Disinformation, **'Fake News'** and Influence Campaigns on **Twitter**

OCTOBER 2018

KNIGHT FOUNDATION

Matthew Hindman
George Washington University

Vlad Barash
Graphika

Contents

EXECUTIVE SUMMARY

This study is one of the largest analyses to date on how fake news spread on Twitter both during and after the 2016 election campaign.

Using tools and mapping methods from Graphika, a social media intelligence firm, we study more than 10 million tweets from 700,000 Twitter accounts that linked to more than 600 fake and conspiracy news outlets. Crucially, we study fake and conspiracy news both before and after the election, allowing us to measure how the fake news ecosystem has evolved since November 2016.

Much fake news and disinformation is still being spread on Twitter.

Consistent with other research, we find more than 6.6 million tweets linking to fake and conspiracy news publishers in the month before the 2016 election. Yet disinformation continues to be a substantial problem postelection, with 4.0 million tweets linking to fake and conspiracy news publishers found in a 30-day period from mid-March to mid-April 2017. Contrary to claims that fake news is a game of "whack-a-mole," more than 80 percent of the disinformation accounts in our election maps are still active as this report goes to press. These accounts continue to publish more than a million tweets in a typical day.

Just a few fake and conspiracy outlets dominated during the election—and nearly all of them continue to dominate today.

Sixty-five percent of fake and conspiracy news links during the election period went to just the 10 largest sites, a statistic unchanged six months later. The top 50 fake news sites received 89 percent of links during the election and (coincidentally) 89 percent in the 30-day period five months later. Critically—and contrary to some previous reports—these top fake and conspiracy news outlets on Twitter are largely stable. Nine of the top 10 fake news sites during the month before the election were still in or near the top 10 six months later.

Our methods find much more fake and conspiracy news activity on Twitter than several recent high-profile studies—though fake news still receives significantly fewer links than mainstream media sources.

Our study finds much more fake news activity than several recent studies, largely because it examines a larger corpus of fake and conspiracy news sites. Fake and conspiracy news sites received about 13 percent as many Twitter links as a comparison set of national news outlets did, and 37 percent as many as a set of regional newspapers.

Most accounts spreading fake or conspiracy news in our maps are estimated to be bots or semi-automated accounts.

Machine learning models estimate that 33 percent of the 100 most-followed accounts in our postelection map—and 63 percent of a random sample of all accounts—are "bots," or automated accounts. Because roughly 15 percent of accounts in the postelection map have since been suspended, the true proportion of automated accounts may have exceeded 70 percent.

Our maps show that accounts that spread fake news are extremely densely connected.

In both the election-eve and postelection maps, our methods identify an ultra-dense core of heavily followed accounts that repeatedly link to fake or conspiracy news sites. Sites in the core are typically *not* the highest-volume tweeters of fake news. However, the popularity of these accounts, and heavy co-followership among top accounts, means that fake news stories that reach the core (or start there) are likely to spread widely. The pre-election fake news network is one of the densest Graphika has ever analyzed, necessitating unusual map drawing procedures.

Fake news during the election did not just adopt conservative or Republican-leaning frames—though it has become more ostensibly Republican since.

While a large majority of fake news came from supposedly pro-Republican and pro-Donald Trump accounts in the month before the election, smaller but still substantial amounts of fake news were passed on by liberal or Democratic-identified accounts. After the election period, though, left-leaning fake news decreased much more than right-leaning fake news.

There are structural changes in the role of Russian-aligned clusters of accounts postelection.

In the pre-election map, clusters of accounts affiliated with Russia serve a brokerage role, serving as a cultural and political bridge between liberal U.S. accounts and European far-right accounts. Postelection, however, accounts in the Russia cluster have become more peripheral, while the International Conspiracy | Activist cluster (which similarly spreads pro-Russia content) is spread broadly through the map. This structure suggests that international conspiracy-focused accounts have become more important as brokers of fake news postelection.

Most of the accounts that linked repeatedly to fake and conspiracy news during the election are still active.

Twitter has claimed repeatedly that it has cracked down on automated accounts that spread fake news and engage in "spammy behavior." Yet of the 100 accounts that were most active in spreading fake news in the months before the election—the large majority clearly engaged in "spammy behavior" that violates Twitter's rules—more than 90 were still active as of spring 2018. Overall, 89 percent of accounts in our fake and conspiracy news map remained active as of mid-April 2018. The persistence of so many easily identified abusive accounts is difficult to square with any effective crackdown.

A few dozen accounts controlled by Russia's Internet Research Agency appear in our maps—but hundreds of other accounts were likely more important in spreading fake news.

Of the more than 2,700 IRA accounts named publicly as of this writing, 65 are included in at least one of our maps. The IRA accounts in our maps include several accounts that were widely quoted in U.S. media, such as @WarfareWW, @TEN_GOP and @Jenn_Abrams. Most of the publicly known IRA accounts are filtered from our map because of relatively few followers and little measurable influence. Plenty of other accounts, though, do tweet in lockstep with the Kremlin's message, including hundreds of accounts with more followers than top IRA trolls.

There is evidence of coordinated campaigns to push fake news stories and other types of disinformation.

Most news stories on Twitter follow a statistically regular pattern: The rate of new links ramps up quickly (but not instantly), peaks in an hour or two, and then decays in an exponential, statistically regular fashion. But many fake news stories do not follow this nearly universal pattern. Organized blocks of accounts appear to coordinate to extend the life cycle of selected news stories and hashtags. Segments of our maps associated with Russian propaganda are key participants in these campaigns, and many of these efforts align strongly with Russian goals and interests.

Coordinated campaigns seem to opportunistically amplify content they did not create.

Public discussion has often vacillated between portraying fake news as an organic, small-scale phenomenon driven by ad dollars, and characterizing it as the product of massive coordinated efforts by state actors. Our data tell a more complicated story, in which some narratives are carefully crafted, but others are amplified because they fit with the agenda of those running these campaigns. This is the information warfare equivalent of giving air cover to a rebel group, using outside technology and resources to augment otherwise-weak organic efforts.

One case study suggests that concerted action against noncredible outlets can drastically reduce their audience.

The Real Strategy was referenced by more than 700,000 tweets in our election sample, the second-most linked fake or conspiracy news outlet overall. After being tied to a large-scale harassment campaign and the "Pizzagate" falsehood, though, The Real Strategy's Twitter account was deleted, it was blacklisted on online forums such as Reddit, and a network of supportive bot accounts was partially disrupted. The postelection sample showed only 1,534 tweets to The Real Strategy, a drop of 99.8 percent. This example suggests that aggressive action against fake news outlets can be effective at containing the spread of fake news.

INTRODUCTION

One of the most remarkable outcomes of the 2016 presidential election cycle in the United States was the rise of so-called fake news. Before 2016, the term fake news referred mostly to satirical media such as "The Daily Show" or The Onion.[1] During the 2016 campaign, though, the label was repurposed to describe a rapidly growing category of digital content: fabricated articles spreading falsehoods that nonetheless appeared to be credible news stories. Hundreds of websites that publish such content have sprung up in recent years, and false stories have spread quickly and widely through social media. False news stories claiming that Hillary Clinton ordered the murder of an FBI agent, or participated in a satanic child abuse ring in a Washington pizza parlor, were shared hundreds of thousands of times on social media on the eve of the 2016 election.[2]

Fake news is now an important part of the political ecosystem—though the term itself has become hotly contested. Understanding the fake news phenomenon both during and after the election is a critically important task for journalists, policymakers, national security professionals, and citizens of all political stripes. Despite the importance of this question, though, public debates and journalistic accounts have often been clouded by conflicting claims and narratives.

Early journalistic accounts of fake news emphasized the role of amateurs and small-scale entrepreneurs motivated by ad dollars. In an indelible early story about fake news, BuzzFeed reporters Craig Silverman and Lawrence Alexander tracked down groups of teenagers in the Macedonian town of Veles who had created dozens of ad-supported fake news sites to earn spending money.[3] Numerous similar reports followed, tracing specific fake news stories to an entrepreneur in the California suburbs,[4] a college-age intern for a Maryland state legislator,[5] computer science students in the country of Georgia,[6] and other ragtag groups of digital creators motivated by politics or cash. Recent reports have suggested that at least one of the Macedonian sites was actually run by the Israeli private intelligence firm Psy-Group as part of a concerted pro-Trump effort.[7] Yet much public discussion still assumes that most fake news is small-scale and money-oriented.

Focusing on a few fake and conspiracy news outlets and a few widely shared stories, though, runs the risk of distorting our understanding of fake news overall. More systematic studies of fake news have painted a very different picture from most early news reports. Rather than a profusion of small, independent news sites, large-scale empirical studies have found that the fake news "ecosystem" is highly concentrated. In a research paper produced by a Harvard and Northeastern university conference, David Lazer and collaborators conclude that most fake news on social media could be traced to a "relatively small, but constantly changing, number of sources."[8] Other large-scale reports looking at fake news as one element in the broader digital media environment have similarly found strong concentration.[9]

Even more ominously, we now know that the Russian government engaged in a large-scale, multipronged effort to influence the 2016 U.S. election. Many important details of this effort are still unknown to the public as of this writing. We do know, though, that these efforts included crafting and promoting fake news stories with tens of thousands of social media accounts,[10] more than 1,000 trained professional "trolls,"[11] and hundreds of thousands of dollars of digital ads seen by millions of Americans.[12] Social media accounts that spread fake news also promoted real-world meetups and demonstrations in U.S. cities—sometimes on both sides of hot-button issues.[13] Understanding the details of these state-sponsored tactics, and their likely effectiveness, is key to mitigating the influence of anti-democratic efforts in the future.

THIS REPORT SHEDS LIGHT ON A NUMBER OF KEY QUESTIONS ABOUT FAKE NEWS:

First, it attempts to benchmark the scale of the phenomenon at the national level. How much fake news content can be found on Twitter? From how many outlets? How does the volume of fake news content compare with that of more credible news sources?

Second, this report seeks to understand how the phenomenon has evolved since the 2016 election. Elections are unusually high-profile times for political activity, and previous work has suggested that the list of prominent fake news sites changes frequently.[14] How much has the fake news landscape changed since the end of the 2016 election? Has the volume of fake news dropped? Do we see the emergence of important new players?

Third, we look at the role of coordinated propaganda and automated accounts in the spread of fake news. How big a part have automated accounts played in pushing fake news—and how has this changed since the election? Can we find evidence of coordinated campaigns (automated or not) pushing particular stories or agendas in ways unlikely to be organic?

A PROBLEM BOTH OLD AND NEW

To set the stage for the study, it is worth reviewing several areas of research that provide context for the study of disinformation in general and fake news in particular. One key piece of context is historical. Media and scholarly accounts have often emphasized the ways in which the fake news phenomenon is unprecedented. Yet the 2016 election is hardly the first time that false news stories, motivated by money or national ideology, have been aimed at the American public.

False news stories spread by The Associated Press helped lead to the inauguration of Rutherford B. Hayes as president and the end of post-Civil War Reconstruction. Most Americans are familiar with "yellow journalism," sensational coverage that sold newspapers at the expense of factual accuracy at the turn of the 20th century. Yellow journalism strongly contributed to the start of the Spanish-American War and (arguably) the U.S. entry into World War I.[15]

Perhaps the most remarkable incident of fake news in American history—and far less known—was the massive, covert British propaganda effort to draw the U.S. into World War II. Run out of an office in Rockefeller Center in New York City, so-called British Security Coordination (BSC) involved as many as 3,000 British agents who manipulated U.S. news coverage on a massive scale.[16] The effort paid friendly columnists and laundered (sometimes fake) British news stories through apparently unconnected outlets. The BSC campaign even developed the "game of Vik," a large-scale campaign to anonymously harass Nazi sympathizers in the United States through tactics such as popping tires and putting rats in water tanks. Today we would call these types of acts trolling.

During the Cold War, of course, the Soviet Union often targeted American audiences with false news stories. Declassified Russian documents show that by the early 1980s, the Soviets were spending more than $3 billion on external propaganda and influence campaigns, more than the U.S. was then spending on the National Security Agency.[17] Soviet

efforts routinely involved publishing fake news, including recruiting journalists as agents and publishing fabricated documents (often in troves of "leaked" genuine material).

Fake news, then, is not unprecedented. Yet as the media environment and the political landscape have shifted, possibilities for fake news have mutated and metastasized. Aggregators and "content farms" have sprung up to produce low-quality, sensational, often misleading news stories framed to maximize clicks. New audience metrics and tools such as A/B testing may have encouraged a shift to sensational content. Changes in the media landscape coincided with broader polarization in the American public, with partisans showing increasing disdain for members of the other party.[18]

Social media is now the most important conduit of digital news, especially for many low-information voters.[19] A substantial and controversial literature has worried about online "echo chambers" or "filter bubbles," in which individuals receive few political messages that contradict their prejudices, because of news self-selection, social homophily, or algorithms on big platforms such as Facebook.[20] While several lines of empirical studies have complicated or directly challenged claims about strong filter bubbles, some research suggests that one-sided information flows produce bigger shifts in public opinion than balanced information flows.[21] These lines of research have potentially important implications for our understanding of the impact of fake news on political attitudes and behavior.

Partly in response to the digitization of the information landscape, there has been a wave of scholarship on how to correct misinformation. Much of this literature, unfortunately, has argued that false beliefs are often resistant to correction. Repeating false stories, even to debunk them immediately, might reinforce misperceptions (though scholarship on this point is conflicted).[22] Even when members of the public do accept corrections, the initial false story can continue to affect attitudes.[23]

Research on misinformation has also emphasized the power of "social proof" in persuading the public to accept false information. People may be more apt to accept news stories as true when they come from friends and acquaintances and supposedly credible sources, and when these stories are more popular overall.[24] Recent work has also found that repetition alone can make false news stories more believable.[25] People are more accepting of the story the third or fourth time they are exposed to it, with familiarity increasing credibility.

NATION-STATES, INFORMATION WARFARE AND 'CYBER TROOPS'

The arrival of social media has inaugurated a new era of news manipulation for profit and political advantage, and many nations routinely try to influence news and discussion on social media platforms. Many observers have especially noted the evolution of Russian information warfare doctrine, along with its "deep roots in long-standing Soviet practice."[26]

Many articles discuss this—somewhat inaccurately[27]—as a so-called Gerasimov Doctrine, with reference to the writings of Russian General of the Armies Valery Gerasimov. Though it is not systematic enough to count as a bona fide doctrine, it is true that Russian military thinking emphasizes hybrid warfare as a new persistent reality, with the "information sphere" and information warfare a critical battlespace.[28] There is evidence that the Russian government's redoubled efforts have been strategically important: For example, areas of Ukraine that receive Kremlin-supported broadcasts have shown sharp pro-Russian shifts in attitude.[29]

Russia promotes false and contradictory stories from outlets across the political spectrum, with the aim of creating confusion and widening political and social divides.

Even before the 2016 election, observers in Europe and the United States alleged that Russian efforts produced a "firehose of falsehood," defined by "high numbers of channels and messages and a shameless willingness to disseminate partial truths or outright fictions."[30] According to these accounts, Russia promotes false and contradictory stories from outlets across the political spectrum, with the aim of creating confusion and widening political and social divides. Consistent with these claims, many of the political ads bought by the Russian-government-linked Internet Research Agency focused on amplifying U.S. social tensions on topics such as race, guns and homosexuality.[31] Indeed, research by Stewart, Arif and Starbird found that IRA accounts were active on both sides of pre-election debates about race and guns, in an apparent attempt to inflame opinion.[32] Another large-scale analysis of IRA tweets found several different types of accounts playing consistent roles, including trolls on both the political left and right, and IRA accounts pretending to be local news outlets.[33]

While much attention has focused on the role of Russia, many other nations and organizations now attempt to shape digital news and social media in favorable directions. Recent work by Bradshaw and Howard at the Oxford Internet Institute has noted the emergence of "cyber troops"—organized teams trying to shape public opinion on social media—in more than two dozen countries.[34] Recent media reports have also raised questions about pro-Trump campaigns run by other foreign groups, including the Israeli private intelligence firm Psy-Group.[35] Iranian fake accounts and sites, along with new Russian sites, have been removed in the runup to the 2018 election.[36]

While much attention has focused on the role of Russia, many other nations and organizations now attempt to shape digital news and social media in favorable directions.

If such tactics are being used on Twitter, by state actors or others, they should be visible in our study. First, we should see stories on favored topics being shared unusually widely, even across ideological groups and geographic units that rarely share news. Second, the chronological pattern of sharing should show evidence of coordination. Most news stories spike quickly and then decay rapidly in a roughly exponential fashion. Strong deviation from that pattern is prima facie evidence of coordinated behavior.[37]

DEFINING FAKE NEWS OUTLETS

Discussing fake news, of course, requires a clear definition of the kind of content we are studying. Following previous scholarship,[38] we define fake news as content that has the appearance of credible news stories, but without going through the process of verification that makes real news valuable. Fake news is fraudulent not just because it is factually false (though of course it usually is), but because it skips the procedures that make real news trustworthy.

Nearly all fake news content also counts as ***disinformation***—a broader category that includes *content (news content or otherwise) created or spread with intent to deceive*. For the outlets that create it, and the automated accounts that often coordinate to spread it, the intent to deceive is clear. But from the perspective of citizens, fake news may also count as ***misinformation***: *false content spread by those who may mistakenly believe it to be true*.

Many political partisans, up to and including heads of state, now routinely use the "fake news" label to disparage articles they disagree with. Some scholars and journalists have recently argued that the term has been so abused that it should be retired.[39] Yet this report continues to use it for several reasons. Disinformation takes far more forms than just fake news—and this important genre of disinformation has no other widely accepted label. Moreover, as other scholars have noted, relabeling fake news is likely to just provoke similar abuse of whatever new term is chosen.[40]

This report goes beyond individual fake news stories to focus on ***fake news outlets***—*sites that regularly publish content that appears to have been rigorously verified, but in fact was not.* In the most clear-cut cases, fake news outlets are designed to look like (nonexistent) traditional media outlets, but any sites that regularly publish content without a genuine verification process count as fake news under our definition.

In the context of state-sponsored disinformation campaigns, conspiracy-focused outlets have long been both more common and more effective than sites that publish only false content (see previous discussion). Conspiracy sites count as fake news outlets under our definition and that of most (though not all) other scholars. For clarity, though, this report often uses the term ***fake and conspiracy news*** to better align with common usage. Some recent scholarly discussions of fake news have excluded outlets such as Sputnik News, Infowars and Zero Hedge from their analysis, to focus on sites that overwhelmingly publish false articles. Our strong view is that such ultra-narrow definitions of fake news outlets are a mistake, overlooking the most important vectors for damaging disinformation. This is doubly true with respect to questions about state-sponsored disinformation, which for decades has been laundered through conspiracy outlets of various kinds.

At the same time, our focus on fake and conspiracy news is narrower than that used in some other recent scholarship.[41] Outlets that are just politically biased or ideologically extreme *do not* qualify as fake news by our measure, even if those sites incline toward sensationalism. We are concerned with factual accuracy, not with issues of framing or tone. And while hypothetical hard cases are easy to construct, they are largely absent from the real data (more on this below). The core findings of this report are thus likely to hold no matter which scholarly definition of fake news one prefers.[42]

In the 2016 election period, our sampled data include 381,369 unique news story URLs on fake and conspiracy news sites.

There are several reasons, contrary to many previous studies of fake news, that we focus on the outlet rather than individual articles. One issue is the sheer scope of the fake news phenomenon. In the 2016 election period, our sampled data include 381,369 unique news story URLs on fake and conspiracy news sites. This report, or any similar report, cannot evaluate the truthfulness of every single story in such a massive corpus.

In addition to practical limitations, there are other compelling reasons to look at outlets rather than individual stories.[43] On its own, a single story is a poor guide to the overall credibility of an outlet. Diligent newsrooms occasionally have to correct articles after getting facts wrong, of course. But even propaganda outlets explicitly designed to deceive often publish more true stories than fabrications. For example, Russian doctrine on disinformation has long emphasized that disinformation should be accompanied by reams of truthful information to make the deception more convincing.[44] We see plenty of outlets in our data that follow this model, filling out their newsfeeds with both a steady stream of fake stories and even more straight news articles (though usually with a sensational headline). Fake Twitter accounts reportedly linked to Russian government efforts, such as the @TEN_GOP account discussed above, have pursued a similar strategy: lots of unremarkable pro-Trump and pro-GOP content with a regular drip of fake news and curiously pro-Kremlin stories. Internet Research Agency accounts that cast themselves (falsely) as local news sites followed the same pattern, with only a small fraction of their content patently false.[45]

Even propaganda outlets explicitly designed to deceive often publish more true stories than fabrications.

Focusing on fake news at the outlet level is especially important, too, for understanding a key question of interest: how fake news sites grow and maintain audience over time. Factually true stories can build trust in otherwise questionable brands and make subsequent mis- or disinformation more likely to be accepted. Just like fake stories, factually true stories on noncredible outlets are an important part of understanding the character of the fake news problem.

BOTS, TROLLS AND 'CYBORGS' ON TWITTER

So-called bots—automated accounts—are believed to play a key role in the spread of fake news and disinformation. These worries have been especially prominent in investigations into Russian attempts to influence the 2016 election. Bots are distinct from professional trolls, which are human-run accounts that usually seek to provoke or to spread disinformation. "Cyborg" accounts combine human-generated content with automated posting.[46]

An explosion of academic research has documented large networks of false accounts that seek to spread disinformation on social media.[47] Social media companies, too, have confirmed that fake accounts and networks of bots played a central role in promoting fake news. Facebook implicitly confirmed the main conclusions of the U.S. intelligence community about both automated accounts and coordinated fake news campaigns by state actors in a public April 2017 report, but cut information on Russia's role from the report after an internal debate.[48] In October 2017, Facebook disclosed that content from accounts linked to Russia had reached more than 126 million users.[49]

In October 2017, Facebook disclosed that content from accounts linked to Russia had reached more than 126 million users.

Twitter reported that it had identified 36,746 accounts—a figure later upped to more than 50,000—that "generated automated, election-related content and had at least one of the characteristics we used to associate an account with Russia."[50] In addition to automated accounts, Twitter ultimately identified 3,817 accounts linked to the Internet Research Agency, the so-called troll farm with links to the Kremlin. Twitter was criticized, however, for focusing its efforts to find automated accounts just on the profiles Facebook had already identified, rather than on its own platform-specific signals.[51]

Automated accounts are explicitly allowed according to Twitter's terms of use, and the platform's open API makes creating them relatively simple. Many Twitter bots or automated accounts are clearly labeled as such, and many serve useful functions. Some sophisticated bots, though, can convincingly mirror human behavior, especially when combined with occasional human intervention.

Still, given the potential importance of automated accounts in the spread of fake news, it is important to note patterns that suggest automated behavior. None of these signs "prove" that a given account is really a bot. But there are many different predictors that, in combination, provide strong evidence that an account is automated. Common signs include—but are not limited to—the following:

- Very high posting rate, round-the-clock posts with no time for sleep, or posts at highly regular intervals.
- Accounts that overwhelmingly just retweet or "like" content, or which have very high retweet-to-original-tweet ratios. This is especially suspicious if only a few sources or accounts are retweeted.
- Multiple tweets of the same link, something human accounts rarely do.
- Accounts with little or no verifiable biographical information.
- Accounts using fake profile pictures.[52]
- Accounts with many thousands of tweets yet few followers. Human users rarely continue to use Twitter heavily if they are mostly ignored.
- High but nearly equal following/follower ratios. This often results from exploiting automatic re-follow behavior to pad numbers of followers, or from accounts in a botnet following each other.
- Very short replies when accounts *are* engaged by others, or replies with grammatical errors unlikely to have been made by native speakers. Shorter replies can hide lack of English language skills, and they can be easier to automate without raising suspicion.

No single feature is a perfect predictor, and bot prediction is probabilistic rather than exact. Detecting fake accounts has also become an arms race, as bot creators devise increasingly sophisticated bots as older versions are discovered. New research, though, has been much more successful at identifying newer types of "social bots" that can often fool human observers.[53]

In addition to qualitative indicators of automated activity, we also used the Tweetbotornot package, developed by University of Missouri professor Mike Kearney.[54] The core package uses gradient boosted machine learning models to provide a probabilistic guess of the likelihood that a given user is a bot: "The default [gradient boosted] model uses both users-level (bio, location, number of followers and friends, etc.) and tweets-level (number of hashtags, mentions, capital letters, etc. in a user's most recent 100 tweets) data." Kearney reports 93 percent accuracy in validation tests.

We can also look for evidence of coordinated activity *across* seemingly disconnected accounts.[55] Automated accounts are not strictly necessary for coordinated campaigns, especially for well-resourced actors (especially governments) who can hire hundreds or thousands of real people. In practice, though, automated accounts are widely used to achieve the scale necessary for success. Coordinated campaigns attempt to push a single story or hashtag, often across groups of accounts with little in common. As we shall see, similar patterns emerge in specific cases in our data.

A recent Pew Research Center report estimated that bots created two-thirds of Twitter links to popular sites.

Recent public research using similar bot classification methods has found that bots are responsible for a large portion of link sharing on Twitter. A recent Pew Research Center report estimated that bots created two-thirds of Twitter links to popular sites.[56] Similarly, in looking at Twitter misinformation during the election period, Shao et al. find that the dense core of misinformation accounts is dominated by social bots.[57] We therefore expect bots and heavily automated accounts to play a key role in our maps of disinformation accounts.

MAP METHODOLOGY

Graphika's key unit of analysis is a map, which catalogs a collection of key social media accounts around a particular topic. A map shows how social media accounts are connected to each other through social relationships embedded in the platform—in the case of Twitter, through patterns of followership. This section walks through the process by which these maps are constructed and the insights they can provide on a given topic.

SEED SET

To find a community of sites that tweet or retweet links to fake news articles, we need to start with a "seed set"—defined in this case by a group of sites that publish fake news. These sites will be the start of our analysis, and we will look for Twitter accounts that link to those fake news outlets. Seed sets need to be *representative* but not necessarily *comprehensive*: Additional fake news outlets can be discovered even if not included in the initial seed set, so long as they are linked to by similar user accounts.

Our goal in constructing the seed set is twofold. First, we strive to be conservative in what counts as "fake news," focusing just on sites that regularly publish unverified stories or flat-out falsehoods. Second, despite these constraints, we wanted to cast as wide a net as possible, collecting data on a broader set of fake news outlets than previous studies.

After discussions with other researchers and a review of previous work, we decided to use a list of news sites maintained by OpenSources (opensources.co). OpenSources describes itself as "a curated resource for assessing online information sources" and includes a large-scale, open-source, human-coded list of both credible and noncredible sources. Our seed set includes outlets that OpenSources lists as "fake" or "conspiracy." Conspiracy sites include many outlets associated with false news stories, such as prominent category member Infowars. Sites may be included in more than one category in the OpenSources data set.

In practice, outlets that OpenSources labels as fake or conspiracy sites are a superset of other public listings of fake news sites. A site listed as fake or conspiracy news in the OpenSources database is nearly always categorized that way in other public lists. Moreover, when comparing various lists of sites judged to be fake news by reputable organizations, there was little disagreement on the sites that multiple entities had investigated.

Sites included in at least one of those two categories (fake news or conspiracy news) produced a seed set of more than 600 outlets. Although the researchers did not classify these outlets themselves, they did undertake efforts to check that the OpenSources list was consistent with the stated claims. As a verification check, 1,000 URLs linking to our seed set of fake news sites were sampled at random from the Twitter database. Sites were considered correctly classified if (1) the story linked was substantially false or (2) the front page of the website when viewed in mid-April 2017 contained at least one false story. This initial check found one site incorrectly classified, a conservative-leaning but credible D.C.-based print publication that was wrongly placed in the conspiracy category. Upon rechecking the OpenSources listing, we found this apparent mistake had already been corrected. A second, 2,000-URL random sample of links to the seed set was conducted with the slightly revised OpenSources list. In this case, no misclassified outlets were discovered.

MAP LAYOUT AND COLORING

Graphika's map-drawing process is roughly 95 percent automated. After data are collected and the least-connected accounts are filtered out, maps are drawn using the Fruchterman-Reingold visualization algorithm.[58] Accounts are placed on the map according to a tug of war between competing forces. All accounts have a centrifugal force trying to push them to the edge of the map. In addition, accounts that follow similar sets of sites are attracted to each other, and they resist the force pushing them toward the edge. This algorithm means that closely interlinked groups with many co-followers end up forming clusters. The closer two sites are on the map, the more "friends" they share on average. Note that the visual clusters produced by the layout algorithm and the segments generated by Graphika's clustering engine are not identical: Though the two frequently overlap, some segments (such as the *International Conspiracy | Activist* cluster in the postelection map) are spread throughout the map.

Algorithms also determine the size and color of the shapes used to represent each Twitter account. The size of each shape is proportional to the logarithm of the number of followers each account has.

GROUPS AND SEGMENTS

Accounts only loosely connected to the network are filtered out using K-core decomposition, leaving just those with multiple links to other accounts.[59] Remaining accounts are then divided first into *groups* and then into *segments*, which are subgroups of sites under the umbrella of the larger group. Segments are collections of accounts that share particular interests, which means that they follow overlapping sets of accounts. The group and segment classification method is a variant of hierarchical agglomerative clustering.[60] HAC is a "bottom-up" method that starts by considering each account as a singleton, and then progressively grouping sites into bigger and bigger clusters based on the similarity of the accounts they follow.

Once groups and segments are generated, supervised machine learning techniques label each set of accounts based on human-categorized examples. After the automated process is finished, a human subject matter expert performs a quality assurance check on the segment and group labels.

In Graphika Twitter maps, accounts are colored based on the group and segment they cluster with. Accounts in each segment are assigned the same color, with different segments in the same overarching group sharing a color palette—for example, different shades of pink.

MEASURING INFLUENTIAL ACCOUNTS AND SUBJECTS OF INTEREST

Categorizing sites into groups and segments also allows for deeper analysis, allowing us to find words, phrases, websites and accounts especially favored by each subgroup compared with other subgroups.[61] Each segment and group thus has an associated collection of *Influencers, Conversation Leaders, Websites* and *Terms*. Influencers and Conversation Leaders represent the accounts that most strongly shape group and segment discussion. Influencers are users especially likely to be *followed* by accounts in that segment, and Conversation Leaders are users preferentially *mentioned* by accounts in that segment. Websites are URLs preferentially linked to by users in that segment, and Terms are keywords preferentially used in tweets from that segment.

We measure these group and segment preferences with *CFI scores* and *M-scores*. CFI scores describe how "focused" the segment or group is on the object: Higher scores mean bigger gaps between a given group (or segment) and the baseline patterns seen in other groups.[62] M-scores combine CFI with raw counts of interactions by segment members.

ELECTION DATA AND MAPS

With the seed set chosen, data were collected from Twitter. We began by gathering data on all tweets that referenced our list of fake news sites in the 30 days before the 2016 election.

All told, we found 6,610,875 tweets or retweets that linked to one of our 600-plus fake or conspiracy websites during the month before the election. These 6.6 million sampled tweets and retweets came from 454,832 separate accounts, an exceptionally broad swath of Twitter. At total of 73,296 accounts tweeted links to one or more of these sites at least 10 times over the 30-day election period.

Despite the enormous number of tweets referencing fake news sites, a few heavily (re)tweeted outlets dominated. During the election period, the top 10 sites accounted for 65 percent of all tweets of fake news links, while the 50 most linked fake news sites accounted for 89 percent of tweets pointing to fake news. These figures are substantially different from the picture of fake news that dominated early media reports, which repeatedly portrayed fake news production as organic, spontaneous and small-scale.

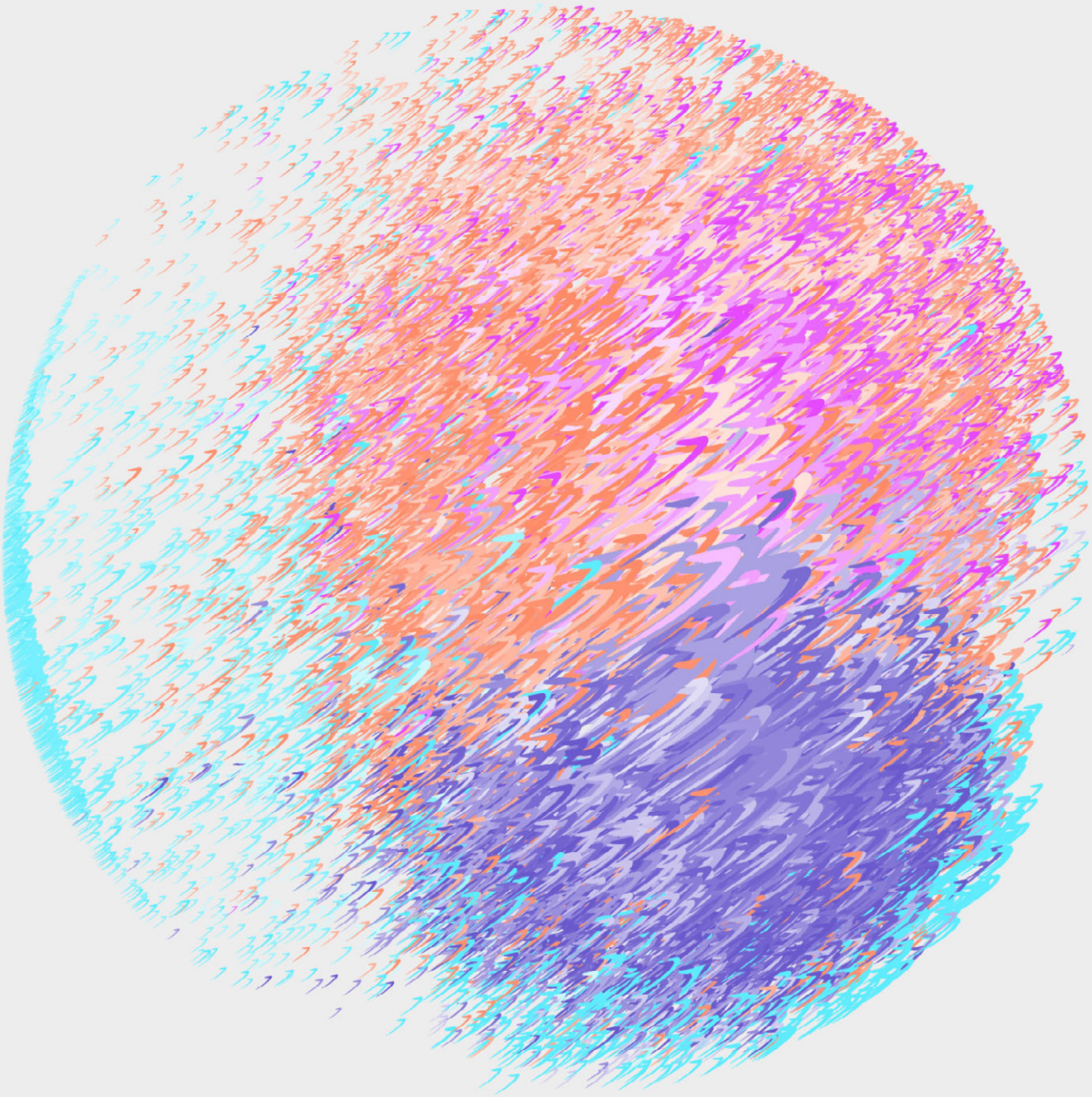
The more than 73,000 accounts that (re)tweeted our fake news sites at least 10 times in our sampled data are our starting set from which we draw the map. From this group, accounts with 10 followers or fewer in common with the rest of the group were removed. Note that this filtering mechanism, by itself, can often remove significant numbers of bots; bots on average have fewer followers and "friends" (accounts they follow which follow them back) and are less densely connected to the Twitter network. Even after this initial filtering step, though, 27,125 sites qualified for inclusion in the overall map. This makes the election map one of the largest and densest maps Graphika has ever produced.

After considering the problem in detail, we decided that the most useful approach would be to pull out the ultra-dense, highly connected core as its own map, with less connected sites mapped out separately (see periphery map below).

Accounts with a K-core of 175 or greater—that shared at least 175 followers on average with the rest of the map—were included in the core map. Remarkably, 13,861 sites met this extremely high bar for inclusion.

FIGURE 1

Election Core MAP



The blue accounts are *Trump Support*

The salmon accounts are *Conservative*

The pink accounts are *Hard Conservative*

The aquamarine accounts are *Others*

Election Core Map

Let us start with the election core map, with reflects Twitter activity surrounding fake and conspiracy news stories among the most followed accounts (Figure 1). Near the center of the map is a cluster of accounts with hundreds of thousands of followers each, including prominent conservative commentators and individuals associated with the Trump campaign. The central placement of these accounts reflects the fact that they are widely followed by other accounts on the map, *not* the volume of fake news that these accounts are tweeting.

From this central nexus we can see the intersection of different groups of accounts colored in shades of blue, salmon and pink. Segments in the *Pro-Trump* group are in shades of blue, and these segments create a dense cluster of interlinked accounts in the bottom center of the map.

Above the center of the map, we can see the *Conservative* group with its component segments in shades of salmon, and the *Hard Conservative* group with segments in shades of pink. The various Conservative segments are highly dispersed and together cover nearly the entire map. The Pro-Trump group and the Hard Conservative group, though, strongly overlap with each other. This unusual pattern, with little spatial separation between the various groups and segments, reflects the densely interconnected nature of political Twitter on the eve of the 2016 election.

The clear outlier segments, as expected, are all placed in the *Other* group. Here we can see clusters of accounts that focus on anti-immigrant or anti-Muslim themes, those that promote conspiracy theories, accounts that defend Julian Assange of WikiLeaks, and a few self-proclaimed racist and "white identity" accounts. These segments, in shades of aquamarine, are scattered mostly through the left half of the map. Many are pushed all the way to the edge, reflecting the relative lack of connection to sites in the middle of the map.

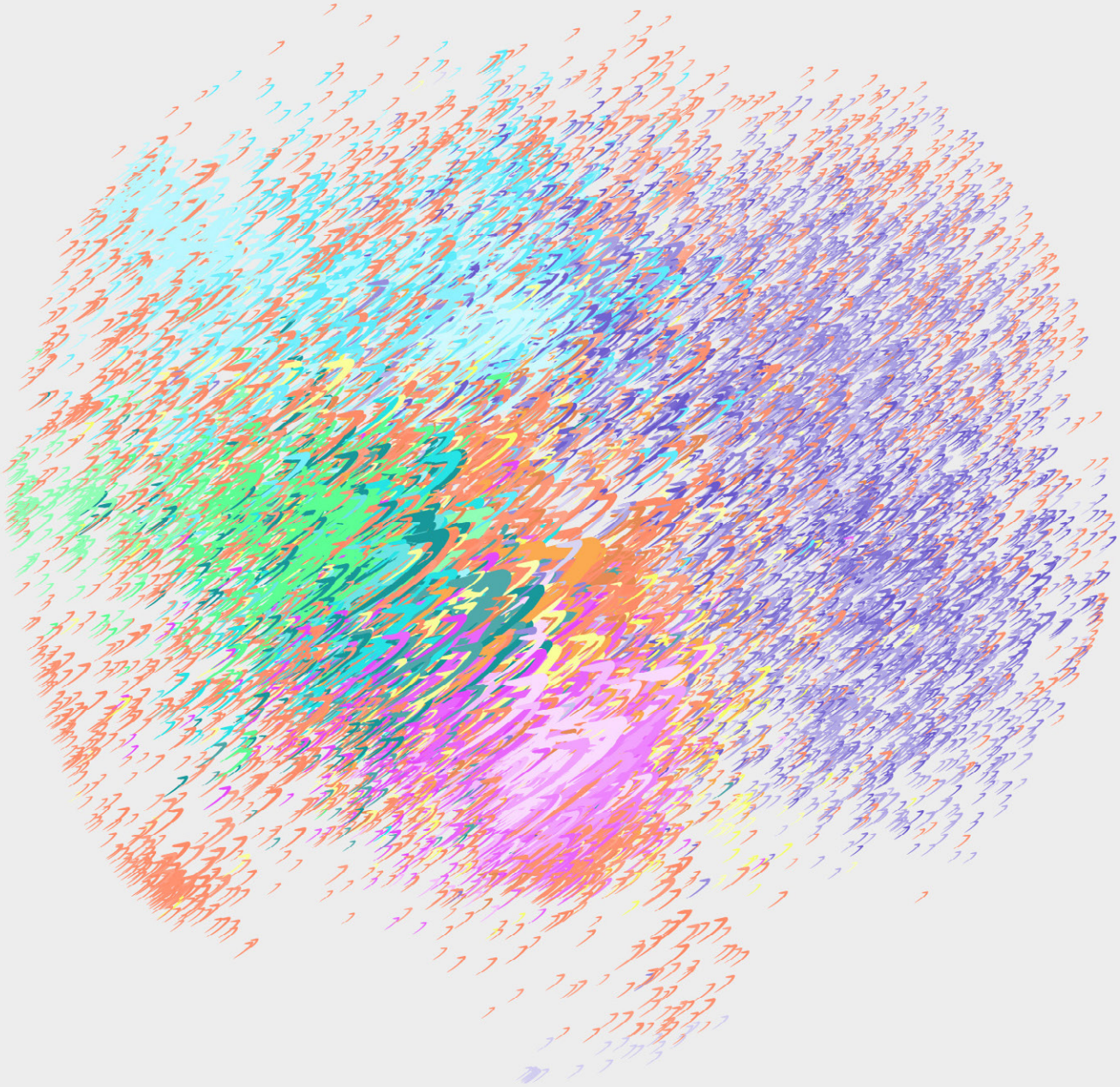
The dense and highly overlapping structure of this map reflects just how strongly integrated noncredible and fake news outlets were with credible discourse in the lead-up to the 2016 election. Links to fake news sites tweeted by this core group are nearly guaranteed to spread widely and quickly.

We do identify a number of segments linking especially often to particular fake news or conspiracy-leaning websites. Accounts within the *Trump Support | Core*, *Always Trump*, and *MAGA | Conservative* segments are especially active in linking to the Truthfeed site. Accounts in the *Constitutional Conservative* segment link often to The Gateway Pundit, while *Libertarian Journos* accounts are more likely to link to Activist Post.

In most segments, however, we do not see links to specific fake news dramatically more than other segments. Partly, this reflects the high baseline rate of links to fake news outlets, which is a function of how the map was created.

FIGURE 2

Election Periphery MAP



The blue accounts are
US Right

The pink accounts are
Liberals

The aquamarine accounts are
European Right

The green accounts are
Russia

The yellow accounts are
Social media marketing

The salmon accounts are
Other

The orange accounts are
Libertarian

The eastern blue accounts are
Int. Conspiracy | Activists

Election Periphery Map

While the election core map is ultra-dense and heavily overlapping, the second, periphery map (Figure 2) looks different. Here we are examining fake and conspiracy news sharing among Twitter accounts outside the ultra-connected central nodes of the previous graph. Despite removing the dense Pro-Trump core, this map still shows a cluster of accounts near the center-left—though these accounts have far fewer followers on average than those in the core map. But in contrast to the previous map, we see greater spatial separation between groups. The periphery map includes 13,264 accounts.

Let us start with the right side of the map, where we can see the *U.S. Right* group in shades of blue, totaling a whopping 4,732 accounts. Most accounts in this group have relatively few followers, but this is largely a selection effect: Many similar accounts with more followers are included in the core map.

A large number of accounts included in the U.S. Right group, particularly those on the periphery of the map, show clear evidence of automated posting. Consistent with indications of widespread automation, nearly all of the segments in the U.S. Right link heavily to multiple fake news outlets—a rate far above similar segments in the core map.

Continuing clockwise around the map, we encounter the *Libertarian* group in orange. The *U.S. Libertarian* and *U.S. Libertarian Journos* segments are widely spread across the map, reflecting their ties to a heterodox set of accounts. Several accounts of libertarian journalists near the center of the maps are the most followed accounts on the entire periphery map. The U.S. Libertarian group, perhaps unsurprisingly, links to a number of libertarian-leaning sites that traffic often in conspiracy theorizing.

The periphery map also shows that fake news is not just the province of accounts claiming to be pro-Trump or right-wing. Continuing clockwise, in the bottom center of the map, is the *U.S. Liberal* group in shades of pink. In this category, 1,206 accounts are placed in six segments. Some of these accounts offer seemingly contradictory messaging, combining attacks on the Democratic Party and Hillary Clinton from the left with endorsement of ultra right-wing conspiracy theories and retweets of Russia propaganda outlets such as RT and Sputnik.

In the bottom-left quadrant, we can find accounts and segments in the *International Conspiracy | Activist* group in eastern blue. These include self-proclaimed anti-New World Order accounts, accounts associated with the hacker collective Anonymous, and accounts supportive of the Occupy movement. U.K. far-left accounts also make an appearance,

along with ostensibly pro-Palestinian accounts. The *Anti-NWO* segments link heavily to Russia Insider and The Russophile, news sites that are overwhelmingly pro-Kremlin. The *Pro-Palestine* segment similarly often links to Russia Insider, a self-proclaimed "debunking" site based in Russia that regularly pushes Putin-friendly articles.

In green, on the left side of the map, we can see the *Russia* group. The *Russian News | Politics* segment is near the far left edge of the map, showing relatively weak ties to other accounts. This is consistent with our expectations, since most of these accounts post only in the Russian language. Of particular interest is the *Russian Trolls Abroad* segment, a cluster of accounts which pushes the Kremlin line on almost everything—often in provocative ways. This segment is among the most aggressive of any on the map in pushing fake news. Several prominent accounts in this segment have been suspended since the election.

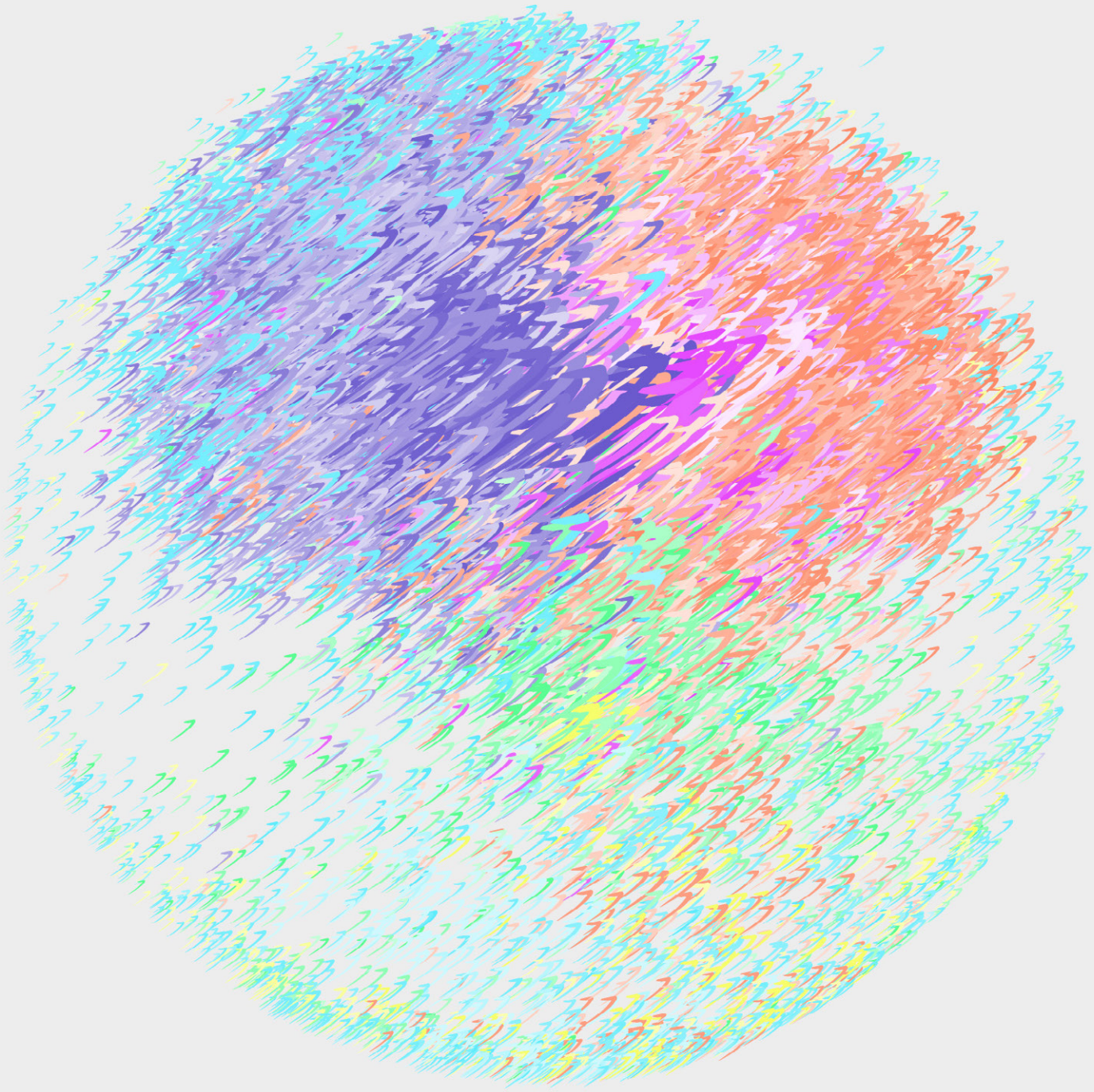
Continuing clockwise around the map, we see the *European Right* group in aquamarine on the top left. Included in this group are segments associated with the U.K. Independence Party, pro-Brexit segments, and segments supportive of Geert Wilders and the right wing of Dutch politics. We can also see strong connections between sites that seem to be right-wing French accounts. Many of these supposedly French accounts, though, focus to a large degree on Russian issues from a pro-Putin perspective, a strong indication of bot or troll accounts. The *Far Right France | Russia* and *European Right* segments often link to the French and German versions of RT, respectively.

Lastly, two groups are spread extremely widely across the maps and cannot be easily localized. The *Social Media Marketing* group, in yellow, consists mainly of accounts that focus on paid promotions. Many of these accounts postelection seem to have nothing to do with politics, instead promoting a motley array of commercial products. Likely these accounts were paid for political tweets and links during the election and have since moved on to other clients.

The *Other* group is similarly a grab bag of segments devoted to a host of different topics. The *International RT | WikiLeaks* segment is one of the most interesting in this group. Curiously, this segment includes several of the official Twitter accounts of fake news outlets. This pattern is particularly striking because these sites seem to have no obvious connection to Russia, WikiLeaks or indeed international content of any type, and yet these fake news sites share a significant fraction of their Twitter followers. This fact alone is curious, particularly in a map dominated by bots and semi-automated accounts.

FIGURE 3

Postelection MAP



The blue accounts are
Trump Support

The salmon accounts are
Conservative

The pink accounts are
Hard Conservative

The yellow accounts are
Russia

The green accounts are
International right / Anti-Islam

The aquamarine accounts are
Others

Postelection Map

For our final map (Figure 3), we turn to the 30-day period between March 12 and April 12, 2017. Overall during this period, 428,182 accounts in our sample (re)tweeted links to fake news, and more than 4.0 million tweets or retweets linked to fake or conspiracy news sites—a drop from the 6.6 million in the month preceding the election, but still an enormous volume of content.

As before, in creating the postelection map, we keep only accounts that linked to fake news at least 10 times in our sample, filtering out accounts that linked to fake news sites less often. We also filter out accounts only minimally connected to the rest of the graph with K-core decomposition: Only sites with a K-core of 10 or greater are included. A total of 12,032 accounts meet both criteria.

We examined accounts included in the postelection map using the Tweetbotornot machine learning package (Kearney 2018; see discussion above). The top 100 accounts, ranked by the number of followers who are also included in the map, averaged a 33 percent probability of being a bot—suggesting that automated posting is relatively common even among the most followed accounts in our map. We also classified 300 randomly selected accounts from the entire map, excluding the top 100; this random set of accounts was given an average 63 percent probability of being a bot.[63] These numbers do not include the 11 percent of the postelection map accounts that were suspended by Twitter as of April 2018, a group that overrepresents bots.

There is thus strong evidence that a majority of accounts in the map—and likely more than two-thirds—are bots or heavily automated cyborg accounts.

This map resembles the election core map much more than the periphery map. While the orientation of the map is different, this does not change the overall relationships between accounts. The same accounts are clustered together even if the map is flipped from left to right, or if the map is rotated from top to bottom.

Like the core election map, the postelection map is ultra-dense and heavily overlapping, with the most popular accounts clustered near the center. The largest of these groups can be seen in the upper-left quadrant. The *Trump Support* group in blue dominates this upper-left section, and it contains 15 distinct segments (subgroups). Particularly notable is the *Pro-Trump Far Right* segment, a set of ultra-popular accounts in the upper middle of the map.

Many accounts in this segment show behavior associated with fake accounts or automated posting: ultra-high posting rates, high retweet-to-tweet ratios, repeating variations of the same tweet over and over, suspicious names, and lack of personally identifiable information. Despite tens of thousands of followers, they receive few or no likes on many original postings. Original tweets often show English errors unusual in native speakers, such as the omission of articles in sentences. It is notable that this cluster is in the densest part of the map, reflecting heavy overlap in the accounts they follow, something that our methods would detect as similarity of interests.

Several of these segments link heavily to specific fake news outlets. The *Pro-Trump | Core* segment links heavily to Truthfeed, while the *Pro-Trump | Pundits*, *Pro-Trump | Tea Party* and *Pro-Trump Right* segments link heavily to both Truthfeed and The Gateway Pundit.

An even larger number of accounts are affiliated with the *Conservative* group in salmon, segments of which cover the entire right side of the map, along with a smattering of overlap leftward. Our clustering algorithms divide the Conservative group into 15 segments. Several of these segments link especially often to specific fake news outlets. The *Conservative | Vets* segment links heavily to Truthfeed, the *Tea Party | Libertarian* segment links heavily to The Gateway Pundit, and the *Libertarian | Pols* segment links heavily to The Free Thought Project. The *Libertarian / International* segment links heavily to Russia Insider.

The third group identified by the clustering algorithm is the *Hard Conservative* group, which contains seven segments. The Hard Conservative map segments, in pink, overlap almost completely with the conservative groups. Despite the overlap, though, we see significantly different linking patterns. In contrast to segments in the Trump Support and Conservative groups, few segments in the Hard Conservative group give disproportionate attention to specific fake news sites. Links to fake news sites from this group are more diffuse and less likely to feature a few favorite outlets.

The *Hard Conservative | Deplorable* segment also includes the @TEN_GOP account. @TEN_GOP claimed to be run by the Tennessee Republican Party, but we now know that it was operated by the Kremlin-linked Internet Research Agency.[64] The @TEN_GOP account does not show up on our pre-election map, though it is included in our pre-election data. When the account was discovered and suspended from Twitter, it had more than 100,000 followers—undoubtedly a popular account, but far from the most followed account in this map. However, our algorithms did place it very near the center of the map, owing to its extremely

diverse set of followers. On our map, 2,248 accounts linked to @TEN_GOP. Given what we now know about its origins, it is worth noting that the @TEN_GOP site did not receive any links from sites included in our Russia group.

The fourth largest group, the *International Right | Anti-Islam* group in green, is spread loosely across the entire map, with a small cluster of sites near the exact center. This group is dramatically smaller than the above three groups, and a very loose spread of this group reflects diverse liking patterns. The *International Right | SMM* segment, which seems to contain accounts focusing on social media marketing, presents an interesting case study: Although they do not link to fake news sites, they heavily retweet the account of the Russian Embassy in South Africa, as well as an automated account that advocates for the impeachment of Donald Trump. This pattern is consistent with paid promotional tweets and links. The *Anti-Islam | International* segment focuses on Southeast Asia, while the *International Anti-Islam* segment links heavily to French language content, including Russian propaganda sites such as RT and Sputnik. Lastly, the *White Identity* segment links heavily to alt-right sites, including the white supremacist Daily Stormer, and it retweets self-proclaimed racist and "white pride" accounts.

The fifth group, smaller still, is the *Russia* group in yellow. Here the clustering algorithm split the group into three segments. As expected, these accounts link heavily to Russian news agencies, and both official and unofficial pro-Putin Twitter accounts. Most of these sites are near the periphery of the map, reflecting their lack of connection with the core of the map.

Lastly, we have the *Other* group in aquamarine, a grab bag of accounts that do not fit neatly within other categories. The *Unclustered* segment mostly finds accounts that link to French-language Russian propaganda, with RT and Sputnik the most prominent examples. Yet the Other group also includes a smattering of ostensibly liberal accounts, though few of these are popular by the standards of other segments. The *International Pundits | Finance* segment is a mishmash of content focusing on British politics, Middle Eastern affairs and Russian propaganda sites, while the *International Media* segment retweets Russian media sites heavily, especially RT and Sputnik.

CHANGE AND CONTINUITY IN FAKE NEWS

In looking at the core network of sites that regularly push fake and conspiracy news articles, we can see both strong continuity and some important changes since the election period.

In terms of stability, the postelection map strongly resembles the election core map. Without the imminent election, the number of sites that meet the threshold for inclusion in the postelection maps drops. Still, the map remains ultra-dense, and the most heavily followed accounts overwhelmingly carry over to the postelection map.

Yet we can also see some structural changes in the postelection period. Accounts affiliated with Russia in the pre-election map seem to serve a brokerage role, serving as a cultural and political bridge between liberal U.S. accounts and European far-right accounts. Their patterns of followership provide a potential route for fake and conspiracy news to reach a broader audience.

The postelection map shows a different pattern. Accounts in the Russia cluster have become more peripheral. At the same time, the International Conspiracy | Activist cluster—also tied to Russia—is spread broadly through the map. International conspiracy-focused Twitter accounts seem to have become more important as brokers for fake news stories postelection.

Another important change in the postelection data—and one that policymakers and platforms should take note of—is the disappearance of The Real Strategy in the postelection data. The Real Strategy, an extreme conspiracy site, is the second-most linked fake news site on our election map. The site was a prominent participant in the Pizzagate hoax. Twitter and Reddit banned the site, apparently for doxing (publishing private information) and organized harassment, though the details on what exactly happened are unclear since many of the key materials have been removed.[65] As of spring 2018, the core website is no longer working, but The Real Strategy remains active on Facebook and other forums.

Whatever transpired, links to The Real Strategy largely disappeared in the postelection data. The site received more than 700,000 links in the pre-election period, the second-most in our sample. Many of these links seem to have come from a botnet; changes in topics tweeted by the accounts may suggest that the botnet was rented.[66] In the postelection period, by contrast, the site received only 1,534 links—a drop of more than 99.8 percent. The case of The Real Strategy suggests that concerted action can indeed be effective in drastically reducing links to fake and conspiracy news, providing that platforms like Twitter and Reddit are willing to act decisively.

FAKE ACCOUNTS FROM RUSSIA'S MOST PROMINENT TROLL FARM

One key question about disinformation on Twitter concerns the role of accounts run by the Russian government.

As of January 2018, Twitter claimed to have identified 3,814 Twitter accounts run by Russia's Internet Research Agency, along with an additional 50,258 automated accounts also run by the Russian government.[67] These more than 54,000 bot and troll accounts linked to the IRA have since been suspended. In a federal indictment made public in February 2018, prosecutors provided evidence that the IRA's activities had been approved at the highest levels of the Kremlin.

Of the nearly 4,000 IRA accounts supposedly identified, 2,752 have been named publicly as this report goes to press. These accounts allow us to see the role this organization played in our network.

Our data provide two countervailing lines of evidence about the role of Russia-aligned accounts on Twitter. On the one hand, only 65 accounts now known to be run by the Internet Research Agency appear in at least one of our maps. Our maps do include a number of prominent IRA accounts. The @WarfareWW, @Jenn_Abrams and @TEN_GOP accounts (among others) each had tens of thousands of followers and were quoted regularly in mainstream media.[68] The repeated quotation of a few dozen prominent IRA accounts in mainstream media is one potential avenue of influence.

At the same time, though, few IRA accounts reached that number of followers and visibility. Most IRA accounts have far too few followers to be included in our map and are automatically filtered. Most publicly known IRA accounts seem to have served as support accounts, providing retweets and amplification of a few high-profile accounts.

DISINFORMATION CAMPAIGNS ON TWITTER: CHRONOTOPES

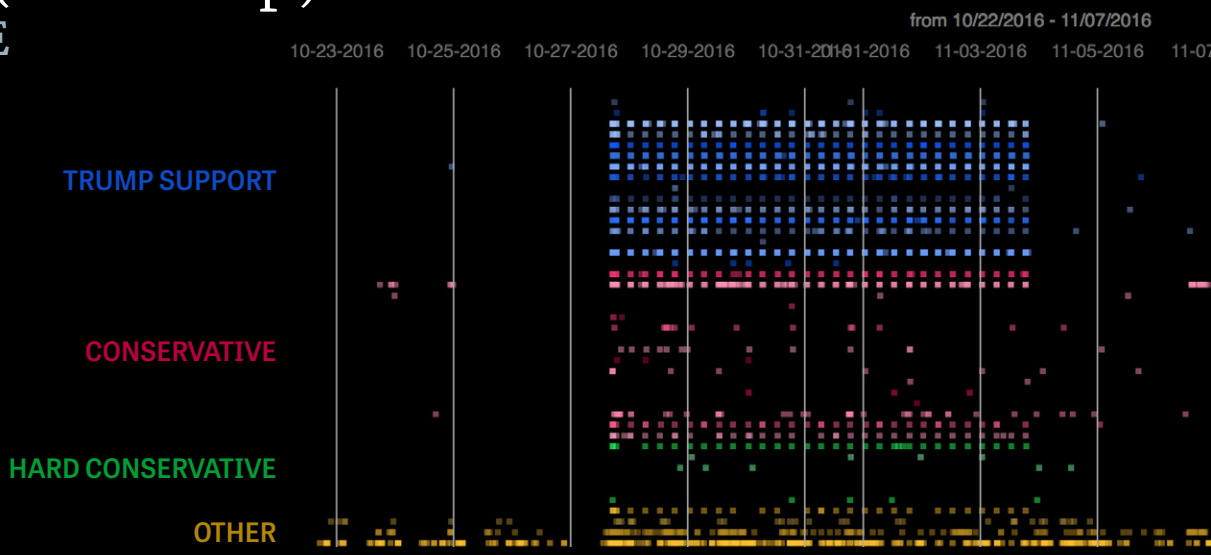
In addition to showing us the structural relationships between accounts that link to fake and conspiracy news, the maps also let us see how specific stories and hashtags are shared. With the maps built, we can look at *chronotopes*, a technique for visualizing network activity over time.

Chronotopes function as a sort of bar code. On the y-axis—in order—are groups and their component segments from the broader map. The x-axis shows time, with hash marks appearing whenever chosen content is tweeted or retweeted. As we read these graphics from left to right, we can see types of content wax and wane in popularity across different groups and segments. In this case we will be looking at hashtags that were especially popular within our network both in the month before the election and during the spring of 2017. Chronotopes are always specific to a particular map—for example, the core and periphery election maps produce two separate chronotopes for the same hashtag.

Looking at these examples gives us insights into the disinformation network's goals and priorities. As noted above, a significant majority of these accounts are social bots or semi-automated accounts. Consistent with this, the hashtag data show repeated efforts to push favored hashtags in ways rarely or never seen in organic Twitter traffic. In the sections below, we will walk through several examples that range from curious to highly suspicious to obviously automated behavior.

FIGURE 4

#NoDAPL (Core Map)
CHRONOTOPE



#NoDAPL: Classic Botnet Behavior

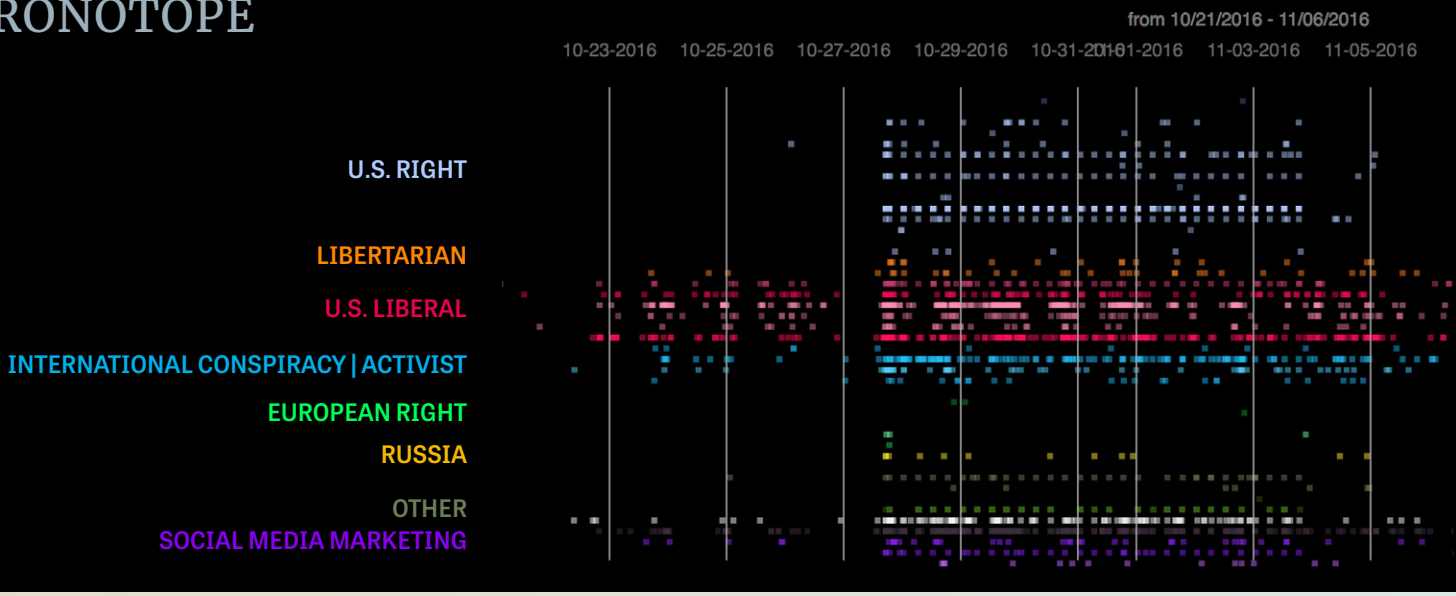
Popular discussion of online disinformation has often obscured the difference between bots—automated accounts—and trolls, human-controlled accounts usually used to provoke or to spread disinformation (see earlier discussion). Most often we can see both bot and troll activity around a particular Twitter topic—and indeed both types of activity from a single account. Yet in a few cases, the core disinformation network shows examples of totally automated behavior.

One of the most glaring examples of such botnet activity can be seen with the #NoDAPL hashtag. #NoDAPL was used to express opposition to the Dakota Access Pipeline, a planned oil pipeline stretching from North Dakota to Illinois. For more than a week in late October 2016—every six hours around the clock—hundreds of accounts started tweeting the hashtag #NoDAPL in unison. The six-hour delay between tweets may have been intended to avoid tripping automated alarm bells at Twitter, which can suspend accounts that tweet the same phrase too often.

We chart a chronotope of #NoDAPL on the core map above (Figure 4). The checkerboard regularity of these tweets is characteristic of botnet behavior. Interestingly, many different tweets—seemingly separate—are included in each every-six-hour #NoDAPL tweet wave, perhaps to obscure coordination. It is notable, too, that the content of these tweets strongly contradicts these accounts' apparent identities. Most of the accounts retweeting the #NoDAPL hashtag are in the Trump Support group, even though candidate Trump proposed a big expansion in oil and gas exploration and drilling.

FIGURE 5

#NoDAPL (Periphery Map)
CHRONOTOPE

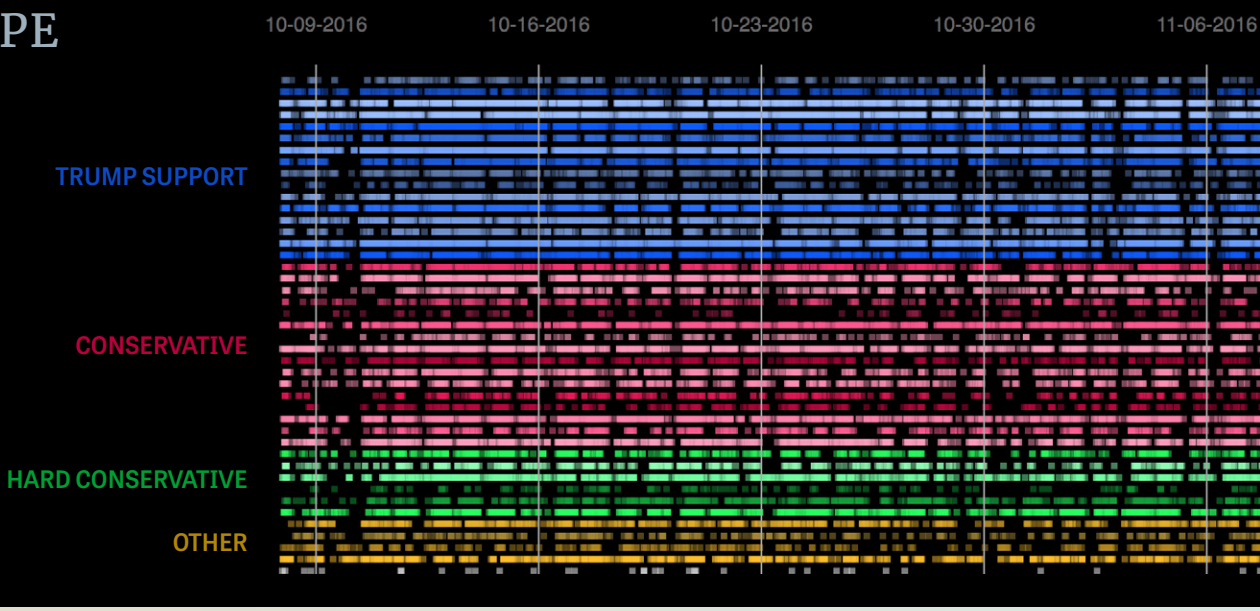


Looking at the periphery map's chronotope for the same hashtag (Figure 5) produces an interesting comparison and contrast. In addition to bot accounts tweeting at the every-six-hours pattern, we can also see less organized tweeting in the U.S. Liberal group—though a majority of these accounts also seem to be at least semi-automated accounts.

Some of most troubling examples of propaganda during the election campaign involved deliberate attempts to stoke conflict and even violence. Many of the #NoDAPL tweets contain references to "shots fired!" as well as promotion of racial and ethnic tension. While the source of the botnet's tweets is not clear, both techniques are common in campaigns we now know to be Russian-directed.

FIGURE 6

#WikiLeaks CHRONOTOPE



The #WikiLeaks Drumbeat

Several other hashtags in our data also suggest coordinated activity. Many of the hashtags retweeted most often by our disinformation network echo the broader conservative Twitter sphere. Much of this repetition of pro-Trump and pro-conservative messages seems to be *hashtag spamming*, exploiting hashtags that are already popular in order to reach a wider audience for message. Hashtag spamming is common, though prohibited by Twitter's terms of service.[69] #MAGA, #Trump, #tcot (top conservatives on Twitter) and #Hillary are the top four hashtags in our sample—all likely examples of automated accounts adopting already-popular hashtags to reach a broader audience. As the federal indictment shows, Internet Research Agency accounts similarly repeated popular campaign hashtags.[70]

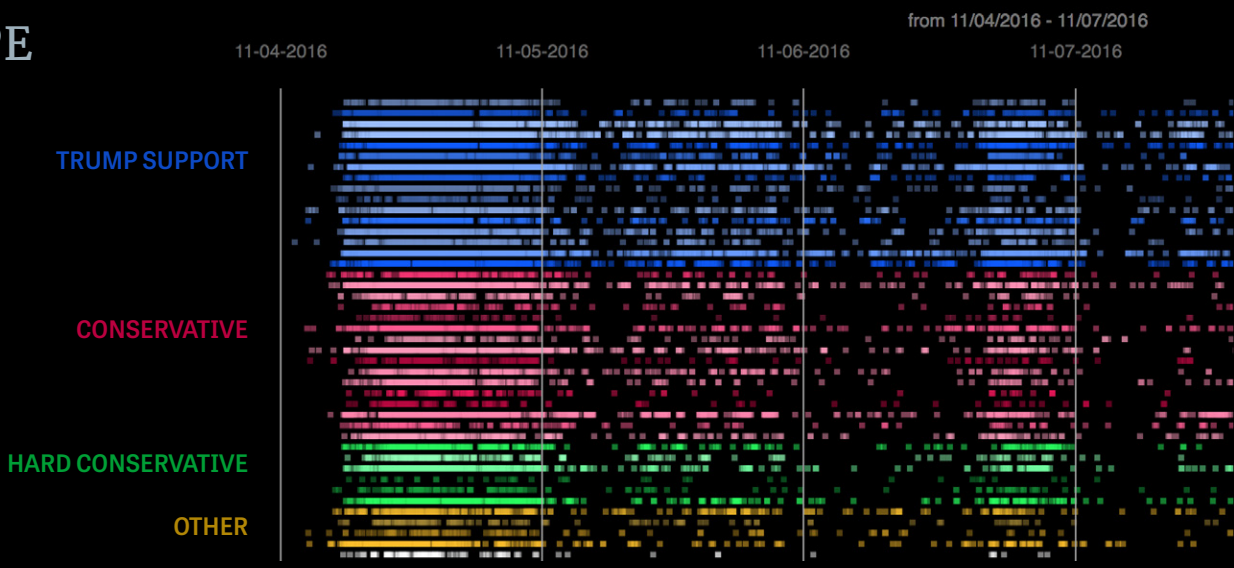
Yet the accounts in our map do not seem to be like others that use campaign hashtags. For starters, they show message discipline far stricter than what is observed in human-run, noncoordinated social media activity. One of the clearest examples of this is the #WikiLeaks hashtag, chronicled in the core map above (Figure 6).

Organic Twitter activity waxes and wanes dramatically from day to day, and it follows the larger news agenda quite closely. In contrast, the chronotope of the #WikiLeaks hashtag shows remarkable regularity and near-total independence from the news cycle. #WikiLeaks is repeated daily (and usually hourly) by accounts in all of the different segments in our map for all 30 days in our sample. This level of consistency is rarely if ever observed in genuine, uncoordinated Twitter activity.

FIGURE 7

#SpiritCooking

CHRONOTOPE



'Pizzagate' and the #SpiritCooking Hashtag

Other hashtags also show dynamics that are unusual outside of coordinated campaigns. The #SpiritCooking hashtag produces another highly unusual pattern.

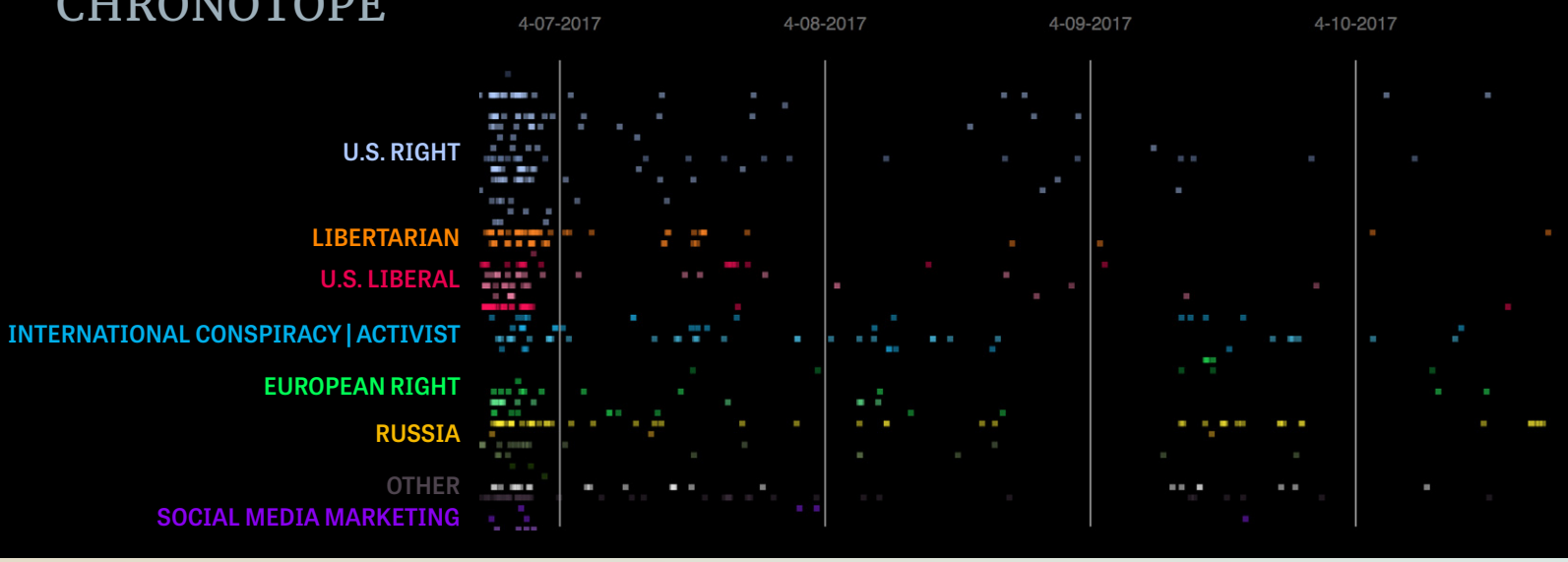
The #SpiritCooking hashtag referenced emails stolen from John Podesta by the Russian military intelligence service and later released through WikiLeaks.[71] Passing references in Podesta's emails to performance artist Marina Abramovic were falsely used to claim that Clinton engaged in satanism and ritual child abuse.[72] These claims were a key part of the so-called Pizzagate conspiracy theory.

An astonishing volume of accounts in our network retweeted the #SpiritCooking hashtag on Nov. 4 and (to a lesser extent) in the three following days (Figure 7). The #SpiritCooking tweets engage all the segments of the main map at off-the-charts volume, racking up more than 57,000 tweets in our map in just a couple of days.

Despite being active for only a few days at the end of the election cycle, #SpiritCooking was the fifth-most tweeted hashtag during the election period in the core map. #SpiritCooking is a case where the volume and repetition alone make it essentially impossible that activity around the hashtag was organic. Whoever runs these accounts—again, most of which seem to be automated—pulled out all the stops to push this story on the eve of the election.

FIGURE 8

#SyriaHoax
CHRONOTOPE



#SyriaHoax

On April 4, 2017, Syrian government forces attacked the town of Khan Sheikhoun with sarin nerve gas. Despite overwhelming evidence that the Syrian air force was responsible, two days later claims that the attack was a hoax began to spread on Twitter using the #SyriaHoax hashtag. Reports about the use of nerve gas in Syria were of great concern to the Russian government, which is closely allied with the Assad regime. Other research has found sustained Russian-sponsored disinformation campaigns focusing on Syria, in an apparent effort to cover up evidence of war crimes.[73] Given this context, the #SyriaHoax hashtag would be a likely locus for Russian disinformation efforts.

The chronotope for the #SyriaHoax hashtag on the postelection map can be seen above (Figure 8). Many features of tweet activity surrounding the hashtag would be unusual without coordination.

First, note that the push behind the #SyriaHoax hashtag and articles comes two days after the sarin attack became public. Unusually, this burst of tweets comes after the high-profile news coverage on the day of the event. Some stories reference the claim by former U.S. Rep. Ron Paul that the Syria attack might have been a "false flag" operation designed to hurt the Syrian government. This might suggest opportunistic amplification of messages.

Second, the earliest tweets using this hashtag in our sample come from accounts likely to be automated or semi-automated. The first 10 accounts (at least) to retweet the hashtag all have high tweet volume, repetitive and formulaic tweets, very low engagement by followers, limited biographical information, etc.—in short, they all have a signature associated with bots. Hundreds of other accounts (including many likely bots) then joined in at high volume in the afternoon and evening of April 6.

Third, the hashtag is used initially to push separate stories from Infowars, Zero Hedge and GlobalResearch. Previous reports have tied both Zero Hedge and GlobalResearch to Russian state influence campaigns.[74] Infowars, too, has been linked to Russian propaganda efforts, including its republishing of more than 1,000 articles from RT on its site.[75] This choice of messengers, then, is consistent with pro-Russian disinformation campaigns.

Fourth, after being pushed out by numerous automated accounts, the hashtag and initial "false flag" stories seem to be everywhere at once. Typical hashtags are limited to a few segments, or across a couple of closely related groups. Here we see the opposite: Widely disparate groups within 30 minutes all adopt the same hashtag and push the same message. In particular, note the extremely heavy retweeting of conservative-leaning content from ostensibly liberal-leaning accounts.

Fifth, we can see how some segments work to keep the #SyriaHoax hashtag atop the news agenda long after the particular news cycle would seem to have ended. Most news stories and hashtags peter out in few hours. Retweeting a hashtag at high volume is unusual except with ongoing live events, such as a football game or a professional conference. Here, though, many accounts retweet the hashtag for days.

Especially notable here are the *Russia* group, the *International Conspiracy | Activist* group and the *Other* group (see descriptions above). Compared with others, accounts in these groups provide regular references to the #SyriaHoax hashtag for the better part of a week. Other segments decay more quickly, with occasional and sporadic retweets. In addition, accounts from these three groups show remarkably correlated patterns of retweeting, especially the timing of tweets on April 8 and 9. This in itself hints at possible coordination.

In total, the patterns are suggestive of coordination across accounts in different segments. We see evidence, too, that specific Russian-aligned clusters of accounts worked to increase the dwell time of the story, attempting to set the news agenda and the framing of the Syrian gas attack.

FIGURE 9

#SethRich CHRONOTOPE

#SethRich

We can find other examples of cases in which this network of accounts pushes falsehoods that align with Russian goals. After U.S. officials reported that Russian intelligence agencies had been behind the hacking of Democratic National Committee emails, a number of stories sprung up attempting to pin the hacking on non-Russian sources. DNC data analyst Seth Rich, who was killed in a botched robbery in summer 2016, was named by false stories as an alternative source for the stolen emails.

The spread of the #SethRich hashtag in our network has several features that suggest a coordinated campaign instead of organic activity—over and above the fact that it was amplified by hundreds of accounts that seem to be automated. The network was used to spread content supposedly from DNC hacker Guccifer 2.0 himself, whom we now know to be a Russian military intelligence officer.[76]

As we can see in the chronotope (Figure 9), in late March and early April, there is little activity in our network surrounding the #SethRich hashtag. Fewer than 20 tweets use this hashtag—though several of these stories link to Russian-aligned media, including stories in Sputnik, RT and Zero Hedge. The early lack of references to the Seth Rich case is itself surprising, given that the network pushes numerous other similarly prominent conspiracy theories over the same period.

In the early afternoon of April 8, 2017, a number of accounts in the network start retweeting several older conspiracy stories about Seth Rich. These initial tweets lack any obvious context or news hook. A few hours later, though, the use of the #SethRich hashtag shifts, with nearly all later tweets linking to a Gateway Pundit story. The Gateway Pundit article is based on newly released text messages from WikiLeaks, in which Guccifer 2.0 appears to name someone called "Seth" as "my whistleblower."

The text messages included in the WikiLeaks story cannot be independently verified, of course. But if these texts were indeed from Guccifer 2.0, this would be a case of the network directly boosting messages of Russian "active measures" intended to influence U.S. politics.

CONCLUSION

A supercluster of densely interlinked, heavily followed accounts plays a large role in the spread of fake news and disinformation on Twitter. Social bots likely make up the majority of the accounts in the supercluster, and accounts in the cluster participate in what appear to be coordinated campaigns to push fake news stories. The core of this network remains highly active as this report goes to press. More than 80 percent of the accounts in our 2016 election maps are still active, and they publish more than a million tweets on a typical day.

These findings raise troubling questions. Some of the disinformation efforts in which these accounts participated during the 2016 election campaign were orchestrated by foreign actors, and they resulted in federal felony indictments. Yet our data show that many accounts active in those disinformation campaigns continue to operate, despite clear evidence of automated activity. The persistence of so many high-profile accounts spreading disinformation casts doubt on the effectiveness of Twitter's efforts to police its platform.

Many of the accounts active in the 2016 election disinformation campaigns continue to operate, despite clear evidence of automated activity.

This report challenges many common beliefs about fake news and gives policymakers a different set of questions to consider in addressing online disinformation. Structurally, the networks of accounts that spread fake and conspiracy news on Twitter are both *large and ultra-dense*. Fake news that reaches the core has countless paths by which to spread. Even worse, the backchannel coordination we document means that the public network of followers is not necessarily a reliable guide to the actual patterns of disinformation spread. Much more can be done to identify and ban popular accounts that repeatedly circulate disinformation, and

accounts with many human followers are costly for bad actors to replace. Still, penalizing popular accounts that disseminate misinformation, by itself, is unlikely to significantly degrade disinformation efforts.

On the other hand, our maps do provide evidence that other types of interventions may be more successful. Many have suggested that fake news is a game of "whack-a-mole," with new fake news sites constantly emerging.[77] Our data tell a different story. Both before and after the election, most Twitter links to fake news are concentrated on a few dozen sites, and those top fake and conspiracy sites are largely stable. Reducing the social media audience of just the dozen most linked fake and conspiracy sites could dramatically reduce fake news on Twitter.

Beyond the core of high-profile accounts, many fake accounts exist to inflate numbers of followers, likes and retweets. Forced labeling of bots—and excluding bots from public like/retweet/follower totals—would require more human activity and expense by bad actors to achieve the same results. Similarly, forcing accounts tweeting about politics to pass an occasional captcha test to prove that they are human would also significantly raise costs for botnet operators with little impact on ordinary users. Firms such as Facebook and Google have long used such techniques in fraud-prone areas like personal finance. Fraud in politics and news is now widespread, and these areas demand similar precautions.

This report will not be the last word on digital disinformation, but one thing is clear: The fake news that matters most is not organic, small-scale or spontaneous. Most fake news on Twitter links to a few established conspiracy and propaganda sites, and coordinated campaigns play a crucial role in spreading fake news. The good news, though, is that policies focused on the largest fake and conspiracy news sites could greatly reduce the amount of fake news people see. Mapping the accounts that spread fake news is a key first step toward reducing its influence on democratic politics.

Reducing the social media audience of just the dozen most linked fake and conspiracy sites could dramatically reduce fake news on Twitter.

Bibliography

Allcott, H., and M. Gentzkow. "Social Media and Fake News in the 2016 Election." Working Paper 23089. National Bureau of Economic Research, January 2017, revised June 2017. http://www.nber.org/papers/w23089.

Alloway, Tracy, and Luke Kawa. "Unmasking the Men behind Zero Hedge, Wall Street's Renegade Blog." *Bloomberg*, April 29, 2016. https://www.bloomberg.com/news/articles/2016-04-29/unmasking-the-men-behind-zero-hedge-wall-street-s-renegade-blog.

Alvarez-Hamelin, José Ignacio, Luca Dall'Asta, Alain Barrat, and Alessandro Vespignani. "K-core Decomposition of Internet Graphs: Hierarchies, Self-similarity and Measurement Biases." *Networks & Heterogeneous Media* 3, no. 2 (2008): 371–93. http://www.aimsciences.org/journals/displayArticles.jsp?paperID=3285.

Barry, Rob, and Shelby Holliday. "Russian Trolls Tried to Torpedo Mitt Romney's Shot at Secretary of State." *Wall Street Journal*, March 8, 2018. https://www.wsj.com/articles/russian-trolls-tried-to-torpedo-mitt-romneys-shot-at-secretary-of-state-1520505000.

Bartles, Charles K. "Getting Gerasimov Right." *Military Review*, January-February 2016. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf.

Bertolin, Giorgio. "Conceptualizing Russian Information Operations: Info-War and Infiltration in the Context of Hybrid Warfare." *IO Sphere*, Summer 2015: 10.

Bessi, Alessandro, and Emilio Ferrara. "Social Bots Distort the 2016 Presidential Election Online Discussion." *First Monday* 21, no. 11 (November 2016). http://firstmonday.org/article/view/7090/5653.

Boyd, William. "The Secret Persuaders." *The Guardian*, August 19, 2006. https://www.theguardian.com/uk/2006/aug/19/military.secondworldwar.

Bradshaw, Samantha, and Philip N. Howard. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Working Paper 2017.12. Oxford Internet Institute, 2017. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf.

Chandrasekharan, E., U. Pavalanathan, A. Srinivasan, A. Glynn, J. Eisenstein, and E. Gilbert. "You Can't Stay Here: The Efficacy of Reddit's 2015 Ban Examined through Hate Speech." *Proceedings of the ACM on Human-Computer Interaction*, November 2017. http://comp.social.gatech.edu/papers/cscw18-chand-hate.pdf.

Chavoshi, Nikan, Hossein Hamooni, and Abdullah Mueen. "Identifying Correlated Bots in Twitter." *Social Informatics*. Lecture Notes in Computer Science 10047 (2016): 14–21. https://link.springer.com/chapter/10.1007/978-3-319-47874-6_2.

Chen, Adrian. "The Agency." *New York Times Magazine*, June 2, 2015. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Chong, D., and J. N. Druckman. "Dynamic Public Opinion: Communication Effects over Time." *American Political Science Review* 104, no. 4 (2010): 663–80.

Cialdini, R. B. "Harnessing the Science of Persuasion." *Harvard Business Review* 79, no. 9 (2001): 72–81.

Clark, Campbell, and Mark MacKinnon. "NATO Research Centre Sets Sights on Canadian Website over Pro-Russia Disinformation." *Globe and Mail*, November 17, 2017. https://www.theglobeandmail.com/news/world/nato-research-centre-sets-sights-on-canadian-website-over-pro-russian-disinformation/article37015521/.

Collins, Ben, Kevin Poulsen, and Spencer Ackerman. "Russia Used Facebook Events to Organize Anti-Immigrant Rallies on U.S. Soil." *Daily Beast*, September 11, 2017. http://www.thedailybeast.com/exclusive-russia-used-facebook-events-to-organize-anti-immigrant-rallies-on-us-soil.

Collins, Ben, Gideon Resnick, Kevin Poulsen, and Spencer Ackerman. "Russians Appear to Use Facebook to Push Trump Rallies in 17 U.S. Cities." *Daily Beast*, September 20, 2017. http://www.thedailybeast.com/russians-appear-to-use-facebook-to-push-pro-trump-flash-mobs-in-florida.

Collins, Ben, and Joseph Cox. "Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World." *Daily Beast*, November 2, 2017. https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world.

Cresci, Stefano, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, and Maurizio Tesconi. "The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race." *Proceedings of the 26th International Conference on World Wide Web Companion*, Perth, Australia, April 2017, 963–72. https://dl.acm.org/citation.cfm?id=3055135.

Crowell, Colin. "Our Approach to Bots & Misinformation." Twitter.com, accessed May 17, 2018. https://blog.twitter.com/official/en_us/topics/company/2017/Our-Approach-Bots-Misinformation.html.

Dave, Paresh. "Without These Ads, There Wouldn't Be Money in Fake News." *Los Angeles Times*, December 9, 2016. http://www.latimes.com/business/technology/la-fi-tn-fake-news-ad-economy-20161208-story.html.

Davies, Jessica. "Facebook's European Media Chief: Fake News Is a 'Game of Whack-a-Mole.' " *Digiday*, January 12, 2017. https://digiday.com/uk/facebooks-european-media-chief-addresses-fake-news-game-whack-mole/.

Dawsey, Josh. "Russian-funded Facebook Ads Backed Stein, Sanders and Trump." *Politico*, September 26, 2017. http://www.politico.com/story/2017/09/26/facebook-russia-trump-sanders-stein-243172.

Digital Forensic Research Lab. "#BotSpot: Twelve Ways to Spot a Bot: Some Tricks to Identify Fake Twitter Accounts." Atlantic Council, August 28, 2017. https://medium.com/dfrlab/botspot-twelve-ways-to-spot-a-bot-aedc7d9c110c.

Digital Forensic Research Lab. "The Russians Who Exposed Russia's Trolls: A Tribute to the Russian Journalists Who Exposed the 'Troll Factory.' " Atlantic Council, March 8, 2018. https://medium.com/dfrlab/the-russians-who-exposed-russias-trolls-72db132e3cd1.

Dorogovtsev, S. N., A. V. Goltsev, and J. F. F. Mendes. "K-core Organization of Complex Networks." *Physical Review Letters* 96, no. 4 (February 2006).

Ecker, Ullrich K. H., Joshua L. Hogan, and Stephan Lewandowsky. "Reminders and Repetition of Misinformation: Helping or Hindering Its Retraction?" *Journal of Applied Research in Memory and Cognition* 6, no. 2 (2017): 185–192. https://www.sciencedirect.com/science/article/pii/S2211368116301838.

European Commission. *Final report of the High Level Expert Group on Fake News and Online Disinformation*, 2018. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions. United States Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism. Testimony of Sean J. Edgett, acting general counsel, Twitter Inc. October 31, 2017. https://www.judiciary.senate.gov/download/10-31-17-edgett-testimony.

Faris, Robert M., Hal Roberts, Bruce Etling, Nikki Bourassa, Ethan Zuckerman, and Yochai Benkler. *Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election*. Berkman Klein Center for Internet & Society Research Paper, 2017. https://dash.harvard.edu/bitstream/handle/1/33759251/2017-08_electionReport_0.pdf.

Ferrara, E., O. Varol, C. Davis, F. Menczer, and A. Flammini. "The Rise of Social Bots." *Communications of the ACM* 59, no. 7 (2016): 96–104.

Ferrara, Emilio. "Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election," 2017. https://arxiv.org/pdf/1707.00086.pdf.

Fletcher, Richard, and Rasmus Kleis Nielsen. "Are News Audiences Increasingly Fragmented? A Cross-National Comparative Analysis of Cross-Platform News Audience Fragmentation and Duplication." *Journal of Communication* 67, no. 4 (2017): 476–98.

Fourney, Adam, Miklos Z. Racz, Gireeja Ranade, Markus Mobius, and Eric Horvitz. "Geographic and Temporal Trends in Fake News Consumption During the 2016 US Presidential Election." *Proceedings of the CIKM,* Singapore, November 2017, 2071–74. https://www.microsoft.com/en-us/research/publication/geographic-temporal-trends-fake-news-consumption-2016-us-presidential-election/.

Francois, Camille, Vladimir Barash, and John Kelly. "Measuring Coordinated vs. Spontaneous Activity in Online Social Movements," 2017. https://osf.io/preprints/socarxiv/ba8t6/.

Frenkel, Sheera, and Nicholas Fandos. "Facebook Identifies New Influence Operations Spanning Globe." *New York Times,* August 21, 2018. https://www.nytimes.com/2018/08/21/technology/facebook-political-influence-midterms.html.

Fruchterman, T. M., and E. M. Reingold. "Graph Drawing by Force-directed Placement." *Software: Practice and experience* 21, no. 11 (1991): 1129–64.

Gabuav, Alexander. "There Is No Objectivity" [«Нет никакой объективности»]. Russian language interview with Margarita Simonyan, editor-in-chief of Russia Today. Kommersant, 2012. https://www.kommersant.ru/doc/1911336.

Galeotti, Mark. "I'm Sorry for Creating the 'Gerasimov Doctrine.' " *Foreign Policy,* March 5, 2018. http://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

Garrett, R. Kelly, and Natalie Jomini Stroud. "Partisan Paths to Exposure Diversity: Differences in Pro- and Counterattitudinal News Consumption." *Journal of Communication* 64, no. 4 (2014): 680–701.

Gerasimov, Valery. "The Value of Science Is in the Foresight." Originally published in *Military-Industrial Courier* (*Voyenno-Promyshlennyy Kurier,* Russia) February 27, 2013, translation published in *Military Review* (U.S.) January-February 2016. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

Giles, Keir. *Handbook of Russian Information Warfare*. NATO Defense College, 2016. http://www.ndc.nato.int/news/news.php?icode=995.

Gorenburg, Dmitry. "New Gerasimov Article on Nature of Warfare." *Russian Military Reform* (blog), March 17, 2017. https://russiamil.wordpress.com/2017/03/17/new-gerasimov-article-on-nature-of-warfare/.

Gotev, Georgi. "Commission: Russian Propaganda Has Deeply Penetrated EU Countries." *Euractiv,* July 13, 2016. https://www.euractiv.com/section/global-europe/news/thurs-commission-official-russian-propaganda-has-deeply-penetrated-eu-countries/.

Griffin, Drew, and Donie O'Sullivan. "The Fake Tea Party Twitter Account Linked to Russia and Followed by Sebastian Gorka." CNN, September 22, 2017. http://www.cnn.com/2017/09/21/politics/tpartynews-twitter-russia-link/index.html.

Grimme, Christian, Mike Preuss, Lena Adam, and Heike Trautmann. "Social Bots: Human-Like by Means of Human Control?" *Big Data* 5, no. 4 (2017): 279–93. https://www.liebertpub.com/doi/10.1089/big.2017.0044.

Hern, Alex, Pamela Duncan, and Helena Bengtsson. "Russian 'Troll Army' Tweets Cited More Than 80 Times in UK Media." *The Guardian*, November 20, 2017. https://www.theguardian.com/media/2017/nov/20/russian-troll-army-tweets-cited-more-than-80-times-in-uk-media.

Higgins, Andrew. "Fake News, Fake Ukrainians." *New York Times,* February 17, 2017. https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html.

Higgins, Andrew, Mike McIntire, and Gabriel J. X. Dance. "Inside a Fake News Sausage Factory: 'This Is All About Income.' " *New York Times*, November 25, 2016. https://www.nytimes.com/2016/11/25/world/europe/fake-news-donald-trump-hillary-clinton-georgia.html.

Howard, Philip N., Gillian Bolsover, Bence Kollanyi, Samantha Bradshaw, and Lisa-Maria Neudert. "Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing Over Twitter?" Oxford, UK: Project on Computational Propaganda, March 26, 2017. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/03/What-Were-Michigan-Voters-Sharing-Over-Twitter-v2.pdf.

Isaac, Mike, and Scott Shane. "Facebook's Russia-Linked Ads Came in Many Disguises." *New York Times,* October 2, 2017. https://www.nytimes.com/2017/10/02/technology/facebook-russia-ads-.html.

Isaac, Mike, and Daisuke Wakabayashi. "Russian Influence Reached 126 Million Through Facebook Alone." *New York Times,* October 30, 2017. https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

Karlsen, Geir H. "Tools of Russian Influence: Information and Propaganda." In *Ukraine and Beyond*, edited by Janne Haaland Matlary and Tormod Heier, 181–208. Palgrave Macmillan, Cham, 2016.

Kearney, Mike. Botrnot: R package for detecting Twitter bots via machine learning [software package]. 2018. https://github.com/mkearney/botrnot.

Kelly, John W. Valence graph tool for custom network maps. *U.S. Patent Application No. 14/101,811*, 2013.

Kiely, Eugene, and Lori Robertson. "How to Spot Fake News." FactCheck.org. November 18, 2016. http://www.factcheck.org/2016/11/how-to-spot-fake-news/.

Killing the Truth: How Russia Is Fuelling a Disinformation Campaign to Cover Up War Crimes in Syria. The Syria Campaign, 2017. http://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf.

Kinder, D. R., and N. P. Kalmoe. *Neither Liberal nor Conservative: Ideological Innocence in the American Public*. Chicago: University of Chicago Press, 2017.

Kirby, Emma Jane. "The City Getting Rich from Fake News." BBC, December 5, 2016. http://www.bbc.com/news/magazine-38168281.

Kollanyi, Bence, Philip N. Howard, and Samuel C. Woolley. "Bots and Automation over Twitter during the U.S. Election." Data Memo 2016.4. Oxford, UK: Project on Computational Propaganda, November 17, 2016. http://comprop.oii.ox.ac.uk/research/working-papers/bots-and-automation-over-twitter-during-the-u-s-election/.

Lazer, David M. J., Matthew Baum, Nir Grinberg, Lisa Friedland, Kenneth Joseph, Will Hobbs, and Carolina Mattsson. "Combating Fake News: An Agenda for Research and Action." May 2017. https://www.hks.harvard.edu/publications/combating-fake-news-agenda-research-and-action.

Lazer, David M. J., Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, Michael Schudson, Steven A. Sloman, Cass R. Sunstein, Emily A. Thorson, Duncan J. Watts, and Jonathan L. Zittrain. "The Science of Fake News." *Science* 359, no. 6380 (March 2018): 1094–96. http://science.sciencemag.org/content/359/6380/1094.

Leonnig, Carol D., Tom Hamburger, and Rosalind S. Helderman. "Russian Firm Tied to Pro-Kremlin Propaganda Advertised on Facebook during Election." *Washington Post*, September 6, 2017. https://www.washingtonpost.com/politics/facebook-says-it-sold-political-ads-to-russian-company-during-2016-election/2017/09/06/32f01fd2-931e-11e7-89fa-bb822a46da5b_story.html.

Linvill, Darren L., and Patrick L. Warren. "Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building." July 2018. http://pwarren.people.clemson.edu/Linvill_Warren_TrollFactory.pdf.

Lister, Tim, Jim Sciutto, and Mary Ilyushina. "Putin's 'Chef,' the Man behind the Troll Factory." CNN, October 17, 2017. https://www.cnn.com/2017/10/17/politics/russian-oligarch-putin-chef-troll-factory/index.html.

Lukito, Josephine, and Chris Wells. "Most Major Outlets Have Used Russian Tweets as Sources for Partisan Opinion: Study." *Columbia Journalism Review,* March 8, 2018. https://www.cjr.org/analysis/tweets-russia-news.php.

Lukito, Josephine, Chris Wells, Yini Zhang, Larisa Doroshenko, Sang Jung Kim, Min-Hsin Su, Jiyoun Suk, Yiping Xia, and Deen Freelon. *The Twitter Exploit: How Russian Propaganda Infiltrated U.S. News*. University of Wisconsin Social Media and Democracy Research Group, February 2018. https://uwmadison.app.box.com/v/TwitterExploit.

Lytvynenko, Jane. "InfoWars Has Republished More Than 1,000 Articles from RT without Permission." *BuzzFeed*, November 8, 2017. https://www.buzzfeed.com/janelytvynenko/infowars-is-running-rt-content.

Mathews, P., L. Mitchell, G. Nguyen, and N. Bean. "The Nature and Origin of Heavy Tails in Retweet Activity." In *Proceedings of the 26th International Conference on World Wide Web Companion,* Perth, Australia, April 2017, 1493–98.

McKew, Molly K. *The Scourge of Russian Propaganda: Evaluating Russian Information Warfare and Shaping the American Response.* Testimony submitted to the Commission on Security and Cooperation in Europe (a.k.a. the U.S. Helsinki Commission). September 14, 2017. https://www.csce.gov/sites/helsinkicommission.house.gov/files/III.b.%20Molly%20McKew%20Testimony.pdf.

McMillan, Robert, and Shane Harris. "Facebook Cut Russia Out of April Report on Election Influence." *Wall Street Journal,* October 5, 2017. https://www.wsj.com/articles/facebook-cut-russia-out-of-april-report-on-election-influence-1507253503.

"Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs." In *Security Awareness in the 1980s: Feature Articles from the Security Awareness Bulletin, 1981 to 1989*. Diane Publishing, 1991. https://books.google.com/books?id=2wNgbdnKuKAC&pg=PA15.

Meyer, Robinson. "Why It's Okay to Call It Fake News." *Atlantic,* March 9, 2018. https://www.theatlantic.com/technology/archive/2018/03/why-its-okay-to-say-fake-news/555215/.

Michel, Casey. "How Russia Created the Most Popular Texas Secession Page on Facebook." *Extra Newsfeed,* September 7, 2017. https://extranewsfeed.com/how-russia-created-the-most-popular-texas-secession-page-on-facebook-fd4dfd05ee5c.

Narayanan, Vidya, Vlad Barash, John Kelly, Bence Kollanyi, Lisa-Maria Neudert, and Philip N. Howard. *Polarization, Partisanship and Junk News Consumption over Social Media in the US.* Data Memo 2018.1. Oxford, UK: Oxford Internet Institute, February 6, 2018. https://arxiv.org/pdf/1803.01845.pdf.

North Atlantic Treaty Organization (NATO). "Robotrolling 1/2017." 2017. http://www.stratcomcoe.org/robotrolling-20171.

Nyhan, B., and J. Reifler. "When Corrections Fail: The Persistence of Political Misperceptions." *Political Behavior* 32, no. 2 (June 2010): 303–30.

Nyhan, B., E. Porter, J. Reifler, and T. J. Wood. "Taking Corrections Literally but Not Seriously? The Effects of Information on Factual Beliefs and Candidate Favorability." 2017.

Oentaryo, Richard J., Arinto Murdopo, Philips K. Prasetyo, and Ee-Peng Lim. "On Profiling Bots in Social Media." *Social Informatics*. Lecture Notes in Computer Science 10046 (2016): 92–109. https://link.springer.com/chapter/10.1007/978-3-319-47880-7_6.

Office of the Director of National Intelligence. "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution." January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Orr, Caroline. "How Russian & Alt-Right Twitter Accounts Worked Together to Skew the Narrative About Berkeley." *Arc Digital,* September 1, 2017. https://arcdigital.media/how-russian-alt-right-twitter-accounts-worked-together-to-skew-the-narrative-about-berkeley-f03a3d04ac5d.

Paquet-Clouston, Masarah, Olivier Bilodeau, and David Décary-Hétu. "Can We Trust Social Media Data? Social Network Manipulation by an IoT Botnet." *Proceedings of the 8th International Conference on Social Media & Society.* Toronto, Canada, July 2017. https://dl.acm.org/citation.cfm?id=3097301.

Paul, Christopher, and Miriam Matthews. "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It." Santa Monica, California: Rand Corporation, 2016. http://www.rand.org/pubs/perspectives/PE198.html.

Peisakhin, Leonid, and Arturas Rozenas. "Electoral Effects of Biased Media: Russian Television in Ukraine." *American Journal of Political Science* 62, no. 3 (July 2018): 535–50. https://onlinelibrary.wiley.com/doi/epdf/10.1111/ajps.12355.

Pennycook, G., T. D. Cannon, and D. G. Rand. "Prior Exposure Increases Perceived Accuracy of Fake News." Forthcoming in *Journal of Experimental Psychology: General*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958246.

Penzenstadler, Nick, Brad Heath, and Jessica Guynn. "We Read Every One of the 3,517 Facebook Ads Bought by Russians. Here's What We Found." *USA Today*, May 11, 2018. https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/.

Pirrong, Craig. "How Do You Know That Zero Hedge Is a Russian Information Operation? Here's How." *Streetwise Professor* (blog), November 20, 2014. http://streetwiseprofessor.com/?p=8947.

Popken, Ben. "Russian Trolls Duped Global Media and Nearly 40 Celebrities." NBC News, November 3, 2017. https://www.nbcnews.com/tech/social-media/trump-other-politicians-celebs-shared-boosted-russian-troll-tweets-n817036.

Poulsen, Kevin, and Spencer Ackerman. " 'Lone DNC Hacker' Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer." *Daily Beast*, March 22, 2018. https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer.

Rangappa, Asha. "How Facebook Changed the Spy Game." *Politico Magazine,* September 8, 2017. http://www.politico.com/magazine/story/2017/09/08/how-facebook-changed-the-spy-game-215587.

Rid, Thomas. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*. Testimony in front of the Senate Select Committee on Intelligence, March 30, 2017. https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf.

Roeder, Oliver. "Why We're Sharing 3 Million Russian Troll Tweets." *Fivethirtyeight*, July 31, 2018. https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/.

Rosenberg, Eli. "Twitter to Tell 677,000 Users They Were Had by the Russians. Some Signs Show the Problem Continues." *Washington Post*, January 19, 2018. https://www.washingtonpost.com/news/the-switch/wp/2018/01/19/twitter-to-tell-677000-users-they-were-had-by-the-russians-some-signs-show-the-problem-continues/

Rotenberg, Becca. "Russian Politician Says on Live TV that Russia Stole U.S. Presidency." *Axios*, September 11, 2017. https://www.axios.com/russian-politician-says-russia-stole-u-s-presidency-on-live-tv-2484056561.html.

Schudson, Michael, and Barbie Zelizer, eds. *Understanding and Addressing the Disinformation Ecosystem*. Annenberg School of Communication at the University of Pennsylvania, Philadelphia, PA, December 15-16, 2017. https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v2.pdf.

Seetharaman, Deepa. "Russian-Backed Facebook Accounts Staged Events around Divisive Issues." *Wall Street Journal*, October 30, 2017. https://www.wsj.com/articles/russian-backed-facebook-accounts-organized-events-on-all-sides-of-polarizing-issues-1509355801.

Shane, Scott. "From Headline to Photograph, a Fake News Masterpiece." *New York Times,* January 18, 2017. https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html.

Shane, Scott. "Mystery of Russian Fake on Facebook Solved, by a Brazilian." *New York Times*, September 13, 2017. https://www.nytimes.com/2017/09/13/us/politics/russia-facebook-election.html.

Shane, Scott, and Mike Isaac. "Facebook to Turn Over Russian-Linked Ads to Congress." *New York Times*, September 21, 2017. https://www.nytimes.com/2017/09/21/technology/facebook-russian-ads.html.

Shao, Chengcheng, Giovanni Luca Ciampaglia, Alessandro Flammini, and Filippo Menczer. "Hoaxy: A Platform for Tracking Online Misinformation." *Proceedings of the 25th International Conference Companion on World Wide Web*, Montreal, Canada, April 2016: 745–50. https://arxiv.org/abs/1603.01511.

Shao, Chengcheng, Giovanni Luca Ciampaglia, Onur Varol, Kaicheng Yang, Alessandro Flammini, and Filippo Menczer. "The Spread of Low-Credibility Content by Social Bots." July 24, 2017. https://arxiv.org/pdf/1707.07592.pdf.

Shao, Chengcheng, Pik-Mai Hui, Lei Wang, Xinwen Jiang, Alessandro Flammini, Filippo Menczer, and Giovanni Luca Ciampaglia. "Anatomy of an Online Misinformation Network." *PLOS One* 13, no. 4 (April 2018). http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0196087.

Shearer, Elisa, and Jeffrey Gottfried. "News Use across Social Media Platforms 2017." Pew Research Center, September 7, 2017. http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

Silverman, Craig. "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook." *BuzzFeed,* November 16, 2016. https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook.

Silverman, Craig, and Lawrence Alexander. "How Teens in the Balkans Are Duping Trump Supporters with Fake News." *BuzzFeed*, November 3, 2016. https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.

Snegovaya, Maria. *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*. Institute for the Study of War, September 2015. http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

Spencer, D. R. *The Yellow Journalism: The Press and America's Emergence as a World Power*. Evanston, IL: Northwestern University Press, 2007.

Stamos, Alex. "An Update on Information Operations on Facebook." Facebook Newsroom, September 6, 2017. https://newsroom.fb.com/news/2017/09/information-operations-update/.

Starbird, Kate. "Examining the Alternative Media Ecosystem through the Production of Alternative Narratives of Mass Shooting Events on Twitter." *Proceedings of the Eleventh International AAAI Conference on Web and Social Media (ICWSM 2017),* Montreal, Canada, May 2017. https://faculty.washington.edu/kstarbi/Alt_Narratives_ICWSM17-CameraReady.pdf.

Starbird, Kate. "Information Wars: A Window into the Alternative Media Ecosystem." *Design Use Build,* March 14, 2017. https://medium.com/hci-design-at-uw/information-wars-a-window-into-the-alternative-media-ecosystem-a1347f32fd8f.

Starbird, Kate, Ahmer Arif, Tom Wilson, Katherine Van Koevering, Katya Yefimova, and Daniel Scarnecchia. "Ecosystem or Echo-System? Exploring Content Sharing across Alternative Media Domains." *Proceedings of the Twelfth International AAAI Conference on Web and Social Media*, Palo Alto, CA, June 2018. https://faculty.washington.edu/kstarbi/Starbird-et-al-ICWSM-2018-Echosystem-final.pdf.

Stewart, Leo G., Ahmer Arif, and Kate Starbird. "Examining Trolls and Polarization with a Retweet Network." Presented at MIS2: Misinformation and Misbehavior Mining on the Web, workshop held in Los Angeles, CA, February 2018. https://faculty.washington.edu/kstarbi/examining-trolls-polarization.pdf.

Stone, Peter, and Greg Gordon. "FBI's Russian-influence Probe Includes a Look at Breitbart, InfoWars News Sites." *McClatchy,* March 20, 2017. http://www.mcclatchydc.com/news/politics-government/white-house/article139695453.html.

Stukal, Denis, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker. "Detecting Bots on Russian Political Twitter." *Big Data* 5, no. 4 (December 2017): 310–24. https://www.liebertpub.com/doi/full/10.1089/big.2017.0038.

Subramanian, Samanth. "Inside the Macedonian Fake News Complex." *Wired,* February 15, 2017. https://www.wired.com/2017/02/veles-macedonia-fake-news/.

Sydell, Laura. "We Tracked Down a Fake-News Creator in the Suburbs. Here's What We Learned." NPR, November 23, 2016. http://www.npr.org/sections/alltechconsidered/2016/11/23/503146770/npr-finds-the-head-of-a-covert-fake-news-operation-in-the-suburbs.

Tandoc Jr., Edson C., Zhang Wei Lim, and Richard Ling. "Defining 'Fake News': A Typology of Scholarly Definitions." *Digital Journalism* 6, no. 2 (2017): 137–53. http://www.tandfonline.com/doi/abs/10.1080/21670811.2017.1360143.

Tau, Byron, and Rebecca Ballhaus. "Israeli Intelligence Firm's Election-Meddling Analysis Comes under Mueller's Scrutiny." *Wall Street Journal,* May 25, 2018. https://www.wsj.com/articles/israeli-intelligence-firms-election-meddling-analysis-comes-under-muellers-scrutiny-1527288767.

Thorson, E. "Belief Echoes: The Persistent Effects of Corrected Misinformation." *Political Communication* 33, no. 3 (2016): 460–80.

Tiku, Nitasha. "How Russia 'Pushed Our Buttons' with Fake Online Ads." *Wired,* November 3, 2017. https://www.wired.com/story/how-russia-pushed-our-buttons-with-fake-online-ads/.

Tucker, Joshua A., Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*. William and Flora Hewlett Foundation report, March 2018. https://www.hewlett.org/library/social-media-political-polarization-political-disinformation-review-scientific-literature/.

Twitter. "Update: Russian Interference in the 2016 US Presidential Election." Blog post, September 28, 2017. https://blog.twitter.com/official/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html.

Vargo, Chris J., Lei Guo, and Michelle A. Amazeen. "The Agenda-Setting Power of Fake News: A Big Data Analysis of the Online Media Landscape from 2014 to 2016. *New Media & Society* 20, no. 5: 2028–49. First published June 15, 2017. http://journals.sagepub.com/doi/abs/10.1177/1461444817712086.

Varol, O., E. Ferrara, F. Menczer, and A. Flammini. "Early Detection of Promoted Campaigns on Social Media." *EPJ Data Science* 6, no. 13 (July 2017). https://doi.org/10.1140/epjds/s13688-017-0111-y.

Del Vicario, Michela, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H. Eugene Stanley, and Walter Quattrociocchi. "The Spreading of Misinformation Online." *PNAS* 113, no. 3 (January 2016): 554–59. http://www.pnas.org/content/113/3/554.

Volz, Dustin, and Joseph Menn. "Twitter Suspends Russia-Linked Accounts, but U.S. Senator Says Response Inadequate." Reuters, September 28, 2017. https://www.reuters.com/article/us-usa-trump-russia-twitter/twitter-suspends-russia-linked-accounts-but-u-s-senator-says-response-inadequate-idUSKCN1C331G.

Vosoughi, Soroush, Deb Roy, and Sinan Aral. "The Spread of True and False News Online." *Science* 359, no. 6380 (March 2018): 1146–51.

Waltzman, Rand. *The Weaponization of Information: The Need for Cognitive Security*. Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity, April 27, 2017. https://www.rand.org/pubs/testimonies/CT473.html.

Wang, Selina. "How the Kremlin Tried to Pose as American News Sites on Twitter." *Bloomberg*, December 5, 2017. https://www.bloomberg.com/news/articles/2017-12-05/how-the-kremlin-tried-to-pose-as-american-news-sites-on-twitter.

Ward Jr., J. H. "Hierarchical Grouping to Optimize an Objective Function." *Journal of the American Statistical Association* 58, no. 301 (1963): 236–44.

Warzel, Charlie. "New Charts Show What the Russian Troll @TEN_GOP Account Was Tweeting This Summer." *BuzzFeed,* October 24, 2017. https://www.buzzfeed.com/charliewarzel/new-charts-show-what-the-russian-troll-tengop-account-was.

Watts, Clint. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*. Testimony in front of the Senate Select Committee on Intelligence, March 30, 2017. https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf.

Webster, S. W., and A. I. Abramowitz. "The Ideological Foundations of Affective Polarization in the U.S. Electorate." *American Politics Research* 45, no. 4 (2017): 621–47.

Weedon, Jen, William Nuland, and Alex Stamos. "Information Operations and Facebook." Facebook report. April 27, 2017, version 1.0. https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

Weeks, B. E., and R. L. Holbert. "Predicting Dissemination of News Content in Social Media: A Focus on Reception, Friending, and Partisanship." *Journalism & Mass Communication Quarterly* 90, no. 2 (2013), 212–32.

Weisburd, Andrew, and Clint Watts. "How Russia Dominates Your Twitter Feed to Promote Lies (and Trump Too)." *Daily Beast,* August 16, 2016. http://www.thedailybeast.com/how-russia-dominates-your-twitter-feed-to-promote-lies-and-trump-too.

Wojcik, Stefan, Solomon Messing, Aaron Smith, Lee Rainie, and Paul Hitlin. "Bots in the Twittersphere." Pew Research Center, April 9, 2018. http://www.pewinternet.org/2018/04/09/bots-in-the-twittersphere/.

Woolley, Samuel C. "The Political Economy of Bots: Theory and Method in the Study of Social Automation." In *The Political Economy of Robots*, edited by Ryan Kiggins, 127–55. Palgrave Macmillan, Cham, 2018. https://link.springer.com/book/10.1007%2F978-3-319-51466-6.

Woolley, Samuel C., and Philip N. Howard, eds. "Computational Propaganda Worldwide: Executive Summary." Oxford, UK: Project on Computational Propaganda, July 2017. http://comprop.oii.ox.ac.uk/2017/06/19/computational-propaganda-worldwide-executive-summary/.

Notes

1 Edson C. Tandoc Jr., Zhang Wei Lim, and Richard Ling, "Defining 'Fake News': A Typology of Scholarly Definitions," *Digital Journalism* 6, no. 2 (2017): 137–53, http://www.tandfonline.com/doi/abs/10.1080/21670811.2017.1360143.

2 Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook," *BuzzFeed*, November 16, 2016, https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook.

3 Craig Silverman and Lawrence Alexander, "How Teens in the Balkans Are Duping Trump Supporters with Fake News," *BuzzFeed*, November 3, 2016, https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo. On the fake news industry in Veles, Macedonia, see also Emma Jane Kirby, "The City Getting Rich from Fake News," BBC, December 5, 2016, http://www.bbc.com/news/magazine-38168281, and Samanth Subramanian, "Inside the Macedonian Fake News Complex," *Wired*, February 15, 2017, https://www.wired.com/2017/02/veles-macedonia-fake-news/.

4 Laura Sydell, "We Tracked Down a Fake-News Creator in the Suburbs. Here's What We Learned," NPR, November 23, 2016, http://www.npr.org/sections/alltechconsidered/2016/11/23/503146770/npr-finds-the-head-of-a-covert-fake-news-operation-in-the-suburbs.

5 Scott Shane and Mike Isaac, "Facebook to Turn Over Russian-Linked Ads to Congress," *New York Times*, September 21, 2017, https://www.nytimes.com/2017/09/21/technology/facebook-russian-ads.html.

6 Andrew Higgins, "Fake News, Fake Ukrainians," *New York Times*, February 17, 2017, https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html.

7 Byron Tau and Rebecca Ballhaus, "Israeli Intelligence Firm's Election-Meddling Analysis Comes under Mueller's Scrutiny," *Wall Street Journal*, May 25, 2018.

8 David Lazer et al., "Combating Fake News: An Agenda for Research and Action," May 2017, https://www.hks.harvard.edu/publications/combating-fake-news-agenda-research-and-action.

9 Robert M. Faris et al., *Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election* (Berkman Klein Center for Internet & Society Research Paper, 2017), https://dash.harvard.edu/bitstream/handle/1/33759251/2017-08_electionReport_0.pdf. See also Chengcheng Shao et al., "Anatomy of an Online Misinformation Network," *PLOS One* 13, no. 4 (April 2018), http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0196087.

10 Eli Rosenberg, "Twitter to Tell 677,000 Users They Were Had by the Russians. Some Signs Show the Problem Continues," *Washington Post*, January 19, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/01/19/twitter-to-tell-677000-users-they-were-had-by-the-russians-some-signs-show-the-problem-continues/.

11 Tim Lister, Jim Sciutto, and Mary Ilyushina, "Putin's 'Chef,' the Man behind the Troll Factory," CNN, October 17, 2017, https://www.cnn.com/2017/10/17/politics/russian-oligarch-putin-chef-troll-factory/index.html.

12 Mike Isaac and Daisuke Wakabayashi, "Russian Influence Reached 126 Million Through Facebook Alone," *New York Times*, October 30, 2017. https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

13 Deepa Seetharaman, "Russian-Backed Facebook Accounts Staged Events around Divisive Issues," *Wall Street Journal*, October 30, 2017, https://www.wsj.com/articles/russian-backed-facebook-accounts-organized-events-on-all-sides-of-polarizing-issues-1509355801; see also Leo G. Stewart, Ahmer Arif, and Kate Starbird, "Examining Trolls and Polarization with a Retweet Network," paper presented at the MIS2: Misinformation and Misbehavior Mining on the Web workshop (Los Angeles, CA, February 2018), https://faculty.washington.edu/kstarbi/examining-trolls-polarization.pdf.

14 Lazer et al., "Combating Fake News."

15 D. R. Spencer, *The Yellow Journalism: The Press and America's Emergence as a World Power* (Evanston, IL: Northwestern University Press, 2007).

16 William Boyd, "The Secret Persuaders," *The Guardian*, August 19, 2006, https://www.theguardian.com/uk/2006/aug/19/military.secondworldwar.

17 "Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs," in *Security Awareness in the 1980s: Feature Articles from the Security Awareness Bulletin, 1981 to 1989* (Diane Publishing, 1991), https://books.google.com/books?id=2wNgbdnKuKAC&pg=PA15.

18 S. W. Webster and A. I. Abramowitz, "The Ideological Foundations of Affective Polarization in the U.S. Electorate," *American Politics Research* 45, no. 4 (2017): 621–47, and D. R. Kinder and N. P. Kalmoe, *Neither Liberal nor Conservative: Ideological Innocence in the American Public* (Chicago: University of Chicago Press, 2017).

19 Elisa Shearer and Jeffrey Gottfried, "News Use across Social Media Platforms 2017," Pew Research Center report, September 7, 2017, http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

20 For a good overview of research on disinformation and its relationship to polarization and supposed filter bubbles, see Joshua A. Tucker et al., *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature* (William and Flora Hewlett Foundation report, March 2018), https://www.hewlett.org/library/social-media-political-polarization-political-disinformation-review-scientific-literature/.

21 On filter bubbles, see for example R. Kelly Garrett and Natalie Jomini Stroud, "Partisan Paths to Exposure Diversity: Differences in Pro- and Counterattitudinal News Consumption," *Journal of Communication* 64, no. 4 (2014): 680–701, and Richard Fletcher and Rasmus Kleis Nielsen, "Are News Audiences Increasingly Fragmented? A Cross-National Comparative Analysis of Cross-Platform News Audience Fragmentation and Duplication," *Journal of Communication* 67, no. 4 (2017): 476–98. On one-sided information flows, see D. Chong and J. N. Druckman, "Dynamic Public Opinion: Communication Effects over Time," *American Political Science Review* 104, no. 4 (2010): 663–80.

22 B. Nyhan and J. Reifler, "When Corrections Fail: The Persistence of Political Misperceptions," *Political Behavior* 32, no. 2 (June 2010): 303–30, and G. Pennycook, T. D. Cannon, and D. G. Rand, "Prior Exposure Increases Perceived Accuracy of Fake News," forthcoming in *Journal of Experimental Psychology: General*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958246. Other research, though, has reached somewhat different conclusions, including B. Nyhan et al., "Taking Corrections Literally but Not Seriously? The Effects of Information on Factual Beliefs and Candidate Favorability," 2017, and Ullrich K. H. Ecker, Joshua L. Hogan, and Stephan Lewandowsky, "Reminders and Repetition of Misinformation: Helping or Hindering Its Retraction?" *Journal of Applied Research in Memory and Cognition* 6, no. 2 (2017): 185–192, https://www.sciencedirect.com/science/article/pii/S2211368116301838.

23 E. Thorson, "Belief Echoes: The Persistent Effects of Corrected Misinformation," *Political Communication* 33, no. 3 (2016): 460–80.

24 B. E. Weeks and R. L. Holbert, "Predicting Dissemination of News Content in Social Media: A Focus on Reception, Friending, and Partisanship," *Journalism & Mass Communication Quarterly* 90, no. 2 (2013), 212–32. On persuasion and social proof more generally, see R. B. Cialdini, "Harnessing the Science of Persuasion," *Harvard Business Review* 79, no. 9 (2001): 72–81.

25 Pennycook et al., "Prior Exposure."

26 Keir Giles, *Handbook of Russian Information Warfare*, NATO Defense College, 2016, http://www.ndc.nato.int/news/news.php?icode=995; see also Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Institute for the Study of War, September 2015, http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

27 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,' " *Foreign Policy*, March 5, 2018, http://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

28 Valery Gerasimov, "The Value of Science Is in the Foresight," originally published in *Military-Industrial Courier* (Voyenno-Promyshlennyy Kurier, Russia) February 27, 2013, translation published in *Military Review* (U.S.) January-February 2016, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf. See also Dmitry Gorenburg, "New Gerasimov Article on Nature of Warfare," *Russian Military Reform* (blog), March 17, 2017, https://russiamil.wordpress.com/2017/03/17/new-gerasimov-article-on-nature-of-warfare/.

29 Leonid Peisakhin and Arturas Rozenas, "Electoral Effects of Biased Media: Russian Television in Ukraine," *American Journal of Political Science* 62, no. 3 (July 2018): 535–50, https://onlinelibrary.wiley.com/doi/epdf/10.1111/ajps.12355.

30 Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It," Santa Monica, California: Rand Corporation, 2016, http://www.rand.org/pubs/perspectives/PE198.html; see also Geir H. Karlsen, "Tools of Russian Influence: Information and Propaganda," In *Ukraine and Beyond*, edited by Janne Haaland Matlary and Tormod Heier, 181–208 (Palgrave Macmillan, Cham, 2016).

31 Mike Isaac and Scott Shane, "Facebook's Russia-Linked Ads Came in Many Disguises," *New York Times*, October 2, 2017, https://www.nytimes.com/2017/10/02/technology/facebook-russia-ads-.html; Nitasha Tiku, "How Russia 'Pushed Our Buttons' with Fake Online Ads," *Wired*, November 3, 2017, https://www.wired.com/story/how-russia-pushed-our-buttons-with-fake-online-ads/; Nick Penzenstadler, Brad Heath, and Jessica Guynn, "We Read Every One of the 3,517 Facebook Ads Bought by Russians. Here's What We Found," *USA Today*, May 11, 2018, https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/.

32 Leo G. Stewart, Ahmer Arif, and Kate Starbird, "Examining Trolls and Polarization with a Retweet Network," presented at MIS2: Misinformation and Misbehavior Mining on the Web, workshop held in Los Angeles, CA, February 2018, https://faculty.washington.edu/kstarbi/examining-trolls-polarization.pdf.

33 Darren L. Linvill and Patrick L. Warren, "Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building," July 2018, http://pwarren.people.clemson.edu/Linvill_Warren_TrollFactory.pdf. See also Oliver Roeder, "Why We're Sharing 3 Million Russian Troll Tweets," *Fivethirtyeight*, July 31, 2018, https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/.

34 Samantha Bradshaw and Philip N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Working Paper 2017.12, Oxford Internet Institute, 2017. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf.

35 Tau and Ballhaus, "Israeli Intelligence Firm's Election-Meddling."

36 Sheera Frenkel and Nicholas Fandos, "Facebook Identifies New Influence Operations Spanning Globe," *New York Times*, August 21, 2018, https://www.nytimes.com/2018/08/21/technology/facebook-political-influence-midterms.html.

37 For a broader discussion of features that predict coordinated campaigns and inorganic mass posting, see O. Varol et al., "Early Detection of Promoted Campaigns on Social Media," *EPJ Data Science* 6, no. 13 (July 2017), https://doi.org/10.1140/epjds/s13688-017-0111-y.

38 Our definition here especially draws on Lazer et al., "Combating Fake News," and Lazer et al., "The Science of Fake News."

39 European Commission, *Final report of the High Level Expert Group on Fake News and Online Disinformation*, 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

40 David M. J. Lazer et al., "The Science of Fake News," *Science* 359, no. 6380 (March 2018): 1094–96, http://science.sciencemag.org/content/359/6380/1094. See also the discussion in Robinson Meyer, "Why It's Okay to Call It Fake News," *Atlantic*, March 9, 2018, https://www.theatlantic.com/technology/archive/2018/03/why-its-okay-to-say-fake-news/555215/.

41 See, for example, the discussion of fake news in Vidya Narayanan et al., *Polarization, Partisanship and Junk News Consumption over Social Media in the US*, Data Memo 2018.1, Oxford, UK: Oxford Internet Institute, February 6, 2018, https://arxiv.org/pdf/1803.01845.pdf. Junk news includes sensationalist and ultrapartisan content, and as a category is much broader than the content we study here.

42 On various scholarly definitions of fake news, see Tandoc et al., "Defining 'Fake News.' "

43 On the importance of focusing on the outlet rather than the news article level, see also Lazer et al., "The Science of Fake News."

44 See, for example, Giles, *Handbook of Russian Information Warfare,* and Snegovaya, *Putin's Information Warfare in Ukraine*.

45 Selina Wang, "How the Kremlin Tried to Pose as American News Sites on Twitter," *Bloomberg*, December 5, 2017, https://www.bloomberg.com/news/articles/2017-12-05/how-the-kremlin-tried-to-pose-as-american-news-sites-on-twitter.

46 On combining human control with automated posting in social media accounts, see Christian Grimme, Mike Preuss, Lena Adam, and Heike Trautmann, "Social Bots: Human-Like by Means of Human Control?" *Big Data 5*, no. 4 (2017): 279–93, https://www.liebertpub.com/doi/full/10.1089/big.2017.0044; see also NATO, "Robotrolling 1/2017."

47 While a comprehensive overview is beyond the scope of this paper, excellent places to start include E. Ferrara et al., "The Rise of Social Bots," *Communications of the ACM* 59, no. 7 (2016): 96–104; Chengcheng Shao et al., "The Spread of Low-Credibility Content by Social Bots," July 24, 2017, https://arxiv.org/pdf/1707.07592.pdf; and Samuel C. Woolley and Philip N. Howard, eds., "Computational Propaganda Worldwide: Executive Summary," Oxford, UK: Project on Computational Propaganda, July 2017, http://comprop.oii.ox.ac.uk/2017/06/19/computational-propaganda-worldwide-executive-summary/. On the role of Russian actors specifically, see Kate Starbird, "Examining the Alternative Media Ecosystem through the Production of Alternative Narratives of Mass Shooting Events on Twitter," *Proceedings of the Eleventh International AAAI Conference on Web and Social Media* (ICWSM 2017), Montreal, Canada, May 2017, https://faculty.washington.edu/kstarbi/Alt_Narratives_ICWSM17-CameraReady.pdf. The Senate Select Committee on Intelligence testimony of Clint Watts and Thomas Rid (*Disinformation*, March 30, 2017) is also a good primer on this subject.

48 Jen Weedon, William Nuland, and Alex Stamos, "Information Operations and Facebook," Facebook report, April 27, 2017, version 1.0, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf. See also Robert McMillan and Shane Harris, "Facebook Cut Russia Out of April Report on Election Influence," *Wall Street Journal*, October 5, 2017, https://www.wsj.com/articles/facebook-cut-russia-out-of-april-report-on-election-influence-1507253503.

49 Isaac and Wakabayashi, "Russian Influence."

50 *Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions*, United States Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, testimony of Sean J. Edgett, acting general counsel, Twitter Inc., October 31, 2017, https://www.judiciary.senate.gov/download/10-31-17-edgett-testimony. See also Rosenberg, "Twitter to Tell 677,000."

51 Dustin Volz and Joseph Menn, "Twitter Suspends Russia-Linked Accounts, but U.S. Senator Says Response Inadequate," Reuters, September 28, 2017, https://www.reuters.com/article/us-usa-trump-russia-twitter/twitter-suspends-russia-linked-accounts-but-u-s-senator-says-response-inadequate-idUSKCN1C331G.

52 For examples of this, see Kate Starbird, "Information Wars: A Window into the Alternative Media Ecosystem," *Design Use Build*, March 14, 2017, https://medium.com/hci-design-at-uw/information-wars-a-window-into-the-alternative-media-ecosystem-a1347f32fd8f, and Scott Shane, "Mystery of Russian Fake on Facebook Solved, by a Brazilian," *New York Times*, September 13, 2017, https://www.nytimes.com/2017/09/13/us/politics/russia-facebook-election.html.

53 For a good example of both the challenges of social bots, and new tools to help identify them, see Stefano Cresci et al., "The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race," *Proceedings of the 26th International Conference on World Wide Web Companion*, Perth, Australia, April 2017, 963–72, https://dl.acm.org/citation.cfm?id=3055135, and Grimme et al., "Social Bots."

54 Mike Kearney, Tweetbotornot: R package for detecting Twitter bots via machine learning [software package], 2018, https://github.com/mkearney/tweetbotornot. Also accessible at https://mikewk.shinyapps.io/botornot/. With May 2018 upgrades, the Botometer service now gives similar results to Tweetbotornot in most cases, something that was not true when this research was originally conducted.

55 For an example of how correlational patterns across accounts can help reveal bots, see Camille Francois, Vladimir Barash, and John Kelly, "Measuring Coordinated vs. Spontaneous Activity in Online Social Movements," 2017, https://osf.io/preprints/socarxiv/ba8t6/; and Nikan Chavoshi, Hossein Hamooni, and Abdullah Mueen, "Identifying Correlated Bots in Twitter," *Social Informatics*, Lecture Notes in Computer Science 10047 (2016): 14–21, https://link.springer.com/chapter/10.1007/978-3-319-47874-6_2.

56 Stefan Wojcik et al., "Bots in the Twittersphere," Pew Research Center, April 9, 2018, http://www.pewinternet.org/2018/04/09/bots-in-the-twittersphere/.

57 Shao et al., "Anatomy of an Online Misinformation Network."

58 T. M. Fruchterman and E. M. Reingold, "Graph Drawing by Force-directed Placement," *Software: Practice and Experience* 21, no. 11 (1991): 1129–64.

59 S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, "K-core Organization of Complex Networks," *Physical Review Letters* 96, no. 4 (February 2006). See also Alvarez-Hamelin et al., "K-core Decomposition of Internet Graphs: Hierarchies, Self-similarity and Measurement Biases," *Networks & Heterogeneous Media* 3, no. 2 (2008): 371–93, http://www.aimsciences.org/journals/displayArticles.jsp?paperID=3285.

60 J. H. Ward Jr., "Hierarchical Grouping to Optimize an Objective Function," *Journal of the American Statistical Association* 58, no. 301 (1963): 236–44.

61 For more detail on this methodology, see John W. Kelly, Valence graph tool for custom network maps, *U.S. Patent Application No. 14/101,811*, 2013.

62 Note that in statistical terms, CFI scores are equivalent to F-statistics.

63 Sampling variation suggests a 95 percent confidence interval of 58-68 percent in this sample, extending these results to the entire sample. However, sampling variation is not the only source of error. Kearney reports that the classifier is roughly 93 percent accurate overall on validation data, but we would expect slightly lower accuracy in applying the model to out-of-sample data sets like ours.

64 On the Internet Research Agency see Adrian Chen, "The Agency," *New York Times Magazine*, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html, and Tim Lister, Jim Sciutto, and Mary Ilyushina, "Putin's 'Chef,' the Man behind the Troll Factory," CNN, October 17, 2017, https://www.cnn.com/2017/10/17/politics/russian-oligarch-putin-chef-troll-factory/index.html.

65 Some of the claims spread by The Real Strategy were libelous, and this likely contributed to the action taken against it by online platforms. For a good discussion of the uncertainty surrounding The Real Strategy's origins—and its associated botnet—see Starbird, "Information Wars," including replies to comments: https://medium.com/@katestarbird/when-we-went-to-track-identities-in-therealstrategy-botnet-looking-at-the-different-twitter-2b2477219a8c.

66 Replies to comments in Starbird, "Information Wars."

67 Rosenberg, "Twitter to Tell 677,000." As press reports have noted, some of these automated accounts may not have been run by the IRA directly.

68 Ben Popken, "Russian Trolls Duped Global Media and Nearly 40 Celebrities," NBC News, November 3, 2017, https://www.nbcnews.com/tech/social-media/trump-other-politicians-celebs-shared-boosted-russian-troll-tweets-n817036. See also Josephine Lukito et al., *The Twitter Exploit: How Russian Propaganda Infiltrated U.S. News*, University of Wisconsin Social Media and Democracy Research Group, February 2018, https://uwmadison.app.box.com/v/TwitterExploit.

69 Specifically, as of spring 2018 Twitter's rules prohibited "post[ing] multiple updates to a trending or popular topic with an intent to subvert or manipulate the topic to drive traffic or attention to unrelated accounts, products, services, or initiatives." Rules posted at https://help.twitter.com/en/rules-and-policies/twitter-rules.

70 "Internet Research Agency Indictment," US Department of Justice, February 16, 2018, https://www.justice.gov/file/1035477/download.

71 Kevin Poulsen and Spencer Ackerman, " 'Lone DNC Hacker' Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer," *Daily Beast*, March 22, 2018, https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer.

72 "Was Clinton Campaign Chairman John Podesta Involved in Satanic 'Spirit Cooking'?" fact check on Snopes.com, November 4, 2016, https://www.snopes.com/fact-check/john-podesta-spirit-cooking/.

73 The Syria Campaign, *Killing the Truth*; Starbird et al., "Ecosystem or Echo-system?"

74 On Zero Hedge, see Craig Pirrong, "How Do You Know That Zero Hedge Is a Russian Information Operation? Here's How," *Streetwise Professor* (blog), November 20, 2014, http://streetwiseprofessor.com/?p=8947; and Tracy Alloway and Luke Kawa, "Unmasking the Men behind Zero Hedge, Wall Street's Renegade Blog," *Bloomberg*, April 29, 2016, https://www.bloomberg.com/news/articles/2016-04-29/unmasking-the-men-behind-zero-hedge-wall-street-s-renegade-blog. On GlobalResearch, see Campbell Clark and Mark MacKinnon, "NATO Research Centre Sets Sights on Canadian Website over Pro-Russia Disinformation," *Globe and Mail*, November 17, 2017, https://www.theglobeandmail.com/news/world/nato-research-centre-sets-sights-on-canadian-website-over-pro-russian-disinformation/article37015521/.

75 Jane Lytvynenko, "InfoWars Has Republished More Than 1,000 Articles from RT without Permission," *BuzzFeed*, November 8, 2017, https://www.buzzfeed.com/janelytvynenko/infowars-is-running-rt-content.

76 Poulsen and Ackerman, " 'Lone DNC Hacker' Guccifer 2.0."

77 See, for example, Jessica Davies, "Facebook's European Media Chief: Fake News Is a 'Game of Whack-a-Mole,' " *Digiday*, January 12, 2017, https://digiday.com/uk/facebooks-european-media-chief-addresses-fake-news-game-whack-mole/.

John S. and James L. Knight Foundation
Suite 3300
200 South Biscayne Boulevard
Miami, FL 33131-2349
(305) 908-2600
knightfoundation.org