MediaWell

Research Review

Election Interference

October 22, 2019

Key Points:

- This review defines “election interference” as one country or group attempting to influence an election in another country.
- The people orchestrating election interference campaigns may be trying to influence results, or they may be simply trying to cast doubt on election processes themselves.
- It is important to distinguish between negative advertising, which can be intended to reduce turnout, and actual voter suppression efforts like voter ID laws. Negative advertising tends to have relatively minimal measurable effects.
- There’s little to no evidence that Russian manipulation on social media in the 2016 US election directly influenced any results, but disinformation campaigns can still have serious consequences for democracies (Benkler 2019, Karpf 2019).

The threat to elections

This literature review addresses the concept of election interference, specifically online or digital election interference. The phenomenon has gained a great deal of popular and scholarly attention in the last few years, particularly following the election of Donald Trump in the United States, the Brexit campaign, and accusations of foreign meddling in European elections (Tucker et al. 2018). However, as we discuss below, these issues are not limited to wealthy Western nations. Societies around the world are grappling with how to secure their elections.

This research review begins with a working definition of election interference, before discussing research on election interference techniques, their effectiveness, related concerns, and possible remedies.

Social scientists and civil society organizations have been analyzing the 2018 elections in Brazil, as well as recent and upcoming elections in India, South Africa, Nigeria, and elsewhere. As their findings emerge, we will update this research review with particular attention to countries, events, and trends in the Global South.

How do we define election interference?

Defining election interference is not as straightforward as it might seem. Elections and referendums inherently involve persuading voters to favor one candidate or position over another. As long as there have been elections, seemingly, there have been efforts at persuasion and manipulation that cross ethical and legal lines. Campaigns, candidates, and their allies have long employed tactics ranging from dishonest advertising to outright skullduggery. Long before personal computers and smartphones, governments sought to repress electorates or manipulate results within their own borders. Since the colonial era, countries have often interfered in elections in their colonies, client states, and regional rivals. According to one survey, the US and the USSR/Russia combined to intervene in nearly one in nine national elections worldwide between 1946 and 2000, with tactics ranging from campaign funding to threats or sabotage (Levin 2016).

In this light, where should researchers attempt to draw lines between dirty-politics-as-usual and election interference? Much of the scholarly attention in recent years has focused on potential foreign interference in the Brexit referendum (June 2016), US presidential election (November 2016), French presidential election (spring 2017), and other major political contests in wealthy Western nations. "Foreign interference" in many of these cases has come to mean state-sponsored interference efforts by the Russian government and its military intelligence service, the GRU. However, many of the same Russian techniques that we describe below are within reach of nonstate actors, as the widespread use of digital technologies has lowered the entry barrier for election espionage and manipulation.

Because of this growth in scholarship, for the purposes of this research review, we treat "election interference" as attempts by a foreign nation or outside group to manipulate opinion and sway results in another polity's election. This is in keeping with Martin and Shapiro's (2019) ongoing database of "foreign influence efforts," though not all of their identified campaigns targeted elections per se. This focus on foreign interference would exclude operations like the "fake news" network of Macedonian youth (Persily 2017; Tucker et al. 2018; Silverman and Alexander 2016; Subramanian 2017) who worked to enrich themselves with ad revenue, but would include similar, contracted "service provider" efforts that were financed by a government.

However, we also follow Applebaum et al. (2017, 20) in noting that the idea of "inside" and "outside" actors is becoming more and more complicated. In a report, Applebaum et al. point to a "rapid expansion of transnational networks of disinformation and toxic speech," networks that combine both state and nonstate actors with "rapidly shifting alliances." As research coalesces around these trends, we may expand our definition of election interference. Our research review on "Producers of Disinformation" discusses scholarship

on disinformation more broadly, including political and commercial motivations.

It is also important to differentiate between negative advertising—which can be intended to reduce turnout—and actual voter suppression efforts like discriminatory laws, purged rolls, and tricks like those designed to fool voters into trying to vote by text message (Levine 2018). In the United States, concrete forms of voter suppression such, as photo ID laws that target poor and minority voters, are often justified with partisan claims of "voter fraud" and ballot tampering, claims that historically have been almost entirely unjustified (Bump 2019; Waldman 2018). Voter suppression is sometimes conflated with negative advertising in both popular conversation and academic writing. Despite the prevalence—one might even say ubiquity—of negative advertising and accompanying hand-wringing over the decline of public discourse, evidence indicates that negative advertising has little effect on voter behavior and turnout (Brooks 2006; Lau, Sigelman, and Rovner 2007; Malloy and Pearson-Merkowitz 2016; compare Krupnikov 2014, who argues that effects vary with context). What we do not yet know is whether online disinformation campaigns as an election interference strategy are more like negative advertising in their effects—relatively minimal—or if they need to be considered alongside more material voter suppression tactics.

This leads us to one important caveat about digital election interference. As yet, we have no idea whether or not such campaigns have ever swung an election, just as we still don't know if online political advertising actually works (Fowler, Franz, and Ridout, forthcoming). Given the extreme difficulty of measuring things like audience exposure to information and voter behavior, we may never know how effective disinformation campaigns can be. It is entirely possible that disinformation campaigns have not had any meaningful effect on elections and that their primary result has been to distract us from other problems and further poison polarized political processes. As societies, we have not yet established the appropriate levels of concern over our (undeniably problematic) poisoned information environments. If we ascribe too much power to producers of disinformation, are we actually furthering their goals?

Is election interference happening?

Under our working definition, cross-border election interference is certainly occurring in a variety of global contexts. Russia has been accused of attempting to polarize electorates and manipulate elections and referendums in the United States, France, and Britain (Brattberg and Maurer 2018). Further, Iran has been accused of trying to polarize US voters and mount disinformation campaigns targeted at regional rivals (FireEye 2018), while news reports have said China has sought to undermine officials and elections in Taiwan (Follain, Lin, and Ellis 2018; Martin and Shapiro 2019; Rogin 2018). In their database compiled from

news media reports, Martin and Shapiro (2019) identified 53 foreign influence efforts aimed at 24 countries from 2013 to 2018, with nearly 40 percent aimed at the United States. Again, not all of those campaigns specifically targeted elections, but Martin and Shapiro's database indicates the known scale of the problem.

It also seems likely that the field of election interference will widen. Freelance "service providers" with experience in dark-web operations, counterfeit pharmaceutical sales, and online ad fraud could put election interference troll-farm tactics within easy reach of smaller states and nonstate actors (Ferrara 2017). Political parties or interest groups could contract for short-term voter polarization or disinformation campaigns without the need to develop their own expertise or fund permanent operations.

It has been difficult for researchers to reach consensus on the specifics of foreign election interference, which are complicated by the question of intent, and by the opaque relationships between state and nonstate actors. For example, given the limited nature and effects of Russian trolling around Brexit, some observers argue that Russia was not engaged in a concerted attempt to interfere in the referendum despite opportunistic trolling with a pro-leave hashtag (Nimmo, Brookie, and Karan 2018). Similarly, there is less research consensus on whether the Kremlin attempted to interfere in the 2017 German elections. Through a combination of media monitoring and investigative journalism, Applebaum et al. (2017) found clear ideological bias from Kremlin-aligned German-language media outlets, which were consistently negative of parties and politicians other than the far-right AfD. Russian-controlled media pushed anti-immigration and election fraud conspiracy narratives, mirroring the nativist discourse in the US political scene. A pro-Kremlin botnet amplified AfD messaging mixed with commercial and pornographic content indicating that at least some accounts blend ideological and commercial motivations. Researchers contacted Russia-based freelance botnet operators who gave a price quote of €2,000 for a package of 15,000 tweets and retweets. On the other hand, Brattberg and Maurer (2018) found no reports of significant interference in Germany's election directed by the Russian government, speculating that despite having laid groundwork for a manipulation campaign, the Kremlin perhaps decided not to run the risk of damaging its relationship with Berlin.

In recent years, according to a report from security firm FireEye, web pages and social media accounts linked to Iran have published and disseminated information supportive of Iranian and Palestinian interests while denigrating Saudi Arabia, Israel and the Trump administration. Some accounts, pretending to be those of US leftists, urged support for Bernie Sanders and candidates aligned with him. The report cautioned, however, that the Iranian influence campaign did not appear to be solely designed to interfere in the 2018 US midterms, as it also targeted audiences and issues outside of US politics, such as support for Venezuelan leader Nicolás Maduro (FireEye 2018).

While interference campaigns aimed at Western democracies have attracted the most attention since 2016, there is growing concern that countries in the Global South will see effective disinformation campaigns aimed at their elections (Cunliffe-Jones 2018). Opponents of Jair Bolsonaro accused his backers of running a widespread and illegal disinformation campaign on WhatsApp leading up to the Brazilian election in late 2018 (Phillips 2018), though this disinformation campaign seems to have originated within the polity. India held general elections in 2019, and around a dozen presidential or general elections have taken place or are scheduled in African countries, including in Nigeria and South Africa, the continent's two largest economies (Cunliffe-Jones 2018; Tshabalala 2018).

What techniques have researchers identified?

Automated social media accounts—bots—are a crucial tool of contemporary political communication, including disinformation or propaganda campaigns (Woolley, forthcoming). Using data from network analysis company Graphika, Hindman and Barash (2018, 42) found that a "supercluster of densely interlinked, heavily followed accounts [played] a large role in the spread of fake news and disinformation on Twitter," and that many of those accounts kept operating despite clear evidence of their automation. Troll accounts and bot accounts also work to spread disinformation by linking to news and political content (Shao et al. 2018) and attempting to promote those URLs on platforms like Twitter, Reddit, and 4chan (Zannettou et al. 2018). However, the lines between fully automated bot accounts and human-directed troll accounts are looking more and more blurry as manipulators refine their techniques and platforms develop their countermeasures. Some "cyborg" accounts (Hindman and Barash 2018) are left automated for a while, then taken over by human agents before being automated again, either in attempts to evade platform countermeasures or to retarget bots toward different wedge issues.

Since online election interference takes place in the shadows, social science researchers have not typically had hard information on techniques. Much of what we know has been extrapolated from news reports and related intelligence agency releases; many of those, again, are centered on Russian interference in the 2016 US presidential election. Russian operatives are known to have employed a variety of tactics to sow divisions in the United States and support Trump's candidacy—without, perhaps, thinking he would actually win (Rutland 2017; compare Tucker et al. 2018). Notably, Russian operatives targeted the Democratic National Committee (DNC) and Clinton campaign chairman John Podesta with phishing attacks. Using stolen credentials, the GRU obtained and later released thousands of emails to the public through WikiLeaks (Marmura 2018; Riley and Robertson 2017).

Outside the United States, operatives thought to be Russian repeated the DNC-Podesta

strategy in 2017 in the French election ultimately won by Emmanuel Macron. They released nine gigabytes of stolen campaign information, timing the dump to coincide with the start of the pre-election campaign blackout period, though Macron's party was able to issue a statement shortly before the blackout period began (Baines and Jones 2018; Brattberg and Maurer 2018).

In another, broader strategy surrounding the 2016 US election, Russian trolls working at the country's Internet Research Agency (Ru-IRA) worked to increase polarization in the American electorate on social media. Researchers from the Oxford Internet Institute and Graphika found that the Ru-IRA encouraged "extreme right-wing voters to be more confrontational," among other strategies. The Ru-IRA efforts began on Twitter in 2013, but soon expanded to Facebook, YouTube, Instagram, and other platforms (Howard et al. 2018, 3). Ru-IRA operatives seem to have taken a highly opportunistic approach, applying themselves to both sides of various wedge issues and switching between topics to capitalize on current events (Nimmo, Brookie, and Karan 2018). In one polarization campaign, Russian troll accounts pushed both pro- and antivaccine narratives on social media, but without much uptake by other users (Broniatowski 2018; Broniatowski et al. 2018).

However, the Ru-IRA's efforts to increase polarization and sow dissension seem to have found more fertile ground in the United States' contentious race relations. Trolls bought Facebook ads, ran both pro–Black Lives Matter and Blue Lives Matter Twitter and Instagram accounts and pushed related narratives on both sides, building on an already divisive issue in American politics. Other efforts targeting black voters seem to have been designed to lower turnout, reduce support for Hillary Clinton, and increase dissatisfaction with the political process (DiResta et al. 2018; Howard et al. 2018; Nimmo 2018; Nimmo, Brookie, and Karan 2018; Stewart, Arif, and Starbird 2018).

In some respects, the early Russian troll operation led by the Internet Research Agency was fairly unsophisticated. Much of their accounts' activity was conducted during Russian business hours, and in some cases accounts that purported to belong to US users were registered with Russian telephone numbers (Giles 2016; Howard et al. 2018; Nimmo, Brookie, and Karan 2018; Timberg and Romm 2018). The Ru-IRA tweets consistently showed distinct stylistic and linguistic variations from tweets in the general population, suggesting that the operation was both carefully orchestrated to maximize its distribution of polarizing content on a budget, and relatively unconcerned with blending in (Boyd et al. 2018). It's also possible that the relatively visible nature of the Ru-IRA operation may have been calculated to distract from subtler and more effective initiatives (Giles 2016). In other words, the early troll farm was not intended to be highly covert operation, as opposed to the GRU hack of the Democratic National Committee, whose more sophisticated perpetrators made at least some effort to cover their tracks (Boyd et al. 2018).

Lastly, far-right political organizations are sharing political tactics and advice online across national borders. Far-right accounts that seemed to be US-based offered advice to German far-right accounts in "memetic warfare, fake account creation, parody accounts and obfuscation" (Applebaum et al. 2017).

How can we evaluate the effectiveness of such efforts?

It's important to note that we have little to no solid evidence that Russian bots or trolls on social media meaningfully affected voter behavior in the 2016 US election (Benkler 2019). (A caveat: That we *have* no firm evidence means only that—it does not mean that there *is* no firm evidence to be found.) However, as Dave Karpf writes (2019), "disinformation does not have to sway many votes to be toxic to democracy. The second-order effects undermine the democratic myths and governing norms that stand as a bulwark against elite corruption and abuse of power." The presence of election-related disinformation can have effects that go beyond the potential for disinformation to convince people of false information. In other words, disinformation doesn't need to "work" in order to be effective.

That said, it is helpful to know how effective election interference campaigns can be in order to direct mitigation efforts. Researchers have made a few recent attempts to assess the potential effectiveness of election interference campaigns, as well as how effective bots can be at either engaging humans in conversation or in disseminating messages. Many of the studies to date have involved Twitter, as it makes at least some data available to researchers in real time, while Facebook and other platforms present significant barriers to access. Some researchers have found that social media bots are not particularly good at engaging humans in conversation… at least not yet (Bessi and Ferrara 2016). However, bots are highly effective at disseminating information among human users, and some researchers have found that they tend to be used for amplification rather than argumentation. Bots are also growing more sophisticated (Howard and Kollanyi 2016; Ferrara et al. 2016). Tucker et al. (2018) argue more research is needed on bot-human interaction and human perception of bots across different topics such as entertainment versus politics.

Bessi and Ferrara (2016) analyzed tweets from 2.8 million accounts before the 2016 US election and concluded that perhaps as many as 400,000 were bots, and that those bots might be generating nearly 20 percent of the total messaging around the election. Notably, they found that tweets from Trump-supporting accounts were far more likely to contain positive messaging than tweets produced by Clinton supporters, and that bot accounts supporting Trump were the most positive in the researchers' data. They suggest that such dynamics can create an illusion of grassroots support despite an artificial origin.

A number of articles have focused on the roughly 2,700 Twitter accounts identified as Russian trolls by US congressional investigations. In a conference paper, Zannettou et al. (2018) identified tweets by accounts in the Twitter 1% Streaming API,[1] using those as their dataset to describe troll-account behaviors and attempting to estimate their effectiveness at steering narratives. They found that trolls had a limited ability to make news URLs go viral, though trolls were somewhat successful in promoting video news content from Russia Today. Zannettou et al. speculated that the troll accounts may have been more concerned with spreading divisive narratives and engaging other human users, relegating the task of news dissemination to the tens of thousands of bot accounts that Twitter had also identified. Badawy, Ferrara, and Lerman (2018) also took the 2,700 identified troll accounts as their starting position, and concluded that conservative users were about 31 times more likely to retweet Russian troll content than liberal users. Moreover, conservative users produced far more tweets than their liberal counterparts. Also drawing from the Twitter Streaming API and the set of identified Russian troll accounts for a conference paper, Stewart, Arif, and Starbird (2018, 4) found that the Russian content drawing on Black Lives Matter and Blue Lives Matter narratives circulated within distinct right-leaning and left-leaning audience clusters but rarely crossed them, and that the trolls' presence "implies a calculated entry into domestic issues with the intent to polarize and destabilize."

But while Russian troll and bot content resonated with some voters in the US elections, and did so along distinct, ideological lines, no evidence has yet emerged about how many votes that aspect of the Russian disinformation operation may have actually changed (DiResta et al. 2018; McKew 2018). As yet, social scientists have not established how effective social-media-based election interference tactics can be. Nimmo, Brookie, and Karan (2018) came to two conclusions—one, that trolls have been less effective than many have feared, and two, "that the most effective Russian trolls used exactly the techniques which drive genuine online activism and engagement. That made it much harder to separate them out from genuine users."

Evidence is still unfolding as to the extent of Russia's role in electing Donald Trump. Even Jamieson (2018), who makes a persuasive case in *Cyberwar* that Russia tipped the scales, says we will never know for sure how much of an effect their interference campaign had. Some argue that the most effective element of that interference was the hacking and release of the DNC-Podesta emails over WikiLeaks (Boot 2018), which, as *Washington Post* writer Philip Bump (2019) pointed out, relied not on social media but traditional media to spread and amplify the story. However, Jamieson's work stands in contrast to another recent, influential work on the 2016 election by Benkler, Faris, and Roberts (2018). In *Network Propaganda*, the authors argue that the media environment in the US leading up to the Trump election was the result of years in which the right-wing mediascape came to be

dominated by fiercely partisan and even extreme outlets and voices. Those sources were then amplified and legitimated by the right-leaning mainstream commercial news outlets—Fox News in particular (Benkler, Faris and Roberts 2018). As Kreiss (2019) points out, there is an as-yet unreconciled divide between these positions—Jamieson's work suggests that strengthening democracy against foreign interference is paramount, while Benkler, Faris, and Roberts argue for a recalibration of the domestic mediascape. *For further discussion of Benkler, Faris, and Roberts's work, see our research reviews on "Defining Disinformation."*

The US intelligence agencies, while accusing Russia, China, and Iran of meddling in the 2018 midterms, said they had not assessed those efforts' effectiveness (Landay and Hosenball 2018; Riechmann and Tucker 2018). Russia's continued efforts and refinements to its tactics would indicate that it believes its agents and techniques have potential. Other states, such as Iran, are employing similar tactics, all seemingly without significant geopolitical repercussions.

In part because it costs relatively little to run a disinformation and election interference campaign, some observers fear that such efforts will spread. Given the low cost and potential reward of mediated online election interference, it seems likely that such efforts will increase in coming years even without hard evidence of their effectiveness unless states are able to develop inoculations, countermeasures, or punishments.

What other concerns have emerged?

While this research review deals primarily with mediated forms of election interference, a few other approaches deserve mention, in part because they could be easily combined with mediated election interference and microtargeting. In recent years, scholars and security experts have voiced rising concern that electronic voting machines are susceptible to hacking and manipulation. In the United States, state and local jurisdictions employ a patchwork of equipment of various ages from a wide range of vendors. Security experts have described hypothetical attacks that could grant hackers access to voter registration databases, as well as voting machines and the back-end systems that manage them. Citing anonymous sources, a 2017 Bloomberg report said investigators had found evidence that Russian hackers targeted voting infrastructure in 39 US states. Elsewhere, Russian or Russia-aligned hackers have been implicated in or claimed responsibility for attacks on election systems in Ukraine and Bulgaria, including a virus designed to declare an incorrect winner (Riley and Robertson 2017; Norden and Vandewalker 2017; Hursti 2017). Crucially, such attacks need not affect election results or go undetected to be effective—coupled with a disinformation campaign on social media, a handful of prominent incursions in key races

might be enough to cast doubt on an entire electoral process. Even completely false claims of hacking or interference, if sufficiently amplified, may be enough to severely damage voter confidence (Fried 2018).

What remedies have been proposed?

A number of governments, particularly in Western Europe, are taking steps to protect their elections from future interference. Their efforts rely on a combination of technical steps, such as securing voting technology and infrastructure or, in the case of the Netherlands, manually counting votes and restricting election officials from using email or USB drives. IT personnel working for Macron's election campaign attempted to flood phishing attempts with real and fake credentials, and set up a system to feed bogus campaign information to attackers to devalue actual leaked documents (Brattberg and Maurer 2018).

Baines and Jones (2018) argue that NATO countries must build more robust capabilities for countering Russian influence, and that political parties and campaigns should be treated as critical infrastructure in the same way as utilities and transportation. They also call for "a more critical and resilient media and electorate." Broadly, Applebaum et al. (2017) recommend increased coordination and cooperation among civil society organizations and fact-checking groups. For the German case specifically, they suggest increased outreach to the Russian diasporic community, along with media literacy efforts.

Other observers have made a variety of recommendations, including nonelectronic voting, secure election result backups, hardened security for voting machines and registration databases, vulnerability analyses, voter education and awareness, and encouraging media organizations and social media platforms to be more proactive in fact-checking and fraud mitigation (Brattberg and Maurer 2018; Norden and Vandewalker 2017).

Emerging research questions

Research into these new forms of election interference is still in its infancy. Tucker et al. (2018) point to a large corpus of ethnographic work on the motivations of individual internet trolls. However, they note the lack of more systematic empirical research on troll behavior and motivations, and call as well for more research into automated detection measures.

Anthropologists and ethnographers of extremist political movements have not generally delved into those movements' online expressions, while on a more theoretical level, political scientists have not adapted traditional theories of states and publics to the transnational realities of the new disinformation networks.

We might plausibly divide the research questions regarding election interference into three general categories. The first involves the perpetrators and targets of election interference—who is interfering in whose elections, and how are they doing so? In many ways this is the easiest question to answer, as some social media platforms make some data available to researchers. Governments, journalists, and analysts also publish reports that provide the necessary geopolitical context.

A second general category asks how effective disinformation campaigns can be in actually changing voter behavior. This question is likely to be much harder to study. Isolating individual factors that influence voter behavior is notoriously difficult, as is assessing individuals' interpretation of and exposure to media messages. We look forward to seeing correlational studies, as well as research designs intended to identify causal relationships, in this area. On a related note, as discussed above, we have yet to determine the appropriate level of concern over these sorts of disinformation campaigns. Pollution of our information environment is a very real problem, but is there a risk that we might make the problem worse by overamplifying the threat and ascribing too much power to producers of disinformation?

The third category, research into potential inoculations and remedies, could have major policy implications. The large social media platforms are already engaged with this question, trying to reconcile increasing demands for intervention and accountability with business models that incentivize addictive content, homophily, and targeted advertising and influence. At the same time, the platforms frequently want to avoid governmental regulation. Researchers have opportunities to help inform platform and governmental responses with research projects that address improved bot detection; assess the effectiveness of fact-checking, voter education, and other interventions; and examine the consequences of exposure to fringe ideas.

Our grateful acknowledgement to Cody Buntain, David Karpf, and Kris-Stella Trump for their feedback during the writing process for this research review.

[1] See Steinert-Threlkeld 2018 for an explanation of how researchers can access random data from Twitter. https://www.cambridge.org/core/elements/twitter-as-data/27B3DE20C22E12E162BFB173C5EB2592/core-reader

Works Cited

Applebaum, Anne, Peter Pomerantsev, Melanie Smith, and Chloe Colliver. 2017. 'Make Germany Great Again' – Kremlin, Alt-Right and International Influences in the 2017 German

Elections. Institute for Strategic Dialogue. https://www.isdglobal.org/isd-publications/make-germany-great-again-kremlin-alt-right-and-international-influences-in-the-2017-german-elections/.

Badawy, Adam, Emilio Ferrara, and Kristina Lerman. 2018. "Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign." In *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 258–65. https://doi.org/10.1109/ASONAM.2018.8508646.

Baines, Paul, and Nigel Jones. 2018. "Influence and Interference in Foreign Elections." *The RUSI Journal* 163 (1): 12–19. https://doi.org/10.1080/03071847.2018.1446723.

Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.

Benkler, Yochai. 2019. Cautionary Notes on Disinformation and the Origins of Distrust. Social Science Research Council, MediaWell. https://mediawell.ssrc.org/expert-reflections/cautionary-notes-on-disinformation-benkler/

Bessi, Alessandro, and Emilio Ferrara. 2016. "Social Bots Distort the 2016 U.S. Presidential Election Online Discussion." *First Monday* 21 (11). https://doi.org/10.5210/fm.v21i11.7090.

Boot, Max. 2018. "Without the Russians, Trump Wouldn't Have Won." *Washington Post*, July 24, 2018, sec. Opinion. https://www.washingtonpost.com/opinions/without-the-russians-trump-wouldnt-have-won/2018/07/24/f4c87894-8f6b-11e8-bcd5-9d911c784c38_story.html.

Boyd, Ryan L., Alexander Spangher, Adam Fourney, Besmira Nushi, Gireeja Ranade, James Pennebaker, and Eric Horvitz. 2018. "Characterizing the Internet Research Agency's Social Media Operations During the 2016 U.S. Presidential Election Using Linguistic Analyses." Preprint, last edited October 1, 2018. https://osf.io/ajh2q.

Brattberg, Erik, and Tim Maurer. 2018. "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks." Carnegie Endowment for International Peace. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

Broniatowski, David. 2018. "Disinformation and American Politics and Policy Debates." Presented at *Contentious Narratives Part Two: Response Strategies to Disinformation Campaigns*, George Washington University, Washington, D.C., October 4. https://smpa.gwu.edu/contentious-narratives-0.

Broniatowski, David A., Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn, and Mark Dredze. 2018. "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate." *American Journal of Public Health* 108 (10): 1378–84. https://doi.org/10.2105/AJPH.2018.304567.

Brooks, Deborah Jordan. 2006. "The Resilient Voter: Moving Toward Closure in the Debate over Negative Campaigning and Turnout." *The Journal of Politics* 68 (3): 684–96. https://doi.org/10.1111/j.1468-2508.2006.00454.x.

Bump, Philip. 2019. "Analysis | A Resignation in Texas Is a Reminder of How Trump's Vote-Fraud Claims Come up Empty." *Washington Post*, May 28, 2019, sec. Politics. https://www.washingtonpost.com/politics/2019/05/28/resignation-texas-is-reminder-how-trumps-vote-fraud-claims-come-up-empty/.

Cunliffe-Jones, Peter. 2019. "The Focus of Misinformation Debates Shifts South." Nieman Lab (blog). 2019. http://www.niemanlab.org/2018/12/the-focus-of-misinformation-debates-shifts-south/.

DiResta, Renee, Kris Shaffer, Becky Ruppel, and David Sullivan. 2018. "The Tactics & Tropes of the Internet Research Agency." New Knowledge. https://www.newknowledge.com/articles/the-disinformation-report/.

Ferrara, Emilio. 2017. "Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election." *First Monday* 22 (8). https://doi.org/10.5210/fm.v22i8.8005.

Ferrara, Emilio, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. 2016. "The Rise of Social Bots." *Communications of the ACM*, July 2016.

FireEye. 2018. "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East." August 21, 2018. https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html.

Follain, John, Adela Lin, and Samson Ellis. 2018. "China Ramps Up Cyberattacks on Taiwan." *Bloomberg*, September 19, 2018. https://www.bloomberg.com/news/articles/2018-09-19/chinese-cyber-spies-target-taiwan-s-leader-before-elections.

Fowler, Erika Franklin, Michael M. Franz, and Travis N. Ridout. Forthcoming. "Online Political Advertising in the United States." In *Social Media and Democracy: The State of the Field and Prospects for Reform*, edited by Nathaniel Persily and Joshua A. Tucker.

Cambridge University Press.

Fried, Ina. 2018. “Tech Firms See Rise in False Claims of Election Interference.” *Axios*, November 5, 2018. https://www.axios.com/latest-election-scare-false-claims-of-interference-373d1db3-e1a8-4137-a8ca-6651e11c0322.html.

Giles, Keir. 2016. “The Next Phase of Russian Information Warfare.” NATO Strategic Communications Centre of Excellence. https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

Hindman, Matthew, and Vlad Barash. 2018. “Disinformation, ‘Fake News’ and Influence Campaigns on Twitter.” Knight Foundation. https://knightfoundation.org/reports/disinformation-fake-news-and-influence-campaigns-on-twitter.

Howard, Philip N., Barath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois. 2018. “The IRA and Political Polarization in the United States.” Oxford Internet Institute. https://comprop.oii.ox.ac.uk/research/ira-political-polarization/.

Howard, Philip N., and Bence Kollanyi. 2016. “Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum.” *SSRN*, June. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2798311.

Hursti, Harri. 2017. “DEF CON 25 Voting Village – Harri Hursti – Brief History of Election Machine Hacking.” Youtube video, October 18. https://www.youtube.com/watch?v=ImgaEqOQlSQ.

Jamieson, Kathleen Hall. 2018. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President – What We Don’t, Can’t, and Do Know*. Oxford University Press.

Karpf, David. 2019. On Digital Disinformation and Democratic Myths. Social Science Research Council, MediaWell. https://mediawell.ssrc.org/expert-reflections/on-digital-disinformation-and-democratic-myths/

Kreiss, Daniel. 2019. “From Epistemic to Identity Crisis: Perspectives on the 2016 U.S. Presidential Election.” *The International Journal of Press/Politics*, April, 1–6. https://doi.org/10.1177/1940161219843256.

Krupnikov, Yanna. 2014. “How Negativity Can Increase and Decrease Voter Turnout: The Effect of Timing.” *Political Communication* 31 (3): 446–66.

https://doi.org/10.1080/10584609.2013.828141.

Landay, Jonathan, and Mark Hosenball. 2018. “Russia, China, Iran Sought to Influence U.S. 2018 Elections: U.S Spy Chief.” *Reuters*, December 21, 2018. https://www.reuters.com/article/us-usa-election-interference-idUSKCN1OK2FS.

Lau, Richard R., Lee Sigelman, and Ivy Brown Rovner. 2007. “The Effects of Negative Political Campaigns: A Meta-Analytic Reassessment.” *Journal of Politics* 69 (4): 1176–1209. https://doi.org/10.1111/j.1468-2508.2007.00618.x.

Levin, Dov H. 2016. “When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results.” *International Studies Quarterly* 60 (2): 189–202. https://doi.org/10.1093/isq/sqv016.

Levine, Ally J. 2018. “The Informed Voter’s Guide to Making Sure Your Vote Counts.” *ProPublica*. October 30, 2018. https://projects.propublica.org/graphics/election-day-voting-guide.

Malloy, Liam C, and Shanna Pearson-Merkowitz. 2016. “Going Positive: The Effects of Negative and Positive Advertising on Candidate Success and Voter Turnout.” *Research & Politics* 3 (1): 1–15. https://doi.org/10.1177/2053168015625078.

Marmura, Stephen M. E. 2018. “WikiLeaks’ American Moment: The DNC Emails, Russiagate and Beyond.” In *The WikiLeaks Paradigm: Paradoxes and Revelations*, edited by Stephen M. E. Marmura, 109–33. Springer International Publishing. https://doi.org/10.1007/978-3-319-97139-1_6.

Martin, Diego A., and Jacob N. Shapiro. 2019. “Trends in Online Foreign Influence Efforts | Empirical Studies of Conflict.” ESOC Publications. Princeton University. https://esoc.princeton.edu/files/trends-online-foreign-influence-efforts.

McKew, Molly. 2018. “Did Russia Affect the 2016 Election? It’s Now Undeniable.” *Wired*, February 17, 2018. https://www.wired.com/story/did-russia-affect-the-2016-election-its-now-undeniable/.

Nimmo, Ben. 2018. “Another of the Most Effective Troll Reddit Accounts Was u/WhatImDoindHere, Which Was Anti-Black Lives Matter.” Tweet. @benimmo. https://twitter.com/benimmo/status/984372267722342401.

Nimmo, Ben, Graham Brookie, and Kanishk Karan. 2018. “#TrollTracker: Twitter’s Troll Farm Archives.” Digital Forensic Research Lab. DFRLab (blog). October 17, 2018. https://medium.com/dfrlab/trolltracker-twitters-troll-farm-archives-d1b4df880ec6.

Norden, Lawrence, and Ian Vandewalker. 2017. “Securing Elections From Foreign Interference.” Brennan Center for Justice. https://www.brennancenter.org/publication/securing-elections-foreign-interference.

Persily, Nathaniel. 2017. “The 2016 U.S. Election: Can Democracy Survive the Internet?” *Journal of Democracy* 28 (2): 63–76. https://doi.org/10.1353/jod.2017.0025.

Phillips, Tom. 2018. “Bolsonaro Business Backers Accused of Illegal Whatsapp Fake News Campaign.” *The Guardian*, October 18, 2018, sec. World news. https://www.theguardian.com/world/2018/oct/18/brazil-jair-bolsonaro-whatsapp-fake-news-campaign.

Riechmann, Deb, and Eric Tucker. 2018. “Russian Woman Charged with U.S. Election Interference through Social Media.” *Associated Press*, October 19, 2018. https://www.chicagotribune.com/news/nationworld/ct-russian-woman-charged-with-election-interference-20181019-story.html.

Riley, Michael, and Jordan Robertson. 2017. “Russian Hacks on U.S. Voting System Wider Than Previously Known.” *Bloomberg*, June 13, 2017. https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

Rogin, Josh. 2018. “China’s Interference in the 2018 Elections Succeeded — in Taiwan.” *Washington Post*, December 18, 2018. https://www.washingtonpost.com/opinions/2018/12/18/chinas-interference-elections-succeeded-taiwan/.

Rutland, Peter. 2017. “Trump, Putin, and the Future of US-Russian Relations.” *Slavic Review* 76 (S1): S41–56. https://doi.org/10.1017/slr.2017.157.

Shao, Chengcheng, Giovanni Luca Ciampaglia, Onur Varol, Kai-Cheng Yang, Alessandro Flammini, and Filippo Menczer. 2018. “The Spread of Low-Credibility Content by Social Bots.” *Nature Communications* 9 (1). https://doi.org/10.1038/s41467-018-06930-7.

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

Stewart, Leo G., Ahmer Arif, and Kate Starbird. 2018. “Examining Trolls and Polarization with a Retweet Network.” In *Proc. ACM WSDM, Workshop on Misinformation and Misbehavior Mining on the Web*.

https://faculty.washington.edu/kstarbi/examining-trolls-polarization.pdf.

Subramanian, Samanth. 2017. “Meet the Macedonian Teens Who Mastered Fake News and Corrupted the US Election.” *Wired*, February 15, 2017. https://www.wired.com/2017/02/veles-macedonia-fake-news/.

Timberg, Craig, and Tony Romm. 2018. “New Report on Russian Disinformation, Prepared for the Senate, Shows the Operation’s Scale and Sweep.” *Washington Post*, December 17, 2018. https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/.

Tshabalala, Tshepo. 2018. “Ahead of African Elections, Unlock Partnerships with Fact-Checkers.” Nieman Lab (blog). December 17, 2018. http://www.niemanlab.org/2018/12/ahead-of-african-elections-unlock-partnerships-with-fact-checkers/.

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

Waldman, Paul. 2018. “Looks like an Actual Case of Election Fraud Has Occurred. Guess Who’s Responsible.” *Washington Post*, December 5, 2018. https://www.washingtonpost.com/blogs/plum-line/wp/2018/12/05/looks-like-an-actual-case-of-election-fraud-has-occurred-guess-whos-responsible/?utm_term=.8c7ac76721ac.

Woolley, Samuel C. Forthcoming. “Bots and Computational Propaganda: Automation for Communication and Control.” In *Social Media and Democracy: The State of the Field and Prospects for Reform*, edited by Nathaniel Persily and Joshua A. Tucker. Cambridge University Press.

Zannettou, Savvas, Tristan Caulfield, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. 2018. “Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web.” In *Companion Proceedings of The 2019 World Wide Web Conference*. https://arxiv.org/abs/1801.09288.