):469–486.
- Simon, D. M. and Ostrom, C. W. (1989). The impact of televised speeches and foreign travel on presidential approval. *Public Opinion Quarterly*, 53(1):58–82.
- Simon, H. A. (1971). Designing organizations for an information-rich world.
- Skyrms, B. (2010). *Signals: Evolution, learning, and information*. Oxford University Press.
- Sordoni, A., Galley, M., Auli, M., Brockett, C., Ji, Y., Mitchell, M., Nie, J.-Y., Gao, J., and Dolan, B. (2015). A neural network approach to context-sensitive generation of conversational responses. *arXiv preprint arXiv:1506.06714*.
- Suárez-Serrato, P., Roberts, M. E., Davis, C., and Menczer, F. (2016). On the influence of social bots in online protests. In *International Conference on Social Informatics*, pages 269–278. Springer.
- Subrahmanian, V., Azaria, A., Durst, S., Kagan, V., Galstyan, A., Lerman, K., Zhu, L., Ferrara, E., Flammini, A., Menczer, F., Waltzman, R., Stevens, A., Dekhtyar, A., Gao, S., Hogg, T., Kooti, F., Liu, Y., Varol, O., Shiralkar, P., Vydiswaran, V., Mei, Q., and Huang, T. (2016). The darpa twitter bot challenge. *Computer*, 49(6):38–46.
- Sullivan, J. (2012). A tale of two microblogs in china. *Media, Culture & Society*, 34(6):773–783.
- Sunstein, C. R. and Vermeule, A. (2009). Conspiracy theories: Causes and cures. *Journal of Political Philosophy*, 17(2):202–227.
- Tan, C., Lee, L., and Pang, B. (2014). The effect of wording on message propagation: Topic-and author-controlled natural experiments on twitter. *arXiv preprint arXiv:1405.1438*.

- Tanash, R. S., Chen, Z., Thakur, T., Wallach, D. S., and Subramanian, D. (2015). Known unknowns: An analysis of twitter censorship in turkey. In *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, pages 11–20. ACM.
- Varol, O. (2016). Spatiotemporal analysis of censored content on twitter. In *Proceedings of the 8th ACM Conference on Web Science*, pages 372–373. ACM.
- Varol, O., Ferrara, E., Davis, C., Menczer, F., and Flammini, A. (2017a). Online human-bot interactions: Detection, estimation, and characterization. In *ICWSM*. ACM.
- Varol, O., Ferrara, E., Menczer, F., and Flammini, A. (2017b). Early detection of promoted campaigns on social media. *EPJ Data Science*, 6(1):13.
- Verkamp, J.-P. and Gupta, M. (2012). Inferring mechanics of web censorship around the world. In *FOCI*.
- Vespignani, A. (2009). Predicting the behavior of techno-social systems. *Science*, 325(5939):425.
- Vuori, J. A. and Paltemaa, L. (2015). The lexicon of fear: Chinese internet control practice in sina weibo microblog censorship. *Surveillance & Society*, 13(3/4):400–421.
- Wagner, C., Mitter, S., Körner, C., and Strohmaier, M. (2012). When social bots attack: Modeling susceptibility of users in online social networks. In *Proceedings of the 21th International Conference on World Wide Web*, pages 41–48.
- West, D. M. (2017). *Air Wars: Television Advertising and Social Media in Election Campaigns, 1952-2016*. CQ Press.
- Wiley, R. H. (1983). The evolution of communication: information and manipulation. *Animal behaviour*, 2:156–189.
- Wood, W. (2000). Attitude change: Persuasion and social influence. *Annual review of psychology*, 51(1):539–570.

- Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday*, 21(4).
- Wrocawia, W. (1981). Wieczr wrocawia. [Online; accessed May 8, 2017].
- Wu, Y., Agarwal, P. K., Li, C., Yang, J., and Yu, C. (2014). Toward computational fact-checking. *Proceedings of the VLDB Endowment*, 7(7):589–600.
- Young, K. K. and Nathanson, P. (2010). *Sanctifying misandry: Goddess ideology and the fall of man*. McGill-Queen’s Press-MQUP.
- Zhang, L. L. (2006). Behind the great firewall decoding china’s internet media policies from the inside. *Convergence: The International Journal of Research into New Media Technologies*, 12(3):271–291.
- Zhu, T., Phipps, D., Pridgen, A., Crandall, J. R., and Wallach, D. S. (2012). Tracking and quantifying censorship on a chinese microblogging site. *arXiv preprint arXiv:1211.6166*.
- Zhu, T., Phipps, D., Pridgen, A., Crandall, J. R., and Wallach, D. S. (2013). The velocity of censorship: High-fidelity detection of microblog post deletions. *arXiv preprint arXiv:1303.0597*.