(DIS)INFORMATION WARFARE:

THE 2016 ELECTION, RUSSIAN HACKERS, AND

U.S. DEMOCRATIC PRECARITY

by

EMILY A. FOWLER

A THESIS

Presented to the Department of Political Science
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Arts

Spring 2021

An Abstract of the Thesis of

Emily Fowler for the degree of Bachelor of Arts
in the Department of Political Science to be taken Spring 2021

(Dis)information Warfare:
The 2016 Election, Russian Hackers, and U.S. Democratic Precarity

Approved: _____*Daniel Tichenor, Ph.D.*_____
Primary Thesis Advisor

The 2016 election of Donald J. Trump irrevocably changed the course of American democracy by revealing the malevolent soft power of disinformation warfare in the American electoral system. Russian troll accounts operated by artificial intelligence bots systematically targeted voters on behalf of Mr. Trump to alter behavior and elicit polarizing reactions, cultivating his campaign of fearmongering and racism. Voters of color in key battleground districts—which won Mr. Trump the Electoral College—were marginalized through campaigns slandering Hillary Clinton's record with Black and Latinx voters. The 2019 special counsel report by Robert Mueller confirmed that Russian disinformation Internet trolls worked to sow discord within the American public in the 2016 election—but what does this reveal about the sustainable future of the United States' democracy as technology continues evolving? What do these campaigns reveal about the targeted audience for foreign actors and consulting firms?

Through my research, I aim to correlate the history of disinformation with the future development of artificial intelligent technologies. After closely examining the

impact of the Russian disinformation social media schemes in 2016, I will suggest techniques to better improve the sanctity of the electoral system. In a world continually fighting towards digital freedoms and data liberties, the United States must protect its citizens from election interference—without these precautions, hacking an election will only become easier.

Acknowledgements

Researching, writing, and completing a thesis is not an easy task, particularly during a year of profound political and cultural change. Without my formidable support system, this thesis would have been an even greater uphill battle.

First and foremost, I'd like to thank my thesis committee. Dan, thank you for your constant support, not only throughout this process, but over the past four years. For those of us lucky enough to work closely with you—be it through the Wayne Morse Center or the Political Science department—your wisdom, kindness, and encouragement nurtures us to be the greatest versions of ourselves and see the future as a blank canvass of our own creation. Professor Moffitt, your academic and professional mentorship has been a guiding light through a storm of my own ideas! Thank you for grounding my research in something more tangible. And Professor Lawrence, thank you for gracing my chaotic introductory email with patience and encouragement—your input has been consequential for this project, and I am incredibly grateful for your help.

A thesis is a marathon, not a sprint, and I'd like to thank the people who ran alongside and cheered me on over the past year. To Hunter Spence, my comrade throughout this process; your outstanding leadership preserves my optimism in a better future! To Siobhán Nolan, Gianna Genova, Drew Betts, and Zack Demars, thank you for sticking by my side and reminding me that I was capable. You're all stars, baby!

Finally, I'd like to thank my parents. You've taught me to believe in good, pursue kindness, and lead with courage. This education is the greatest gift anyone could have honored me with—everything would mean nothing without you.

Table of Contents

List of Figures

List of Tables

I. An Introduction

> We knew the 14 million people we needed to win 270. We targeted those in over 1000 different universes with exactly the things that mattered to them… We won exactly where we laid our money…Wisconsin, Michigan, Pennsylvania, Ohio.
>
> - Brad Parscale, digital director of the 2016 Trump campaign.[1]

American Politics in 2021

Democracy in the United States is in crisis. Between 2016 and 2021, the Capitol was sieged, an election was widely questioned by prominent lawmakers, and internal strife threatened to deteriorate any semblance of peace. Nationalism plagues American society, while the leftwing policy agenda of progressives has fueled conservative fears of an ever-growing government. And while an emergent population of Americans are adamant about dismantling racist institutions and finding reparations for Black Americans, a not-so-silent minority works towards preserving the historical legacies of slavery and Jim Crow. This profound division elevates political animosity to a level unseen in the United States since the Civil War.[2]

How did we get here? What led to the deep division between Americans on the left and right? Despite one's political affiliation or personal opinion of the Trump administration, the 2016 election of Donald J. Trump is widely regarded as the boiling point of contemporary American strife.[3] His administration marked a new chapter in Conservative politics and instigated a party realignment rapidly shifting mainstream Republican ideologies.

---

[1] Institute of Politics, Harvard Kennedy School. *Campaign for President.*
[2] Paisley, Laura. "Political polarization." 2016.
[3] Pew Research Center, "The Partisan Divide on Political Values Grows Even Wider." 2017.

The 2016 election was not an independent shift in American politics. Robert Mueller's 2019 special counsel investigation concluded that the Russian government successfully interfered in the election, heavily influencing Trump's eventual victory.[4] Mueller's report found that that the Russian government interfered in the election in three primary ways: creating social media bots to spread disinformation, hacking the Democratic National Committee, and hacking into local government electoral offices. While the Mueller Report found that all three methods contributed to Trump's victory, Russian weaponization of social media for disinformation marked a new era of government technology. Russia had been interfering in presidential and parliamentary elections globally since 1991, but never before had it advanced cyberattack technology in such a sophisticated and disturbing proportion.[5] Rather than chasing the market and lagging behind technology's rapid evolution, the Russian government championed malicious artificial intelligence (AI). These disinformation campaigns were used as information warfare to alter people's individual votes, but also to incite polarizing reactions.[6] By enabling more votes for Trump and cultivating his cult-like, alt-right rhetoric, Russian agents sought to create further systemic division in American politics.

As a political scientist interested in emerging technologies, the Trump election prompted a series of questions for my own scholarship. How has technology impacted democratic elections? What did the Russian disinformation campaigns reveal about the Kremlin's short-term and long-term interests in the United States? And what can be done to safeguard the sanctity of future democratic elections around the world from

[4] Mueller, Robert. Report on The Investigation into Russian Interference in the 2016. 2019.
[5] Kamarck, Elaine. Malevolent soft power, AI, and the threat to democracy. 2018.
[6] Ibid.

technical interference? This thesis attempts to bridge these questions and examine how disinformation spread through AI technologies, fulfilling a Russian interest in instigating animosity and internal strife in the United states.

2016 Election Interference

While Mueller was unable to determine Trump's potential involvement in the Russian scheme, reporters linked Trump's adversaries and campaign officials to Cambridge Analytica, a consulting firm that used leaked Facebook data to create individualized social media bots for most American voters to influence their political leanings in 2016.[7] The artificially intelligent robots gained insight from gargantuan databases of detailed personal data mined from Facebook to better target individual voters. While the precise number of bots operating in 2016 is still unknown, experts estimate that Cambridge Analytica created 220 million profiles for the bots to target.[8] These bots seemingly worked in tandem with the Russian disinformation bots—they both were personalized to individual voters, created to incite division, and succeeded at targeting key voters to influence swing districts.[9] While Russia faced little backlash for its interference tactics, Cambridge Analytica came under global scrutiny for its nefarious use of Facebook's data and led to many public officials interrogating the role of Big Tech in electoral politics.

My research will prove that these disinformation programs contributed to amplified national division. These technologies mobilized foundational Conservative voters—Evangelical Christians and rightwing veterans—to arrive in droves at the ballot

[7] Rosenberg, Matthew, et al. "How Trump Consultants Exploited the Facebook Data of Millions."
[8] Bergdahl, Jacob. "How AI Can Make You the President." 2019.
[9] Rosenberg.

box. They demobilized Black voters by spreading disinformation regarding Hillary Clinton's record with the Black Lives Matter campaigns and law enforcement policies. And the bots helped shift frustrated young progressives away from the Democratic base, instead voting for the Green Party's candidate, Jill Stein.[10]

These disinformation schemes revealed the malevolent soft power of artificial intelligence in the American electoral system. While the public may view the tech industry as a space filled by social media companies and Internet conglomerates, few understand the dark underbelly of these emerging technologies. Artificial intelligence remains essentially unregulated and unmonitored in 2021, despite its emergent role in everyday life. From online shopping to insurance quotes, artificial intelligence and machine learning technologies increasingly interact with users on an incredibly regular basis—typically multiple times each day. By wielding and dominating these technologies, the Russian government controlled the most insidious contemporary weapon against American democratic institutions to date.

Methodology and Terminology

Throughout the course of my thesis, I relied upon a wide plethora of prominent pundits in political science, computer science, and communications. These experts came from diverse backgrounds—many were investigative journalists, intelligence experts, academics, pollsters, programmers, or legal theorists. While I primarily synthesized and evaluated the findings of each of them in this piece, they conducted several various methods within their own research that is worth discussing.

[10] Kamarack.

A significant portion of my thesis relied upon Kathleen Hall Jamieson's book, *Cyberwar.* Jamieson, an acclaimed communications scholar from the University of Pennsylvania, conducted several telephone surveys, ultimately interviewing 2,021 U.S. adults during the 2016 election season to garner national opinions on Donald Trump and Hillary Clinton. These survey results were merged to test the aggregate differences within audiences, thus beginning to understand how media messaging shaped the way many adults viewed the candidates.[11] Similar polling methods were utilized by experts at the Pew Research Center, the *New York Times*, and *NBC News,* three institutions that aided my scholarship.

Many of the political scientists I evaluated utilized a process tracing methodology in their research. I framed much of my research around Elaine Kamarack's report, *Malevolent soft power, AI, and the threat to democracy,* published by the Brookings Institution. Kamarack used case studies to link possible causes of disinformation with observed outcomes of the 2016 election.[12] As did Adam Casey and Lucan Ahmad Way, two academics from the University of Toronto who collected evidence of Russian electoral interventions from 1991–2017.[13] Process tracing was a particularly useful method of analysis, as it allowed researchers to contextualize disinformation hypotheses with the real outcome of the election.

Most notably, I considered several congressional reports within my thesis as well. These reports—including the 2020 Select Committee on Intelligence report and the Mueller investigation report—utilized intelligence that would otherwise be

[11] Jamieson, Kathleen Hall. *Cybercrime.* 2018.
[12] Kamarack.
[13] Casey, Adam and Lucan Ahmad Way. "Russian Electoral." 2017.

inaccessible to me as a private citizen.[14] Many of the details around the 2016 election remain classified by foreign intelligence officials, state agencies, and tech companies.[15] This data was consequential to my research and allowed me to gain a more nuanced understanding of the disinformation campaigns, their effect on the American public, and what they symbolized for Russian foreign policy.

Paradigms in My Research

I also utilized a behaviorist model of analysis. Based on psychology, behaviorism postulates that human behavior is constantly conditioned by the media we ingest and our personal histories. In other words, humans will likely act in a similar way to the television shows, books, music, movies, periodicals, or social media they regularly consume, as long as it aligns with their historical experiences.[16] For example, a left-leaning woman who reads liberal newspapers and has experienced sexism in her lifetime is more likely to support a new bill created by a popular male Democrat, as the media she interacts with suggests that the politician is a feminist. Behaviorism theory argues that these conditions are manipulatable under a precise understanding of each person's identity and media consumption. If an instigator deeply understands a victim, it can easily influence the victim's actions.[17]

And finally, it is essential to distinguish between *misinformation* and *disinformation*. While misinformation is false information spread without poor intent, disinformation is deliberately biased and incorrect information spread to mislead

[14] Select Committee on Intelligence, *Russian Active Measures.* 2020
[15] Mueller.
[16] Staats, A. W. *Social Behaviorism.* 1975.
[17] Ibid.

others.[18] In the case of the 2016 election, I will be referring to the fake news created by the AI bot accounts as 'disinformation' because they were designed maliciously.[19]

[18] Think of disinformation as a subsect of misinformation, just with a different intention behind it.
[19] While not essential to define, it's important to remember that many of the articles and posts created by AI were later shared by real people on their real accounts. In these cases, the disinformation would transform into misinformation, as many of the users were unaware that the information was inaccurate and purposely misleading.

II. Literature Review

Civic technology—and its subsequent academic scholarship—is an ever-emerging field, but still considerably neglected in computer science research. Between 1998 and 2018, the number of peer-reviewed journal entries on artificial intelligence has expanded more than 300%, now accounting for 3% of peer-reviewed computer science journal publications.[20] While there is a growing body of work focusing on politics and artificial intelligence, this remains significantly smaller than other topics in the academic field of computer science. Many academics study how artificial intelligence affects advertising, automobiles, or law enforcement, but only a handful discuss political science and elections.[21] This is not new; political science and civic society has rarely been discussed in conversation with computer engineering, much less artificial intelligence. However, as the federal government begins exploring the capabilities of technological innovation in the public sphere, academic research followed suit.[22] A small, but growing, body of politically oriented computer science scholarship has emerged from policy researchers and legal scholars, intent to study how technology can alter or enhance civil rights. This was a significant portion of the literature I utilized in my research, in addition to other interdisciplinary sources from communications, law, and policy fields.

Each year, Stanford Law School's Freeman Spogli Institute in the Cyber Policy Center conducts an Index Report tracking and visualizing data related to artificial intelligence. This report is broad, focusing on several chapters of AI use, as well as

[20] Perrault, Raymond et al. "The AI Index." 2019.
[21] Ibid.
[22] Ibid.

public perceptions and societal considerations. Most notably, the 2019 Index reported that the most dominant topics associated with AI in that year were data privacy and ethics—typically defined through fairness, interpretability, and explainability.[23] These characterizations are often mentioned in AI applications to economics, education, the workforce, and the government.[24] This is an encouraging trend, as it suggests that the public and private sectors are beginning to address how AI can be used to promote civil rights, as well as disenfranchise marginalized communities.

To first learn about how AI affected the 2016 election, I turned to the 2018 Brookings Institute report, *Malevolent soft power, AI, and the threat to democracy.*[25] This report, authored by Senior Fellow Elaine Kamarck, describes Russian interference in the 2016 U.S. election but also highlights similar disinformation interferences in the United Kingdom's Brexit vote, and elections in the Ukraine, Scotland, Austria, Belarus, Bulgaria, Czech Republic, France, Germany, Italy, Malta, Moldova, Montenegro, Netherlands, Norway, and Spain.[26] By examining data from 1991 through 2017, Russia has proved to regularly interfere in presidential and parliamentary elections around the world, beginning by offering electoral funding support and then evolving into cyber-attacks and artificial intelligence bot production.[27] Kamarack's report compared these methods to the 2016 U.S. Presidential election, drawing note to key counties successfully targeted by Russian trolls.

[23] Ibid.
[24] Ibid.
[25] Kamarck.
[26] Ibid.
[27] Casey and Way.

Another incredibly useful publication was *Cybercrime,* by Kathleen Hall Jamieson. This book, published in 2018, describes the initial findings regarding Russia's involvement in the 2016 election, and how they utilized disinformation warfare to erode democratic norms and elect Donald Trump. Jamieson's book is an extensive insight into the ongoing investigations, while also clarifying how disinformation acts as a form of mind control.[28] Jamieson is effective because she presented conclusive, sound data to prove how voting changed due to disinformation, as well as what these tactics meant for civil society as a whole. I relied upon her work as a foundational start for my own scholarship, which suggested policies to safeguard the election process and protect against disinformation.

Many of my other sources were academics and researchers. As civic technology blossoms into an emerging field of research, universities and think tanks employ an array of experts working to establish new digital freedom norms worldwide. These institutions are leading the fight against electoral disinformation, and published reports essential to my research. The Oxford Internet Institute, operated in conjunction with Oxford University, is one of the most prominent centers considering how technology interacts with the public sphere. Samuel Woolley and Douglas Guilbeault first reported on Russian disinformation in their 2017 report, *Computational Propaganda in the United States of America: Manufacturing Consensus Online.* This study was one of the foundational works examining the power of disinformation in the 2016 election.[29] Another report from the Brookings Institute, *Ethical algorithm design should guide*

[28] Jamieson.
[29] Woolley, Samuel and Douglas Guilbeault. *Computational Propaganda.* 2017.

technology regulation, helped inform my proposals to improve technical governance.[30] Additionally, I interviewed Brenda Leong and Sara Jordan from the Freedom of Privacy Foundation, who helped me understand the technical side of disinformation and how legislation can better impact algorithms.[31]

Furthermore, I greatly utilized research from the Pew Research Center. Many of these polls contained fantastic data that helped contextualize public opinion on the 2016 campaign, the partisan divide, and voter turnout each year. Pew's data informed my analysis on religious voters,[32] on the partisan divide before and after Trump's presidency,[33] and the actual voter turnout in 2016.[34]

I also relied upon congressional hearings, reports, and intelligence investigations. While these were not pieces of literature, they were through lines within many of the sources that I reviewed in my research. Most predominately, I analyzed data from the Special Counsel Mueller investigation, the 2020 Special Intelligence Committee report on Russian disinformation campaigns, and several hearings before the Senate intelligence committee between 2018 and 2020. Not only did these provide crucial data and intelligence reporting I would otherwise be unable to access, but they also captured the testimony of policymakers and prominent researchers.[35] While all of my materials were highly reliable and accurate, these federal documents were the closest I came to accessing primary sources—they were the only documents with concurrent data insinuating the classified intelligence collected by federal officials.[36]

---

[30] Kearns, Michael and Aaron Roth. *Ethical algorithm design.* 2020.
[31] Leong, Brenda and Sara Jordan. Interview. 2021.
[32] Pew Research Center. *Faith and the 2016 campaign.* 2016.
[33] Pew Research Center. *The Partisan Divide.* 2017.
[34] Pew Research Center. *Voter Turnout by Population.* 2016.
[35] Select Committee on Intelligence.
[36] Mueller.

When I was unable to find declassified information, I turned to investigative journalism. Experts at the *New York Times, Politico Magazine,* and *Wired* were some of the first journalists reporting on Russian disinformation campaigns, both in 2016 and in 2020.[37] Many of these articles contained screenshots and images of the actual disinformation spread on Facebook and Twitter—a large collection of which has been since deleted.[38] Additionally, investigative journalism helped me draft a timeline of Russian disinformation interference in foreign campaigns.[39]

Throughout my research, I relied upon a wide variety of literature. This helped me understand more comprehensively my research questions, but also granted me with an interdisciplinary perspective that was crucial to such a technical topic. Civic technology and Internet regulation is not merely an issue for policy makers, but they are complex topics with complex answers, ones which need to consider the legal, technical, and political implications. I only expect that civic technology research will proliferate in the years to come, much as these debates will experience similar growth alongside technical developments.

[37] Sanger, David E. and Julian E. Barnes. "U.S. Warns Russia." 2020.
[38] Robinson, Meyer. "The Grim Conclusions." 2018.
[39] Parkinson, Joe and Georgi Kantchev. "Document: Russia Uses Rigged." 2017.

III. How Electoral Misinformation Became Disinformation

Before discussing the 2016 election, it is important to note that electoral misinformation is not a novel concept. "Fake news" has plagued the public sphere since the printing press was invented in the early 15th century. From Galileo's persecution by the Vatican to fabricated stories of sea monsters, the printing press allowed misinformation to rapidly proliferate and, for the first time, impact society.[40] And as democracy slowly spread across the Western hemisphere, misinformation campaigns soon followed. Democratic governments particularly relied upon journalists and the media to inform the public on state matters, global affairs, and local issues—thus, reliable journalism is a crucial element to any well-functioning democracy.[41]

History of Misinformation in the United States

Objective journalism is a contemporary novelty in the United States, and only established in the early 20th century. Prior to the creation of the journalistic norms that we are familiar with today—like truthfulness and nonpartisan reliability—yellow journalism inundated the public sphere. Since the American Revolution, yellow journalism favored melodrama over factual accuracy, opting to profit rather than inform. Even Benjamin Franklin's newspapers fabricated reports of King George III to increase hostility against the British.[42] As the United States developed into a sovereign nation, yellow journalism grew more powerful and influential, like by initiating the Spanish-American War with contrived articles about Spain's hostilities against Cuba.[43]

[40] Doyle, Aine. "Tracing 'Fake News:'" 2019.
[41] Soll, Jacob. "The Long and Brutal History." 2016.
[42] Ibid.
[43] Ibid.

The model of objective journalism arose for a wide plethora of reasons in the 1900s. Journalists began building reputations of trust and dependability through reputable publications, like the *New York Times*, and congressional encouragement. Throughout the 20th century, Americans learned of major government programs and scandals—like Watergate—because of investigative journalism and leaked federal documents. Yellow journalism faded away into tabloids and political news, largely dismissed by the America public and replaced with reliable sources.[44]

However, misinformation lingered in the public sphere. Throughout the 1940s and 1950s, the U.S. government was highly concerned over ideological and nuclear threats from the Soviet Union. In April 1950, the National Security Council and State Department drafted the top-secret report NSC 68, which detailed the government's concern about Communist misinformation and propaganda schemes.[45]

NSC 68 described the fundamental difference between the Kremlin and the U.S. government. The Kremlin represented the antithesis of traditional American values like freedom and liberty, instead signifying a "slave state" which "eliminate the [civilian] challenge of freedom" against the government.[46] This iron curtain polarized the Soviets from every Western democracy, automatically creating global tension and concern for violence. NSC 68 expressed concern for nuclear attack, but also for an insidious violation of American ideals. It described that:

> Every institution of our society is an instrument which it is sought to stultify and turn against our purposes. Those that touch most closely our material and moral strength are obviously the prime targets, labor unions, civic enterprises, schools, churches, and all media for influencing opinion. The effort is not so much to make them serve obvious Soviet

[44] Ibid.
[45] Miller, Jennifer M. "Democracy and Misinformation." 2019.
[46] National Security Council Report 68, "United States Objectives." 1950.

> ends as to prevent them from serving our ends, and thus to make them sources of confusion in our economy, our culture and our body politic.[47]

Here, the report is identifying a clear concern for domestic misinformation campaigns by the Kremlin, which could also be characterized as information warfare. While the Soviet Union worked to create corporeal weapons of mass destruction, it simultaneously enacted verbal campaigns to deteriorate the fabric of American society. By integrating Soviet propaganda on a wide scale, the misinformation threatened to "increase anxiety and defeatism in all the free world."[48] NSC 68 laid foundation for McCarthyism and Cold War politics that further exacerbated a rise of division in the public sphere.[49]

This foundation led to the Central Intelligence Agency's 1967 Operation Mockingbird. Originally beginning in the early 50s, Operation Mockingbird partnered the federal government with American journalists and media sources to influence public opinion. The CIA sought to counter Soviet misinformation with American propaganda by secretly sponsoring over 400 reporters and editors to publish anti-communist articles.[50] These articles were published in the *New York Times, Washington Post,* and other highly regarded, nonpartisan periodicals. Many of these disinformation articles were written after surveilling anti-war activists and individuals believed to be associated with the communist party, primarily to better target similar populations.[51]

It is important to note that the American federal government has conducted misinformation campaigns in foreign countries for decades. This foreign policy is not uncommon—most large states attempt to influence international elections with overt or

---

[47] Ibid.
[48] Ibid.
[49] Miller.
[50] Hadley, David P. *The Rising Clamor.* 2019.
[51] Ibid.

covert support of a favorable candidate. The United States has spread misinformation in El Salvador, Panama, Venezuela, Iran, and many other foreign states to help pro-U.S. candidates.[52] As Michael Sulmeyer, a senior director for cybersecurity at the United States Cyber Command, stated, "America lives in the glassiest of glass houses."[53] Cyber interference in foreign elections has only proliferated since the beginning of the 21st century, but what distinguishes U.S. actions from the Russian 2016 interference is a mastery of emerging technology unseen before.

Russian Misinformation Campaigns

The foreign intelligence community first identified evidence of Russian interference in Western elections in 1994. Originally, Russian officials focused on interfering with elections in former Soviet Union states—primarily Ukraine, Belarus, and Moldova—and assisted candidates that tended to be more nationalistic, conservative, and supportive of the Russian agenda.[54] At the time, Western Europe was recovering from the Cold War and the rupturing of the Soviet Union. Many of the former Soviet states were adjusting to the new normal of geopolitics, and soon had to decide between drawing allegiances with the European Union or Russia. To promote Russian regional authority, the Russian government began covertly interfering in many of these early elections in newly independent countries.[55] Russian agents shared articles favoring their selected candidates and spread misinformation through media and community organizing. In 1994, the Russian government provided support for Leonid

[52] Ibid.
[53] Sanger, David E. and Nicole Perlroth. "Trump Contradicts Pompeo." 2020.
[54] Casey and Way.
[55] Tolstrup, Jakob. *Russia v. EU.* 2013.

Kuchma, a politician challenging Ukraine's first President, Leonid Kravuchuk. While Kuchma's term was defined by corruption and scandal, he promoted Russian policy and worked to reshape the nascent country into a state reliant upon Putin and his power. In short, the clandestine misinformation campaigns worked.[56]

Over the next decade, Russian agents continued manipulating the results of Ukrainian, Belarusian, and Moldovan elections, but often with very minimal tangible results. While the misinformation schemes worked for Kuchma, all of the other politicians did little to advance Russian agendas or promote Russian regional authority. Subsequently, the Russian interference campaigns evolved in 2004. Instead of covertly supporting candidates through misinformation campaigns, the Russian government additionally massively funded politicians for further advantage. When Kuchma stepped down from the Ukrainian presidency in 2004 and named Yanukovych as his successor, the Russian government provided between $50 and $600 million to Yanukovych's campaign.[57] Despite Yanukovych's ultimate electoral loss, the Russians began transforming their role in electoral politics. Soon, the Kremlin continued providing massive amounts of funds to politicians, promising to lower gas prices if they win, and publicly urging state media sources to distribute misinformation on the candidate's behalf.[58]

The Kremlin first used cyberwarfare in the 2014 Ukrainian election. In an attempt to disrupt and falter the Presidential election, Russian operatives spawned a series of coordinated cyberattacks dismantling the election. These attacks faked voter

[56] Ibid.
[57] Tolstrup, Jakob. "Black knights and elections." 2014.
[58] Ibid.

totals and integrated malware into state servers to completely revert the election results.[59] This proved unsuccessful; the election continued, and an anti-Putin candidate won office. However, these cyberattacks laid the foundation for future interference, and shifted towards a more contemporary way of spreading misinformation through cyberwarfare. Foreign intelligence gathering found that similar hacking techniques were used in 2015, when Russia expanded out of Western Europe and interfered in British and German elections for the first time.[60]

However, everything changed in 2016. Russian operatives interfered in elections in the United States, the United Kingdom, the Netherlands, Norway, Montenegro, Italy, Bulgaria, and Austria, proving its interest in dominating not only regional authority, but establishing a global power over Western states.[61] By creating and implementing a new form of cyberattack—AI social media bots—the Kremlin was able to spread disinformation at a massive scale unseen before. In the days leading to the Brexit referendum, over 150,000 Twitter accounts owned by Russian users posted tens of thousands of messages in English that supported Brexit and spread faulty accounts of politicians and celebrities that supposedly voted to leave.[62] In the Netherlands, Russia instigated a disinformation campaign for a referendum modifying Ukrainian membership in the European Union. Media outlets run by Russian operatives, like Sputnik and RT, shared incorrect articles prompting Dutch readers to widely criticize Ukraine.[63] And in Bulgaria, journalists located a document proposing a Russian-

[59] Le Miere, Jason. "Russia Election Hacking." 2017.
[60] Reinhold, Fabian. "Germany Prepares." 2017.
[61] Casey and Way.
[62] Kirkpatrick, David. "Signs of Russian Meddling." 2017.
[63] Higgins, Andrew. "Fake News, Fake Ukrainians." 2017.

sponsored victory plan for the Socialist Party to "plant fake news and promote exaggerated polling data" to ensure that "the party emphasize issues that dovetailed with Kremlin policy: calling for an end to Russian sanctions, criticizing NATO and talking up the UK's vote to leave the EU."[64] While the exact number of fake news accounts operating within Bulgaria remains unknown, the Socialist Party's candidate, Rumen Radev, won the presidency and strengthened ties with Russia.

While Russian meddling began as a way to dominate regional authority, they transformed into an effort for global power. In 1998, former KGB Major General Oleg Kalugin described Russian disinformation as "the heart and soul of Soviet intelligence," stating that it was

> not intelligence collection, but subversion; active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO; to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs.[65]

These campaigns prove that the Kremlin is actively attempting to dismantle the European Union, minimalize the United States' role in global politics, and create a new global environment fit for Russian dominance. They are achieving this through supporting Nationalistic, inflammatory politicians that embody a potential to build or reinforce connections with the Russian government.[66] This is not a whimsical support of a specific individual—it is a long-term scheme to control global politics and dismantle the current world order.

[64] Parkinson and Kantchev.
[65] Kalugin, Oleg. "Inside the KGB." 1998.
[66] Tolstrup.

By influencing Brexit, helping Donald Trump, and dismantling the voter bases of Angela Merkel, the Kremlin is exposing its intentions for chaos and making it easy to guess its next steps: whatever serves their best interest.[67]

[67] Le Miere.

IV. Transitioning Technology

The Invention of the Internet

First invented in the early 1970s, the Internet began as a Department of Defense program for academic communication in an attempt to further protect national security. After the Soviet Union launched the Sputnik spacecraft in 1957, the American government feared that they were conducting widespread surveillance on American citizens.[68] The government, in an attempt to better secure the country against Soviet interference, funded the Advanced Research Project Agency (ARPA), a project by the Department of Defense to facilitate communication between scientists across the country. By 1969, ARPANET was created—a system of computers across the West Coast that could communicate and work together through the Internet.[69] Despite operating through public and private universities across the United States, ARPANET remained operated by the Department of Defense until 1983. The rise of global computer operating companies, like Intel and Microsoft, quickly projected the nascent Internet into a popularized technology with personal computers in the late 1980s. By then, the Internet was a bare-boned tool, primarily used for word processing and software programs in professional environments.[70]

The Internet exponentially grew during the 1990s, resembling what we are more familiar with today. After the World Wide Web was developed in 1989, companies rapidly shifted onto online platforms. Soon, the electronic mail would be invented,

[68] Hafner, Katie. *When Wizards Stay Up Late.* 1996.
[69] Berners-Lee, Tim. *Weaving the Web.* 2000.
[70] Naughton, John. *A Brief History of the Future.* 2000.

enabling individuals to use the Internet for personal and social matters for the first time.[71]

It is important to note that the Internet is different from the Web or the cloud—it is a system of digital wires. The Internet is an elaborate and colossal infrastructure of global networks, all connected through wires existing in cyberspace. When someone accesses the Internet, they are logging onto their own private wire that is automatically networked to every single other Internet-accessing device in the world. The Web, which is easily accessed on every computer, is built above the Internet, and operates as a portal to different sites. When individuals hack online, they hack into both the operating systems as well as sites accessible through the Web.[72]

The Rise of Social Networking Sites

Social media has existed throughout modern history, only in different forms than we are familiar with today. Periodicals and magazines have operated in similar fashions as today's major companies, like Facebook and Twitter—before the Industrial Revolution, these media brought news and stories into communities, allowing individuals to connect with one another by extensive means. Social media first shifted onto an electronic platform in 1844, when the telegraph was first invented. Samuel Morse's invention was rudimentary compared to contemporary social media sites, but operated in a shockingly similar matter, complete with popularized acronyms similar to

[71] Hafner.
[72] Berners-Lee.

today's digital slang.[73] "G M" meant "good morning" and "S F D" stood for "stop for dinner."[74]

Despite the popularity of telegraph communications, social media websites first appeared online as the Internet grew more mainstream in the late 20th century. A plethora of digital communication sites—like CompuServe, America Online, and Prodigy—allowed users to connect with and talk to other users across the country, riding the success of widely popular e-mail technology. Six Degrees, created in 1997, and Friendster, launched in 2001, were the first two social media platforms where users were able to upload personalized profiles to facilitate digital networking, rather than just messaging others. Later, in 2002, LinkedIn launched for early career professionals to connect, digitally network, and find jobs. Despite the prevalence of these sites, they remained somewhat unpopular on the mainstream Web.[75]

Myspace was the catalyst for the social media frenzy. Launched in 2003, Myspace rapidly became the most trafficked website globally. Users praised the unique ability to upload music, artwork, and writing on the site, prompting more personalization of each profile. Myspace was the first mainstream social media platform and revolutionized the way users interacted online.[76]

But in 2004, Mark Zuckerberg invented Facebook and permanently changed the Internet. Originally designed as Facemash in 2003, Zuckerberg created a site to vote on the attractiveness of different female students at Harvard University. Facemash gained

[73] There are also reports of people "online dating" through the telegram, albeit without modern apps or websites. One could only expect that Farmers Only, the dating site exclusively for agricultural workers, would have been particularly popular in the late 1800s.
[74] Standage, Tom. *Writing on the Wall.* 2014.
[75] Van Dijck, José. *The Culture of Connectivity.* 2013.
[76] Kapoor, Kawaljeet Kaur et al. "Advances in Social Media Research." 2018.

massive popularity, and Zuckerberg transformed it into "The Facebook" in 2004. The Facebook became a global site with individual profiles for users to meet other college students. Its distinguishing factor was its timeline function, allowing users to post status updates and messages available to each of their Facebook friends.[77]

Since 2004, social media has taken over the world. Today, Facebook is used by 1.7 billion people worldwide.[78] YouTube is used by 73% of adults in the United States, while seven-in-ten adults operate Facebook accounts.[79] Instagram, now owned by Facebook, has more than 1 billion global users.[80] Twitter has instigated social revolutions in the Middle East and helped spread crucial political messaging in the past decade.[81] And most recently, TikTok has grown in popularity, resulting in more than 800 million users worldwide.[82]

As social media continues to evolve, as does its role in society. Like other forms of technology, social media companies have remained relatively unregulated since their creation. However, as technology thinktanks proliferate and pundits consider the role of technology in modern America, many individuals are questioning the unchecked power of big tech. Facebook consistently buys out its competitors, including Instagram and WhatsApp, seeking to dominate the social networking market. Meanwhile, TikTok faces enhanced scrutiny for its ties to the Chinese government and its secret data collection projects. With a new presidential administration in 2021, increased calls in the public sphere to scale back large social media companies, and widespread advocacy

[77] Cuthbertson, Richard et al. "Facebook and MySpace." 2015.
[78] Gramlich, John. "10 facts about Americans and Facebook." 2019.
[79] Ibid.
[80] Decker, Allie. "Instagram Marketing." 2020.
[81] Smidi, Adam et al. "Social Media and Social Mobilisation." 2017.
[82] Meola, Andrew. "Analyzing Tik Tok." 2020.

for data privacy regulations, the tech industry will only remain as a prevalent and influential presence around the world.[83]

Artificial Intelligence and Machine Learning

Science aficionados—both professional and recreational—have obsessed over robots since the beginning of the Information Era in the early 20th century. As Internet technologies evolved and complexified, computer scientists searched for ways to create artificially intelligent robots using programming. British polymath Alan Turing first instigated the AI thought experiment by considering the mathematical likelihood an intelligent machine could reason in 1950.[84] Unfortunately, without the Internet, there was no way computers could store and maintain commands independently. While Turing's experiment failed, it inspired Logic Theorist, a program by Allen Newell, Cliff Shaw, and Herbert Simon widely considered the first AI program ever created. Logic Theorist proved that AI was achievable, even if it needed an additional twenty years of research to succeed.[85]

As technology developed, artificial intelligence followed suit. By the 1980s, $400 million was invested by the Japanese government to revolutionize machine learning and AI capabilities.[86] Edward Feigenbaum invented expert systems, a technological process where a computer mimicked the deliberation process of a human expert. By 1997, AI chess computer programs were beating global grandmasters, speech recognition software was widely used on Windows computers, and a robot could detect

[83] Wheeler, Tom et al. "The need for regulation of big tech beyond antitrust." 2020.
[84] Smith, Chris et al. "The History of Artificial Intelligence." 2006.
[85] Ibid.
[86] Ibid.

and simulate human emotions.[87] In the early 2000s, computers gained the capacity to store profoundly more data, opening even more doors for AI research and capabilities.

Today, artificial intelligence is widely used in less glamorous manners. Banking, marketing, media, and insurance companies regularly use machine learning and AI tools in their outreach programs. Many of the phishing calls received are instigated by AI bots, and most commercial companies rely upon robot receptionists instead of human agents. Technology companies employ highly advanced algorithms to precisely track people's digital footprints, only strengthening their AI capabilities.[88] By championing big data networks and machine learning trees, AI continues gaining rapid amounts of momentum across the Web.

What's Next?

With the emergence of driverless cars, real-time language translations, and digital doctors, artificial intelligence and technological interference in everyday life will only continue snowballing. Finally, lawmakers are beginning to adjust to the new normal: tech is not slowing down. Ethical questions, like who should govern the Internet and what the best guidelines are for AI, are being discussed to a greater extent than ever before. Agencies around the world are championing digital rights, advocating for widespread data privacy and open-sourced platforms promoting ethical AI.[89] And by interrogating the power of Facebook, Google, and Amazon, the U.S. government has begun defining the federal role in maintaining these systems.

[87] For whatever reason, chess abilities have been a high bar for success in the AI industry.
[88] Anyoha, Rockwell. "The History of Artificial Intelligence." 2017.
[89] Bostrom, Nick and Eliezer Yudkowsky. "The Ethics of Artificial Intelligence." 2014.

However, the American government still does not have a national policy for data protection. Without concrete and extensive regulations online, the Internet is an ambiguous cyberspace lacking clear jurisdictions. This is a huge problem: The United States simply does not have a good technology policy. After the European Union passed the General Data Protection Regulation (GDPR) in 2016, nations around the globe raced to meet the budding norm for citizen data rights.[90] Instead of a broad piece of national legislation, the United States has a mélange of state and federal laws providing different frameworks of digital privacy. Recently, California passed the California Consumer Privacy Act (CCPA), the most progressive U.S. Internet policy to date.[91] To dismantle the sweeping power of big technology companies, Congress must also build legislation similar to CCPA, ensuring the needs of the consumer are always protected. Until then, the monopoly of tech power will remain unrestrained.

[90] DataGuidance & Future of Privacy Forum. "Comparing privacy laws" 2019.
[91] Ibid.

V. Algorithms of Control

At their core, algorithms are a set of rules that dictate how a computer program operates. They are dynamic and designed to personalize content for users on most websites, including Facebook, Twitter, Google, and Instagram. These lines of code are the reason why search results are tailored to what you have visited before, why YouTube can recommend similar creators to what you already subscribe to, and why your Facebook feed always tends to show updates from the profiles you interact with most before other posts.[92] Algorithms help the Web function as a complex, personable, and accessible space, but they also easily lead to abuse and corruption. By deeply understanding the nature of algorithms, individuals and organizations can attempt to persuade users to buy a product, learn about a topic, or vote for a politician.[93]

It is important to note that algorithms on highly visited websites are already designed to customize content to each user. There are a variety of motivations behind this: a commerce site might want to tailor its marketing more directly, or search engine might desire to have its results already directed towards what a user is interested in. But for social media websites, these algorithms are designed for continuous user engagement. As Woodrow Hartzog, a law professor specializing in computer science at Northeastern University, described, "if you want to know when social media companies are trying to manipulate you into disclosing information or engaging more, the answer is always."[94] Feeds are designed to constantly provide new content and capture a user's attention for a long period of time, therefore confining them to the social media app and

[92] Petrescu, Maria and Anjala S. Krishen. "The dilemma of social media." 2020.
[93] Girish, Devika. "'The Social Dilemma.'" 2020.
[94] Bogle, Ariel. "How the internet tricks you." 2018.

promoting continued use. From the profiles recommended to the posts prioritized in a user's feed, an app's algorithm curates a formidable vortex designed purely for its addictiveness.[95] These vortexes operate as separate communities, spaces, and ecosystems dominated by other users with similar likes, interests, and ideologies. Typically, users are surrounded by other like-minded accounts, almost totally unaware of what occurs in different online ecosystems.[96]

In many ways, digital footprints have transformed from minute, passive identities into significant representations of who a person is, what they believe in, and how they define themselves. Someone's presence online is more than their Amazon browsing history or news website preference: each minute data point acts as a tiny piece to a huge, all-encompassing puzzle.[97] Algorithms use these dismissed data points to power their operations, ultimately to deeply and complexly understand what makes a user unique and distinct.[98]

By controlling these algorithms, a programmer can essentially control a user's digital world. They can dictate which communities and spaces a user's account operates within, and which content they end up exposed to and receptive towards. Without our knowledge, these digital worlds end up more influential than tangible, real-life communities outside of cyberspace. And by controlling the content that a user sees and interacts with, a hacker or programmer can begin to change the way they view and think

[95] Many would argue that this is not inherently a negative thing. The Spotify algorithm, for example, is written to expose users to new music and artists based on their prior listening and interests indicated through their Facebook account. It is why I, for example, was recommended the *Pride & Prejudice* (1998) soundtrack earlier this morning. Like many other inventions in the tech world, algorithms can be used for both good and bad things; more often than not, the negative associations outweigh the potential for good.
[96] Daley, Beth. "Do social media algorithms." 2020.
[97] Halpern, Sue. "Cambridge Analytics and the Perils." 2018.
[98] Bagrow, James P., Xipei Liu and Lewis Mitchell. "Information flow reveals." 2019.

of the world. They cannot control their physical mind, but they can begin controlling or shaping a user's digital one. And often, that can be more influential than we may like to believe.

Behind every algorithm is a coder or programmer that is writing that algorithm for a purpose. That person's biases, preconceptions, and interests are translated through their algorithm, similar to any other form of writing or self-expression.[99] For many social media sites, the algorithm's purpose is to consume a user's attention span and prevent them from leaving the app. But for individuals with nefarious interests, or criminal motivations, controlling the algorithm becomes an important tool in converting new audiences.[100]

[99] An interesting debate emerging from this area is how racism and bigotry is encoded in many algorithms. Facial recognition software, job application programs, and home security systems have all been subject of scrutiny by operating already prejudiced against people of color. While this debate is not entirely relevant to my thesis, it is worth noting as another way computer science and technology interacts with civil liberties and digital freedom.

[100] Halpern.

VI. The 2016 Election

The Mueller Report formally acknowledged in the public sphere that the Russian government manipulated and interfered in the 2016 Presidential election.[101] However, even after a Special Counsel investigation and calls to break up Big Tech social media companies, the consequences of Russian involvement remain vague and abstract in the public sphere. Little is understood regarding the motivations of the Russian government, what Donald Trump's involvement might have been, or what exact impact the AI bots had on voter turnout and the election's results. But considering the history of Russian disinformation interference in democratic elections illustrates the Kremlin's desire to discredit Western democracies through political violence, increased partisanship, and irrevocable ideological divisions. As Senator Charles E. Grassley said in a 2017 Judiciary Committee hearing, "Russia does not have loyalty to a political party in the United States. Their goal is to divide us and discredit our democracy."[102]

By manipulating the 2016 election, the Russian government wanted to enshrine the U.S. electoral system with doubt and exacerbate preexisting discords of race and gender in American politics. This involvement was not unexpected; Vladimir Putin and Hillary Clinton were widely regarded as adversaries after her harsh criticism of Russia while Secretary of State.[103] During the 2011 Russian election, Clinton sharply criticized

[101] Mueller.
[102] C-SPAN. "FB, Google, Twitter Exec." 2017.
[103] Throughout Hillary Clinton's extensive political career, she has outwardly and explicitly condemned the legitimacy of Putin's office. At one point, she even compared him to Hitler. What marked her comments as Secretary of State, however, was the increased weight of her remarks. Clinton's comments carried the full power of the U.S. State Department, indicating the country's rejection of Russian ideals and power.

Putin's victory and the Russian electoral system as a whole, supposedly showing American support for Putin's political opponents and undermining his authority.[104]

Meanwhile, Donald Trump showed potential to disrupt the status quo of American foreign policy and align domestic norms to more closely resemble those within Russia, particularly through reduced aid to Ukraine.[105] Additionally, his business interests closely aligned with Russian economic prosperity. According to the declassified joint CIA, FBI, and National Security Agency report in 2017, "Putin and the Russian government developed a clear preference for President-elect Trump."[106] The Kremlin intended to damage both Clinton's campaign and the democratic process as a whole.

What followed was a sophisticated campaign to sway the 2016 election. The intelligence community has identified several complex schemes used by Russian operatives to broadly attack the election. Specifically, they created campaigns that where:

> Russian intelligence and Kremlin-connected hackers infiltrated voting systems, leaked Clinton campaign emails to Wikileaks, created fake documents alongside real documents to Wikileaks, used Facebook pages to spread anti-immigrant propaganda, paid for pro-Trump Facebook ads, used Facebook to organize anti-immigrant protests in the US.[107]

While all of these tactics highly impacted the 2016 election, the most disturbing and invasive was the infiltration of voting systems. Congressional and academic investigations found that the Russian infiltration of American voting systems was an elaborate and multifaceted attack. These programs were designed to shed doubt on the

[104] Crowley, Michael. "Why Putin hates Hillary." 2016.
[105] Kamarck.
[106] *Assessing Russian Activities and Intentions.* 2017.
[107] Casey and Way.

electoral process as a whole, while igniting preexisting embers of oppression within American civil society.[108]

Russia's Information Warfare

The Mueller investigation found evidence of the Russian government used disinformation to infiltrate the election in several ways. The Kremlin used paid "trolls" to create fake social media accounts that spread disinformation through state-sponsored propaganda, deep fakes, and fake news in United States cyber communities. Many of these accounts also marketed the WikiLeaks documents engineered by Russian officials. By weaponizing social media and spreading disinformation, the Russian government engaged in a new form of "information warfare" to "sow discord in the U.S. political system."[109] These accounts interacted with tens of millions of Americans on several social media platforms, attempted to "polarize Americans on the basis of societal, ideological, and racial differences," and showed "covert support of Russia's favored candidate in the U.S. presidential election."[110]

This attack was broad by design; the vast array of disinformation forms was purposefully diverse so that, at some point, the content would appear on a social media account of most Americans. It was a "firehouse of falsehoods" with "incredibly large volumes" and a "rapid, continuous, and repetitive" barrage of constant content generation.[111] Furthermore, the Russian government engineered disinformation media that played off of preexisting partisan divides. This niche content was expertly crafted

[108] Select Committee on Intelligence.
[109] Ibid.
[110] Ibid.
[111] Paul, Christopher and Miriam Matthews. "The Russian 'Firehouse of Falsehood.'" 2016.

to seamlessly integrate itself into each algorithm, thereby achieving a different goal based on that affected community. For evangelical Christians and veterans, state-sponsored propaganda was widely spread through fake Twitter, Facebook, and YouTube accounts, resulting in a huge turnout on election day; Black voters were demobilized and pressured by fake "blacktivist" accounts to extract themselves from voting; and previous supporters of Bernie Sanders were encouraged to support Green Party candidate Jill Stein.[112]

Figure 1: Connecticut Senator Richard Blumenthal and an engineered photo of comedian Aziz Ansari circulated by Russian operatives during the 2016 election.[113]

The disinformation media created by Russia was used to extensively and unilaterally attack American voters. By flooding timelines and accounts with content designed to manipulate the user's sense of community and reality, the Kremlin hoped to impact the voting behavior of that individual. These were not always overtly supporting Trump; more often than not, the content was engineered to draw doubt on an

[112] Jamieson.
[113] Harnik, Andrew. "Photoshopped Aziz Ansari." 2017.

individual's support of Clinton or convince them to simply not participate in the election as a whole.[114] In the three months before the election, 38 million Facebook posts with disinformation were shared and received 760 million clicks, or "about three stories read per American adult" each day.[115] Relatively, these were only a small portion of the content a user viewed online; however, three stories per day for the average adult is a significant symbol of the sheer number of disinformation that existed online.

Artificial Intelligence, Trolls, and the Internet Research Agency

To achieve such a significant high caliber of content generation, the Russian government relied upon the Internet Research Agency (IRA), a quasigovernmental organization with close ties to the Kremlin. The IRA hired hundreds of Russian hackers to act as online trolls, crafted fake news stories and spread disinformation on Twitter, Facebook, Instagram, and YouTube. While the full extent of the IRA's reach on these platforms is still unknown, Facebook reports that the IRA's political posts reached 140 million Facebook users leading up to the 2016 election.[116] The IRA worked in conjunction with Russian business leaders, government operatives, and cybersecurity professionals to spread disinformation on the widest scale in modern history.

The IRA used several different methods to share disinformation. First, it created over 140 U.S. political websites, including WorldPoliticus.com, TrumpVision365.com, USConservativeToday.com, and USADailyPolitics.com.[117] These sites generated

[114] Ibid.
[115] Allcott, Hunt and Matthew Gentzkow. "Social Media and Fake News." 2017.
[116] *United States v. Internet Research Agency*, et al. 2018.
[117] Silverman, Craig and Lawrence Alexander. "How Teens in the Balkans." 2016.

hundreds of thousands of views in 2016 and published many of the fake news articles spread within American cyberspace.[118] Additionally, the IRA placed 3,400 advertisements for Trump on Facebook, valuing at $100,000.[119] But most shocking of all was the quantity of social media posts from the Russian troll accounts. In the six months before the election, Russian-linked accounts posted 61,500 posts on Facebook, 116,000 photos on Instagram, and 10.4 million tweets on Twitter.[120]

The accounts linked back to IRA Russian trolls were often automated by artificial intelligence bots. In a study by the Oxford Internet Institute, AI troll accounts "reached positions of measurable influence" by closely learning the habits and interests of users and crafting content to better appeal to those individuals.[121] These "did infiltrate the upper cores of influence and were thus in a position to significantly influence digital communications during the 2016 election" to the point where Russian disinformation was "almost completely bounded by highly automated accounts, with a high degree of overall automation."[122] The bot accounts primarily reshared disinformation posts of other Russian-operated users, which generated even greater traction within the various social media algorithms. For many of these platforms, the algorithms are designed to cycle through trending media posts, thereby sharing content that has already been deemed as 'interesting' through the digital interactions by a wider audience.[123]

---

[118] *United States v. Internet Research Agency*, et al.
[119] Mueller.
[120] Select Committee on Intelligence.
[121] Woolley and Guilbeault.
[122] Ibid.
[123] Select Committee on Intelligence.

Sites like Facebook, Twitter, and Instagram were flooded with disinformation posts. Automated troll accounts produced 25 to 30 times more content than real news accounts, inundating social media platforms with inflammatory, extremist, and aggressive views.[124] These posts containing disinformation also were 70 percent more likely to be retweeted than reliable news stories.[125] In the month before the election, Twitter identified 50,000 bot accounts linked to Russian servers that shared only election-related content.[126] The real amount is estimated to be much higher.

Despite the difference in audiences, similar trends followed all of the messaging. In right-wing cyberspheres, disinformation focused on the quantity of illegal immigration, xenophobia and Islamic terrorism, and an assault on Christian values. Much of the rhetoric perpetuated fears of an assault on law enforcement and veterans, as well as an awareness of Black nationalism and continuing social justice movements. Meanwhile, left-leaning profiles spread that Clinton rigged the primary against Bernie Sanders, that she was anti-Black, and corrupted by Wall Street. They shared her history of supporting incarceration legislation and claimed she would perpetuate institutionalized racism.[127]

The disinformation itself that was spread reached a wide audience and was intended to appear reliable. On Facebook, a story that Trump was endorsed by Pope Francis received over 960,000 shares, reactions, and comments.[128] A story that Clinton sold weapons to ISIS engaged with 789,000 accounts.[129] "Blacktivist," a Facebook

[124] Kelly, John. "Hearing before the Senate Select Committee on Intelligence. 2018.
[125] Robinson.
[126] Twitter. "Updated on Twitter's review." 2018.
[127] Jamieson.
[128] Silverman, Craig. "This Analysis Shows How Viral Fake Election." 2016.
[129] Ibid.

group created by IRA trolls that appeared as a community for Black social justice activists, generated over 500,000 followers and outpaced the growth of the official Black Lives Matter account.[130]

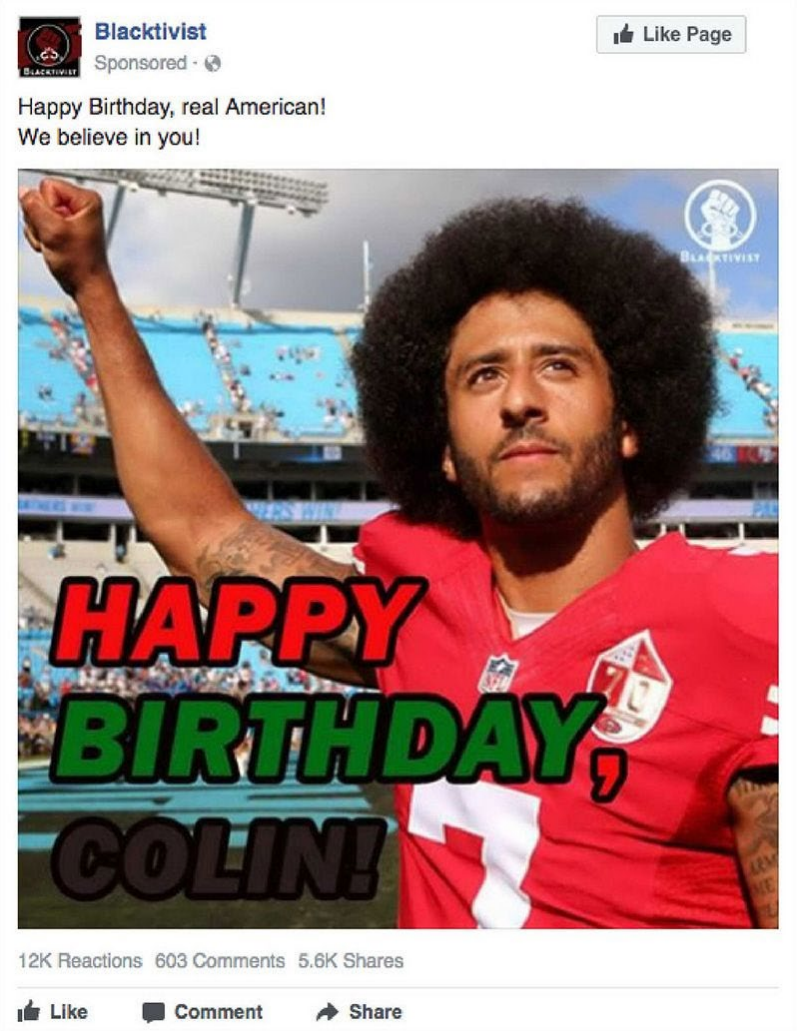

Figure 2: Ad from the "Blacktivist" celebrating Colin Kaepernick's birthday with over 12,000 reactions and almost 6,000 shares.[131]

The posts were designed simply, thereby easier for users to quickly share and process without significant consideration of its content.

[130] Parham, Jason. "Russians posing as black activists on Facebook." 2017.
[131] "Colin Kaepernick, Blactivist Ad." Senate Intelligence Committee. 2018.

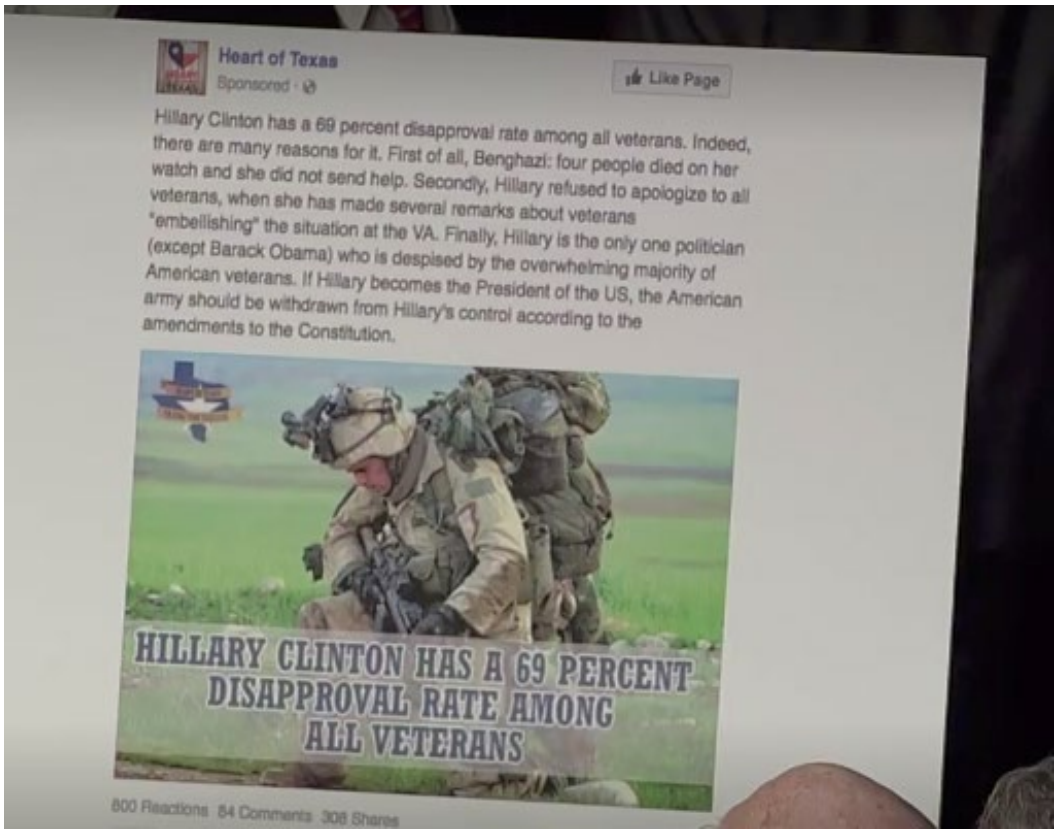

Figure 3: Ad from "Heart of Texas" claiming that Clinton had a 69 percent disapproval rating from veterans.[132]

An advertisement by "Heart of Texas," a Russian Facebook page, claimed that Clinton had a 69 percent disapproval rating. This was false, and a piece of disinformation used against Clinton on a page with over 250,000 members.

[132] "Heart of Texas, Veteran Approval Rating." US Senate. 2017.

Figure 4: "South United" which had over 130,000 community members.[133]

Many of the groups were focused on national identity, like "South United." These Facebook groups planned real events, shared disinformation, and allowed users to interact with one another continuously. These echo chambers spiraled into communities where like-minded individuals were fueled by disinformation designed to garner enraged and extreme reactions.[134]

These bot accounts also shared Russian propaganda from state-operated media agencies. RT, formerly known as Russia Today, had an influx of American views leading up to the 2016 election. RT contributed to the cult-like following of Trump by focusing primarily on negative Clinton news, widely exploiting her leaked emails and accusations of corruption. Trump was hailed as a pioneer for American values, who

[133] "South United Screenshot." *New York Times*. 2018.
[134] Jamieson.

would seemingly rebuild the American legacy and work with Putin to establish a global dominance of power. For the first time, RT became one of the most shared accounts in American social media.[135]

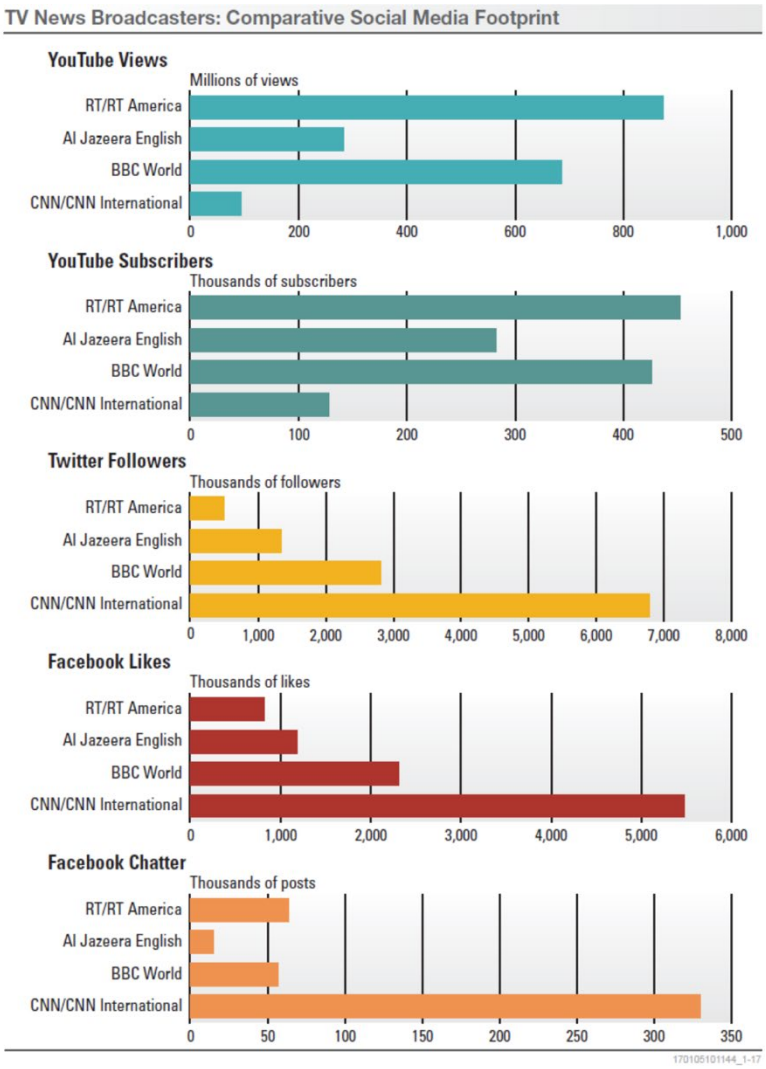

Figure 5: RT's engagement leading up to the election. On YouTube, RT surpassed the views of many other accredited global media outlets.[136]

While working in conjunction with the IRA, RT aired documentaries, news segments, and strategically oriented talk shows focused on volatile current events in the US. These

[135] Select Committee on Intelligence.
[136] "TV News Broadcasters: Comparative Social Media Footprint." Intelligence Community. 2017.

stories fueled partisan tensions, particularly in the right-wing social media spheres that the Russian bot accounts shared them in.[137]

Despite an awareness of these automated troll accounts after the 2016 election results, the IRA-owned accounts merely intensified their activity after the election. Instagram posts each month increased by 238 percent, Facebook by 69 percent, Twitter by 52 percent, and YouTube by 84 percent.[138] When testifying before Congress, John Kelly, a social media researcher, described that

> after election day, the Russian government stepped on the gas. Accounts operated by the IRA troll farm became more active after the election, confirming again that the assault on our democratic process is much bigger than the attack on a single election.[139]

The American government may be acutely attuned to these disinformation schemes, and the American public may be somewhat aware of what is occurring in our cyberspaces, but the damage is only continuing. Even with Congressional attention and federal investigations, Russia's information warfare remains insidiously unraveling partisanship and comradery in the public sphere.

The 2016 Victims of Disinformation Warfare

The electoral college makes every U.S. Presidential election a game. Candidates must secure 270 electoral college votes to win the presidency, which often results in a concentrated focus on swing state turnout. While most states tend to historically fall into a voting pattern of red or blue, states like Arizona, Florida, Michigan, Pennsylvania, Wisconsin, Ohio, and North Carolina are battlegrounds for each candidate. The 2016

[137] Assessing Russian Activities and Intentions.
[138] Mueller.
[139] Kelly.

election was no different; Trump won the presidency because he secured Michigan, Pennsylvania, Wisconsin, and Ohio, leaving him with 304 electoral college votes over Clinton's 227.[140]

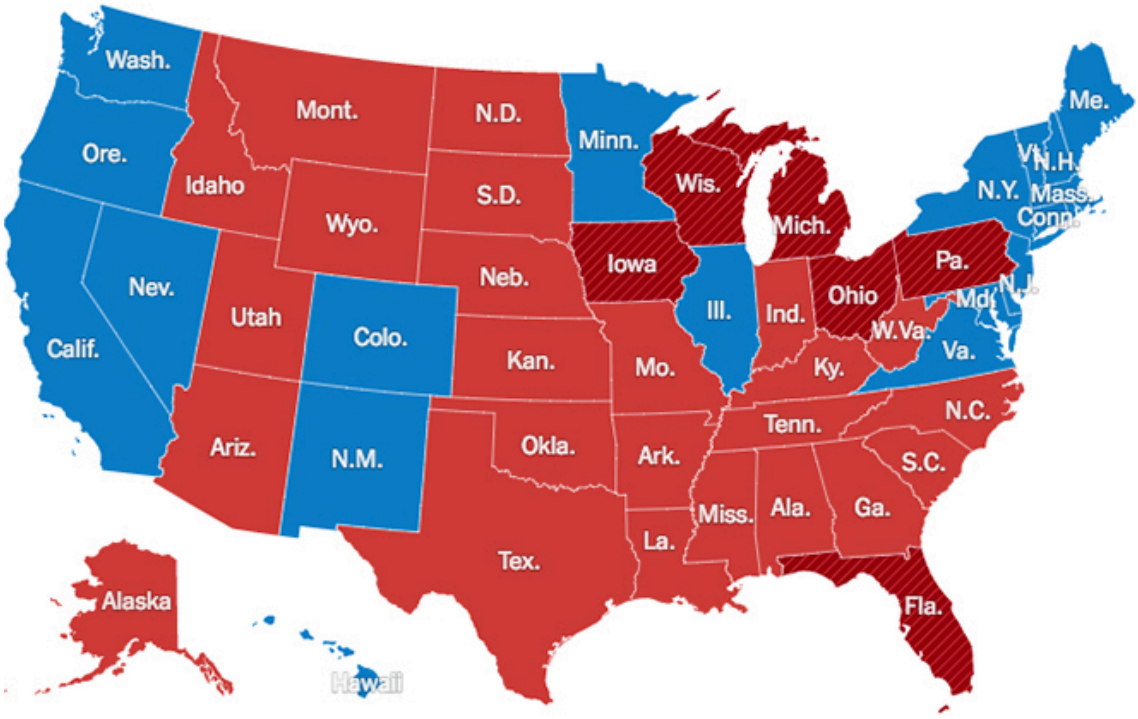

Figure 6: 2016 election results.[141]

By all accounts, polling suggested that Clinton was a clear favorite to secure most battleground states. They were populated with Black and Latinx voters, who traditionally leaned left, and young college-educated voters, who vastly supported Bernie Sanders in the primary and were predicated to vote blue.[142] But political pundits and Clinton's campaign were shocked to see the voter results, with scores of veterans and evangelicals outvoting young liberals. These were the same demographics targeted by Russian disinformation schemes.

[140] Jamieson.
[141] "2016 Election Results." *The New York Times.* 2016.
[142] Jamieson.

Mobilizing Evangelicals and Veterans

While evangelicals and veterans traditionally supported Republican candidates, the Trump campaign feared neither demographic would turn out to vote. In early 2016, evangelicals were not expected to comprehensively support Trump. The Pew Research Center found that 44 percent of white evangelical voters discredited his candidacy, as Trump was "not at all religious." 55 percent were dissatisfied with the choice of presidential candidates, and 42 percent agreed that "it will be difficult to choose between Trump and Clinton because *neither one* would make a good president."[143] Meanwhile, veterans showed a lack of enthusiasm for Trump, as he only led by 10 points over Clinton—in 2012, Mitt Romney outperformed Barack Obama by 20 points.[144]

To win Michigan, Pennsylvania, and Wisconsin, Trump had to ensure evangelicals and veterans arrived in droves to the polls. This was safeguarded by the rhetoric in Russian-backed disinformation social media accounts. Groups like "South United" and "Heart of Texas," both Facebook communities with veterans and religious voters from across the United States, featured media with Bible quotes, religious imagery, and anti-Clinton articles describing her hatred towards the military. RT videos that claimed Clinton was corrupt and anti-Christian were circulated in these spheres, as well as articles posted on Russian-backed conservative news outlets. One post on Facebook claimed that, "at least 50,000 homeless veterans are starving dying in the streets, but liberals want to invite 620,000 refugees and settle them among us."[145] A

[143] Pew Research Center. "Faith and the 2016 campaign." 2016.
[144] Hartig, Hannah et al. "Poll: Trump leads Clinton." 2016.
[145] Facebook user: Patriotus. "At least 50,000." 2016.

Russian Instagram account, "American.veterans," posted an image of a crying woman that was viewed over 17,654 times, writing that "Killary Clinton will never understand what it feels like to lose the person you love for the sake of your country."[146]

Inflammatory posts, similar to these, were concentrated in Philadelphia, Detroit, and Milwaukee in an effort to increase voter turnout for religious conservatives. In the months leading to the election, posts increased tenfold. Ultimately, 81 percent of evangelicals and 60 percent of veterans voted for Trump in 2016, two demographics in which he outperformed all of the previous Republican candidates in the past 20 years.[147] While this turnout certainly helped Trump win the election, it was more of an insurance policy. Russian operatives' greater victory was using disinformation to suppress millions of votes.

Disenfranchising Black Voters

Since 1996, Black voters have historically remained one of the largest demographics to turn out and vote in each election, despite constant efforts of the Republican party to suppress them. While white voter turnout consistently fell, Black turnout was the opposite; non-Hispanic white voters fell from 67.2% in 2004 to 64.1% in 2012.[148] Meanwhile, Black voters increased from 60% to 66.2%, and thereby surpassing white voter turnout.[149] But in 2016, Black voters fell to 59.4%, the lowest it had been since 2000, while every other demographic increased.[150]

---

[146] Jamieson.
[147] CNN. "Exit polls 2016." 2016.
[148] Kamarack.
[149] Pew Research Center. "Voting Turnout." 2016.
[150] Ibid.

Black communities were drowned in disinformation online leading up to the election. The "Blacktivist" Facebook group generated 11.2 million interactions in the six months before the 2016 election, and the "Woke Blacks" page was viewed over 307,000 times.[151] Many of these accounts touched on Clinton's "super predator" characterization from 1996, as well as the extreme increase of Black incarceration after Bill Clinton's administration. Fake ads were shared to voters of color encouraging them to vote from home or not cast a ballot at all. One Russian user posted "no one represents Black people. Don't go to vote. Only this way we can change the way of things…" which was interacted with 8,500 times.[152] The "Woke Blacks" page told its followers that "We'd surely be better off without voting AT ALL" because "A particular hype and hatred for Trump is misleading the people and forcing Blacks to vote Killary. We cannot resort to the lesser of two devils."[153]

During the Federal investigations into the Russian disinformation attacks, Congress determined that Black voters were targeted at an exponentially greater extent than any other group. The Committee:

> found that no single group of Americans was targeted by IRA information operatives more than African Americans. By far, race and related issues were the preferred target of the information warfare campaigns designed to divide the country in 2016.[154]

The Mueller investigation came to the same conclusion. Ultimately, Trump's margin of victory was reduced to three counties in Michigan, Pennsylvania, and Wisconsin, all of which were counties with high populations of color.

[151] Select Committee on Intelligence.
[152] Jamieson.
[153] Berman, Ari. "Russians Tried to Suppress." 2018.
[154] Select Committee on Intelligence.

Voting Breakdown in 2016

State	Statewide Clinton vote	Statewide Trump vote	Trump margin of victory	Difference from 2012 to 2016 in key counties
Michigan	2,268,839	2,279,543	10,704	Wayne County: 76,402
Pennsylvania	2,926,441	2,970,733	44,292	Philadelphia County: 4,781
Wisconsin	1,382536	1,405,284	22,748	Milwaukee County: 43,616

Election results by state.[155]

The Democratic vote fell drastically in three counties which Clinton narrowly lost and Obama dominated in 2012. And in two of these three states, Trump's margin of victory equates the difference in voter turnout in that same county. Had Clinton performed as expected, she would have won all three states and the election itself. Instead, evangelical Christian and veteran voters overperformed, and Black representation sharply declined. Consequentially, the same demographics encouraged to stay home and not vote by IRA disinformation drastically fell in turnout rates as well.

From Sanders to Stein

The third demographic significantly targeted were young, college-educated liberals. The Mueller indictment described that the IRA specifically attempted to enrage former Sanders supporters through an incessant stream of content alleging that Clinton rigged the primaries, that the Democratic Party manipulated the results, and that Bernie

[155] Kamarack.

Sanders was set up to fail because of Clinton's financial corruption within the DNC.[156] Young liberals were encouraged to either stay home and not vote or vote for third-party candidate Jill Stein. RT shared videos describing Stein as a likely alternative to Clinton, one which stood a chance at winning the election.[157]

The Stein rhetoric was spread throughout disinformation bots. The "Blacktivist" Facebook page posted "Choose peace and vote for Jill Stein," which received 18,888 impressions.[158] A commentor, whose account was also linked to a Russian bot, replied "trust me, it's not a wasted vote…. The only way to take our country back is to stop voting for the corporations and banks that own us."[159] Additionally, RT posted more than 100 stories on-air and online supporting Stein, even interviewing her personally.[160] Many of the left-leaning progressive social media communities which these were disseminated through also witnessed stories that claimed Clinton was involved with Al-Qaeda and armed ISIS, exploited the Benghazi incident, and perpetuated the fake news report that she ran a pedophile ring in a Washington, D.C. pizza shop.[161]

Not only did these voters support Stein in the election, but some of them even flipped and voted for Trump. 12 percent of voters who supported Sanders in the primary voted for Trump in November—most of these switches were concentrated in Michigan, Wisconsin, and Pennsylvania.[162] Additionally, while voters 18-29 years old had the most supporters for Sanders in the primaries, they also had the lowest turnout rate in the

[156] Mueller.
[157] Jamieson.
[158] Ibid.
[159] Ibid.
[160] Tracy, Abigail. "Washington's Russia circus comes for Jill Stein." 2017.
[161] Kamarack.
[162] Le Miere, Jason. "Bernie Sanders Voters." 2017.

2016 election as a whole.[163] According to a study from The Cooperative Congressional Election Committee, "four out of every five Obama-to-nonvoters identify as Democrats, and 83 percent reported they would have voted for a Democrat down-ballot" had they voted.[164]

These disinformation schemes worked in perfect harmony with each other and necessitated a delicate political environment to succeed. By embedding distrust and infuriation within right-wing communities, disenfranchising Black voters, and indoctrinating young progressives with pro-Stein literature, Russia and the Internet Research Agency capitalized on an already fragile political ecosystem in the United Stattes. On November 8, 2016, white conservatives arrived in droves at the ballot box, prepared to defend their country from a corrupted, anti-military politician entrenched in the Washington swamp. Meanwhile, Black voters and young progressives in Pennsylvania, Michigan, and Wisconsin remained home or cast a ballot for Sein. All three groups were unreservedly unaware that their trusted timelines and social media communities were riddled with disinformation and fake news engineered to illicit their exact reactions.

Collusion? Connections to the Trump Campaign

Currently, it is still unknown if the Trump campaign colluded with Russia and the Internet Research Agency in 2016. The Mueller investigation was unable to come to a formal conclusion to the criminality of Trump's connections with the Kremlin, but federal investigations are still ongoing. Several key individuals in the campaign have

[163] Jamieson.
[164] McElwee, Sean et al. "The Missing Obama Millions." 2018.

admitted to meeting with Russian officials, including Donald J. Trump Jr., Paul Manafort, Jared Kushner, Jeff Sessions, and Michael T. Flynn. Sessions recused himself from the federal investigation after it was revealed he lied during his confirmation hearing, originally claiming that he never communicated with the Russians during the campaign despite later admitting to meeting with Sergey Kislyak, Russia's former ambassador to the United States. Manafort plead guilty to conspiracy to launder money and failure to register as a foreign agent, as he was allegedly paid millions of dollars by Russian operatives as an unregistered lobbyist. Richard Gates, a key operative in Trump's campaign, also admitted to defrauding the United States during the election and lying to federal investigators.[165]

While much remains unknown, it is clear that Putin's and Trump's interests were aligned throughout the campaign. Russia began disseminating disinformation through its troll accounts during the Republican primaries, working within conservative groups online to discredit Ted Cruz and Jeb Bush.[166] And despite what Trump's adversaries may claim, their campaign exploited the same groups as the Russians while working with the computer research consulting firm, Cambridge Analytica.

Like the Internet Research Agency, Cambridge Analytica relied on artificial intelligence and social media data to profoundly learn how most American voters behaved. This was characterized as microtargeting: using hundreds of data points to master what a user needs to hear to vote a certain way. Cambridge Analytica coordinated the spread of Russian disinformation using its microtargeting schemes and utilized the algorithms within each social media platform to better disseminate the

[165] Mueller.
[166] Select Committee on Intelligence.

disinformation on a wider scale. Cambridge Analytica, while working for the Trump campaign, used the data of over 50 million Facebook users to microtarget Russian disinformation to each user.[167] While Cambridge Analytica may now be defunct, their microtargeting shared disinformation-based ads to billions of viewers, resulting in a "Google manipulation" unlike any other communication method used in a political campaign ever before.[168]

So, Was the Election Rigged?

Like everything else in contemporary society, technology has shattered the norms defining election manipulation. The public sphere has merged into cyberspace, and it is impossible to separate a successful political campaign from its manipulated digital strategy. It may be unclear what, if any, impact the Russian trolls had on the election results itself. While specific votes were not tampered with or altered, there is no denying the influence Russian information warfare had on the American public in 2016. The sheer amount of disinformation, designed to illicit inflammatory and divisive reactions, contributed to a political climate that was partisan, radical, and incredibly sensitive.

Social media is powerful not because it forces people to act in certain ways, but because it *influences* them to. Digital communities have become, to many, more reliable and comforting than the humans they interact with daily. Many of us learn about the news, discover new ideas, meet new people, sustain ourselves, and find consolation through the Internet. We have been conditioned to appreciate and depend upon what we

[167] Mueller.
[168] Lewis, Paul and Paul Hilder. "Leaked: Cambridge Analytica's blueprint." 2018.

see online, because we believe that our digital neighborhoods are our true friends and trusted communities. This is what defines the 21st century human experience.

In 2016, the Russian government used this against the American public. Aware that most users accept what is presented to them online as factual, the IRA engineered media to convince Americans of a fake reality. This reality was seemingly no different than our normal interactions with content and users online, but was designed to manipulate our behavior, to motivate us to act in a way we believed to be normal and right. And in the end, we acted just as they predicted us to.

What happened in 2016 may not have been a traditional act of war, but it was still an attack on the American public. These disinformation accounts resulted in increased political animosity, polarization, and radicalism across the country, and they also elected a President who was all but endorsed by Putin. Russia had a long and extensive history of influencing elections to help its own interests; the 2016 election was an exhibition to see how powerful their tactics could actually be.

VII. The New Normal?

The 2016 election was only a premonition of what is to come. As technology continues evolving at a radical rate and machine learning capabilities innovate exponentially, technology will only make it easier to act nefariously, be it by a private individual or foreign adversary. Since 2016, more than 80% of the disinformation troll Twitter accounts are still active, publishing more than a million tweets each day.[169] And despite a national awareness of Russian election interference, little has been done to amend the crimes. Is this the new normal? Or can technology be reformed to promote digital civility and justice?

The 2020 Election

After Trump's victory in 2016, the American public was warned against continued attempts to influence the election with disinformation. Many of the Russian troll accounts were still active and posting fervidly against Joe Biden.[170] These bots shifted their message from 2016 in response to the current political climate, often attempting to prevent voters from using mail-in ballots, or by instructing liberal communities that they could submit their mail-in ballot later than their state actually accepted. Some communities received robocalls produced by Russian operatives, with one even claiming that

> did you know that if you vote by mail your personal information will be part of a public database that will be used by police departments to track down old warrants and be used by credit card companies to collect outstanding debts? Don't be finessed into giving your private information to the man. Stay safe and beware of vote-by-mail.[171]

[169] Select Committee on Intelligence.
[170] Ibid.
[171] Fessler, Pam. "Robocalls, Rumors and Emails." 2020.

There were also reports that ballot drop-boxes were changed, QR codes had been altered, or that deadlines were switched for voters to submit their ballots. All of these were traced back to malicious foreign adversaries attempting to sway the election.

However, the nation was focusing its attention on domestic-based disinformation, rather than foreign interference. QAnon, a conspiracy movement that originated as an online forum in 2019, claimed to utilize a similar method of information warfare employed by the Russians in 2016. However, QAnon relabeled these tactics as "meme warfare," with one user describing that

> part of the 2020 memewar NEEDS to be strategically targeting these now VERY VULNERABLE democrats with memes so that not only are they voted out of office but democrats lose the House… Don't forget that we are waging an information war, and this and the 2020 memewar are part of it.[172]

By rebranding Russian information warfare into a more niche and effective scheme, QAnon reclaimed this form of digital terrorism and made it more impactful and community oriented. In February 2020, even Trump retweeted QAnon accounts over 70 times, once even 20 times in one day.[173]

A majority of Americans were unable to identify disinformation that was embedded by QAnon during the election. One-third of Americans believed that Joe Biden wielded voter fraud schemes against conservatives to win the election, a widespread conspiracy theory spread by QAnon supporters.[174] 40% of Americans argued that COVID-19 was created by Chinese operatives to gain global power.[175] And 47% thought that the 2020 Black Lives Matter protests were overtly violent, despite

[172] Thomas, Elise. "Qanon Deploys 'Information Warfare.'" 2020.
[173] Ibid.
[174] Rose, Joel. "Even If It's 'Bonkers.'" 2020.
[175] Ibid.

significant testimony arguing the opposite.[176] And as QAnon garners more national support, 39% of Americans believe that Trump is undermined by a deep state comprised by the political elite, including Obama, Clinton, and Biden.[177]

While foreign disinformation efforts did not win Trump the presidency in 2020, they did not disappear from national politics either. In July 2020, American intelligence officials reported that China, Russia, and Iran were all attempting to influence the 2020 election results in a similar manner to 2016.[178] Russia and Iran were accused of "spread[ing] disinformation in the U.S." to "undermine confidence in our democratic process" on social media.[179] Chinese officials were accused of using disinformation to "shape the policy environment in the United States" based on China's interests.[180] As of April 2021, the details of these three campaigns, and which politician they worked to elect, remain classified information without much public awareness. However, they indicate a growing interest of state governments to utilize emerging technology in foreign elections—a trend that could change the way the Web is governed forever.

Disinformation is a major threat to the American democracy, regardless of who is wielding it. When utilized properly, it can erode the fabric of our electoral system and promote widespread chaos and corruption. But what can be done to safeguard our democratic processes? Has technology evolved to an unmaintainable point?

[176] Ibid.
[177] Ibid.
[178] Sanger and Barnes.
[179] Ibid.
[180] Ibid.

Can Anything Be Done?

Today, it is clear that the Russian government utilized American social media platforms for the widest spread of disinformation in modern history. More individuals are growing apprehensive to the power social media companies have in their lives and started interrogating how much influence these cyber communities should have in their lives, and in society as a whole. The American democracy was founded on a belief that every individual, regardless of political affiliation or personal beliefs, should be entitled to equitable liberties. Foreign interference and manipulation of our communication systems seizes autonomy from every American who experiences disinformation, and something must be done to better protect the American public of information warfare. As technology evolves and transforms, data and private information will only become more valuable within an economy that operates off of data-based technology.

Artificial intelligence poses a massive and existential threat to democracy. The 2016 election is just a starting point; as technology and machine learning advance, new tools will be used by adversaries to erode the American public sphere. As Elaine Kamarack stated,

> when applied to the actions of governments, many AI innovations are positive; for instance, who would not want faster and better emergency response systems? But when the same technologies are applied to the messy world of politics, the potential for mischief equals or exceeds the potential for good.[181]

Even recently, facial recognition algorithms can manipulate videos to perfectly align people with audio clips from entirely new videos, convincing viewers that the person said something completely different—and altering their reality. And social media

[181] Kamarack.

companies have done little, if anything, to correct the wrongs from 2016. No algorithms have been changed, no new policies implemented, so is there anything that can be done to fix what went wrong?

Kathleen Hall Jamieson, a political scientist from the University of Pennsylvania, argues that journalism norms must be reformed to rebuild trust in the media. With more reliable media sources, the public will be less inundated by fake news and disinformation.[182] While this is a worthwhile argument—trust in journalism should be restored, regardless—it does little to account for the responsibility of the tech companies creating the algorithms designed to entrench users. Under Jamieson's model, Americans will rely upon local journalists and media sources, but still be vulnerable to high-quality disinformation, like what was used in 2016.

Others, like Elaine Kamarck from the Brookings Institution, emphasizes the reformation of political parties as the linchpin to solving the disinformation crisis. If campaigns simply stop using foreign operatives of disinformation schemes to advertise their candidate, then significantly less fake news will be circulated online. Campaigns that do not follow these guidelines will be sanctioned or criminalized, ultimately placing the burden on each candidate to ensure they are playing by the rules.[183] What Kamarack fails to consider, however, is how this will do little to prevent foreign interference in elections. Even today, four years after the 2016 election, the federal government is still unable to determine if Trump played a role in Russia's electoral attack. If little evidence can corroborate this connection, then it is highly unlikely that a political party will be willing to identify, if it can identify at all, their candidate's

[182] Jamieson.
[183] Kamarack.

collusion with a foreign power. Regardless of how vigilant the Democratic or Republican parties may be, sanctions will do little to deter foreign officials committed to furthering their interests.

Unfortunately, in the world of tech policy, it is impossible to regulate innovation before invention. While some policies, like Section 230 of the Stored Communications Act, may improve over time and find additional applications in new political discourses, the government is unable to research, draft, and pass tech policy before the technology itself has been disseminated on a broad scale. While policy to protect civil society from electronic disinformation would be ideal, its likely improbable within the near future.

Tech norms must shift to begin enacting systemic change. Historically, a line has always divided consumers from citizens—but technology is erasing that line. Users must be protected through national policy, ethical technology, and algorithms that promote transparency and autonomy. This norm would promote just practices and prevent disenfranchisement across civil society.[184] Companies throughout the tech industry, from social media platforms to automated employment software companies, utilize algorithms to streamline almost every output. Even local governments have used algorithms to identify accurate bail and parole decisions, as well as to decide police assignments.[185] While these algorithms make work easier, they are also landmines for misbehavior and abuse. Ethical algorithms should be mainstreamed to ensure the tech industry promotes and advocates for fairness, regardless of who may be using their devices. By reforming the algorithms operating the sites, disinformation will be less likely to spread, and cyberspace will become more fruitful and equitable as a whole.

[184] Leong and Jordan.
[185] Kearns and Roth.

Experts working in technology ethics agree that norms must shift to prioritize data privacy. By rebuilding community standards, both technology companies and governments will have a clearer role with prioritizing the digital rights of every user. This can only be achieved through a regulation of technology, enacting new tech policies, creating legal boundaries, and establishing systemic ethical practices for large companies.[186] Reforming AI and machine learning necessitates federal guidance and formal legal boundaries, but norms cannot be legislated either. All four components must be achieved to address ethical issues arising from technological change.[187]

Additionally, tech companies, like Facebook and Twitter, must be held accountable for the harm they caused in 2016. Despite being passive throughout the election, research shows that executives at Facebook and Twitter were complicit in aiding the IRA with information to perfect their strategies of disseminating disinformation, primarily through a detailed description of the operating algorithms.[188] As Big Tech companies, like Facebook and Amazon, continue to grow, they entrench the industry with monopolies and corruption. In order to promote fairness and transparency, Big Tech companies involved in the 2016 election interferences must be regulated and found liable for their passive role they played in the disinformation warfare.

Without competition, Big Tech companies will only grow bigger and more powerful, thereby controlling more of cyberspace than they do now.[189] Most recently, Twitter and Amazon were scrutinized for silencing QAnon supporters after the January

[186] Leong and Jordan.
[187] Ibid.
[188] Select Committee on Intelligence.
[189] Yglesias, Matthew. "The push to break up Big Tech." 2019.

6th Capitol Hill unrest—while these censors calmed many who were concerned over the growing influence of alt-right conspiracy theories, it also concerned tech policy professionals fearful of unlimited power for Big Tech. When there is no line drawn limiting the power of industry giants, the government must draw that line.[190] Only then will tech companies and social media platforms begin protecting their users against data hacks and disinformation tactics.[191]

Finally, the fight against foreign disinformation must be undertaken globally. For decades, Russian operatives worked to wield disinformation against burgeoning democracies and its political adversaries. Recently, more countries have begun to do the same, with the federal government reporting Iranian and Chinese interference in the 2020 election.[192] Without reformed global norms preventing cyber and information attacks, these infiltration schemes will only proliferate. Just like the norms that delineate warfare and economic relations, some form of international guideline must be established to normalize digital transparency and cyber freedoms. Without it, states will only continue to utilize technology to perpetuate their interests, despite what it might cost another country.

What happened in 2016 should scare the American public, but it should also motivate lawmakers to establish formidable norms promoting digital liberties through policy and partnerships. Technology's impact on civil society has long been ignored by policy makers and technological scholars, but with an ever-blurring line between the two, a reckoning impends over Washington, D.C. and Silicon Valley. All citizens are

[190] Dwork and Mulligan.
[191] Leong and Jordan.
[192] Sanger and Barnes.

now consumers, and all consumers are owed a burden of care from their retailers. Until tech companies are held accountable to reformed norms, Russian disinformation warfare will only evolve through new technologies and innovation. The 2016 election may have been tampered with, but until we protect our cyberspace, every election that is to follow is doomed to the same fate.

Bibliography

2016. "2016 Election Results." The New York Times. *The New York Times.*

Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 election." *Journal of Economic Perspectives* 211-236.

Anyoha, Rockwell. 2017. "The History of Artificial Intelligence." *Harvard University.* August 28.

2017. *Assessing Russian Activities and Intentions in Recent US Elections.* Intelligence Community Assessment, National Intelligence Council.

Auxier, Brooke, Lee Raine, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Infromation.* Reporot, Pew Research Center.

Bagrow, James P., Xipei Liu, and Lewis Mitchell. 2019. "Information flow reveals prediciton limits in online social activity." *Nature Human Behavior* 122-128.

Barthel, Michael. 2019. *5 key takeaways about the state of the news media in 2018.* Study, Pew Research Center.

Bergdahl, Jacob. 2019. "How AI Can Make You The President." *Towards Data Science*, June 3.

Berman, Ari. 2018. "Russians Tried to Suppress Minority Turnout, Spread Lies About Voter Fraud." *Mother Jones*, February 16.

Berners-Lee, Tim. 2000. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web.* Harper Business.

Blacktivist, Facebook user:. 2016. "Choose peace and vote for Jill Stein." *Facebook.* November 3.

Bogle, Ariel. 2018. "How the internet tricks you out of privacy using 'dark patterns' of desigb." *ABC Science*, April 29.

Bostrom, Nick, and Eliezer Yudkowsky. 2014. "The Ethics of Artificial Intelligence." In *Cambridge Handbook of Artifical Intelligence*, by Ed. Keith Frankish and William Ramsey. New York: Cambridge University Press.

Boyd, Dana, and Kate Crawford. 2011. "Six Provocations for Big Data." *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society.* Oxford: Oxford Internet Institute, Oxford University.

Casey, Adam, and Lucan Ahmad Way. 2017. *Russian Electoral Interventions, 1991-2017.* Dataset, University of Toronto.

CNN. 2016. "Exit polls 2016." *CNN*, November 23.

2018. *Colin Kaepernick, Blactivist Ad.* Senate Intelligence Committee.

Crowley, Michael. 2016. "Why Putin hates Hillary." *Politico*, June 25.

C-SPAN. 2017. *FB, Google, Twitter Exec on Russian Disinformation Opening hearing.* Comp. Charles E. Grassley.

Cuthbertson, Richard, Peder Inge Furseth, and Stephen J. Ezell. 2015. "Facebook and MySpace: The Importance of Social Networks." *Innovating in a Service-Driven Economy.*

Daley, Beth. 2020. "Do social media algorithms erode our ability to make decisions freely? The jury is out." *The Conversation*, October 11.

DataGuidance & Future of Privacy Forum. 2019. *Comparying privacy laws: GDPR v. CCPA.* Report, DataGuidance & Future of Privacy Forum.

Decker, Allie. 2020. "Instagram Marketing." *HubSpot.*

Doyle, Aine. 2019. "Tracking "Fake News:" The Printing Press, Social Media, and Politics." *The Criterion* 53-62.

Dwork, Cynthia, and Deirdre K. Mulligan. 2013. "It's Not Privacy, and It's Not Fair." *Stanford Law Review.*

Eddington, Patrick. 2019. "The Snowden Effect, Six Years On." *Just Security*, June 6.

Facebook user: Patriotus. 2016. "At least 500,000 homeless veterans are starving dying in the streets, but liberals want to invite 620,000 refugees and settle them among us." *Facebook.* September 8.

Fessler, Pam. 2020. "Robocalls, Rumors and Emails: Last-Minute Election Disinformation Floods Voters." *National Public Radio*, October 24.

Girish, Davika. 2020. "'The Social Dilemma' Review: Unplug and Run." *The New York Times*, September 9.

Gramlich, John. 2019. "10 facts about Americans and Facebook." *Pew Research Center*, May 16.

Hadley, David P. 2019. *The Rising Clamor: The American Press, the Central Intelligence Agency, and the Cold War.* Louisville, KY: The University Press of Kentucky.

Hafner, Katie. 1996. *When Wizards Stay Up Late: The Origins of the Internet.* New York: Simon and Schuster.

Halpern, Sue. 2018. "Cambridge Analytica and the Perils of Psychographics." *The New Yorker*, March 30.

Harnik, Andrew. 2017. *Aziz Ansari Photoshop.* Associated Press.

Harttig, Hannah, John Lapinski, and Stephanie Psyllos. 2016. "Poll: Trump Leads Clinton Among Military Households." *NBC News*, August 16.

2017. *Heart of Texas, Veteran Approval Rating.* US Senate.

Higgins, Andrew. 2017. "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote." *The New York Times*, February 16.

Institute of Politics, Harvard Kennedy School. 2017. *Campaign for President: The Manager Look at 2016.* Rowman and Littlefield.

Jamieson, Kathleen Hall. 2018. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President.* New York: Oxford University Press.

Jha, Manu Siddharth. 2019. "How AI and Machine Learning Can Win Elections." *Great Learning Blog*, December 17.

Kalugin, Oleg, interview by CNN. 1998. *Inside the KGB: An interview with retired KGB Maj. Gen. Oleg Kalugin* (January).

Kamarck, Elaine. 2018. *Malevolent soft power, AI, and the threat to democracy.* Report, Washington, DC: Brookings Institute.

Kapoor, Kawaljeet Kaur, Kuttimani Tamilmani, Nripendra P. Rana, Pushp Patil, Yogesh K Dwivedi, and Sridhar Nerur . 2018. "Advances in Social Media Research: Past, Present and Future." *Information Systems Frontiers* 531-558.

Kearns, Michael, and Aaron Roth. 2020. *Ethical algorithm design should guide technology regulatiton.* Report, Brookings Institute.

Kelly, John. 2018. *Hearing before the Senate Select Committee on Intelligence* (August 1).

Kirkpatrick, David D. 2017. "Signs of Russian Meddling in Brexit Referendum." *The New York Times*, November 15.

Krootoszynski Jr., Ronald J. 2015. "Reconciling Privacy and Speech in the Era of Big Data: A Comparative Legal Analysis." *William & Mary Law Review* 1279-1338.

Le Miere, Jason. 2017. "Bernie Sanders Voters Helped Trump Win and Here's Proof." *Newsweek*, Augustt 23.

Leong, Brenda, and Sara Jordan, interview by Emily Fowler. 2021. *Freedom of Privacy Foundatioon* (January 26).

Lewis, Paul, and Paul Hilder. 2018. "Leaked: Cambridge Analytica's blueprint for Trump victory." *The Guardian*, March 23.

McElwee, Sean, Jesse H. Rhodes, Brian F. Schaffner, and Bernard L. Fraga. 2018. "The Missing Obama Millions." *The New York Times*, March 10.

Meola, Andrew. 2020. "Analyzing Tik Tok user growth and usage patterns in 2020." *Business Insider*, February 12.

Miere, Jason Le. 2018. "Russia Election Hacking: Countries Where the Kremlin Has Allegedly Sought to Sway Votes." *Newsweek*, May 9.

Miller, Jennifer M. 2019. "Democracy and Misinformation: The Cold War and Today." *Perspectives on History, American Historical Society.*

Mueller, Robert S. 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* Federal investigation, US Department of Justice.

National Security Council Report 68. April 14, 1950. *United States Objectives and Programs for National Security.* National Security Council.

Naughton, John. 2000. *A Brief History of the Future: Origins of the Internet.* Orion.

Paisley, Laura. 2016. "Political polarization at its worst since the Civil War." *University of Southern California*, November 8.

Parham, Jason. 2017. "Russians posing as black activists on Facebook is more than fake news." *WIRED*, October 18.

Parkinson, Joe, and Georgi Kantchev. 2017. "Document: Russia Uses Rigged Polls, Fake News to Sway Foreign Elections." *The Wall Street Journal*, March 23.

Paul, Christopher, and Miriam Matthews. 2016. "The Russian 'Firehouse of Falsehood,' Propaganda Model." *RAND Corporatiton.*

Perrault, Raymond, Yoav Shoham, Erik Brynjolfsson, Jack Clark, John Etchemendy, Barbara Grosz, Terah Lyons, James Manyika, Saurabh Mishra, and Juan Carlos Niebles. 2019. *The AI Index 2019 Annual Report.* Annual Report, Stanford, CA: AI Index Steerling Committee, Human-Centered AI Institute, Stanford University.

Petrescu, Maria, and Anjala S Krishen. 2020. "The dilemma of social media algorithms and analytics." *Journal of Marketing Analytics* 187-188.

Pew Research Center. 2016. *Faith and the 2016 campaign.* Poll, Pew Research Center.

Pew Research Center. 2017. *The Partisan Divide on Political Values Grows Even Wider.* Study, Pew Research Center.

Pew Research Center. 2016. *Voter Turnout By Population, November 2016 and Earlier Years.* Report, Pew Research Center.

Podesta, John. 2014. *Big Data and the Future of Privacy.* Federal report, Washington, DC: The Obama Administration.

Reinbold, Fabian. 2017. "Germany Prepares for Possible Russian Election Meddling." *Spiegel International*, September 7.

Robinson, Meyer. 2018. "The Grim Conclusions of the Largest Ever Study of Fake News." *The Atlantic*, March 8.

Rose, Joel. 2020. "Even If It's 'Bonkers,' Poll Finds Many Believe QAnon And Other Conspiracy Theories." *National Public Radio*, December 30.

Rosenberg, Matthew, Nicholas Confessore , and Carole Cadwallader. 2018. "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times*, 17 March.

Rotenberg, Marc. 2012. "The Reform of the EU Data Protection Framework—Building Trust in a Digital and Global World." *Committee of the European Parliament on Civil Liberties, Justive, and Home Affairs.* Brussels: European Parliament.

Sanger, David E., and Julian E. Barnes. 2020. "U.S. Warns Russia, China and Iran Are Trying to Interfere in the Election. Democrats Say It's Far Worse." *New York Times*, August 18.

—. 2020. "U.S. Warns Russia, China and Iran Are Trying to Interfere in the Election. Democrats Say It’s Far Worse." *The New York Times*, July 24.

Sanger, David E., and Nicole Perlroth. 2020. "Trump Contradicts Pompeo Over Russia's Role in Hack." *The New York Times*, Decemmber 19.

Select Committee on Intelligence. 2020. *Russian Active Measures Campaigns and Interference in the 2016 US Election Volume 2: Russia's Use of Social Media with Additional Views.* Committee Report, 116th Congress.

Silverman, Craig. 2016. "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook." *Buzzfeed News*, November 16.

Silverman, Craig, and Lawrence Alexander. 2016. "How Teens in the Balkans are Duping Trump Supporters with Fake News." *BuzzFeed News*, November 3.

Smidi, Adam, and Saif Shahin. 2017. "Social Media and Social Mobilisation in the Middle East: A Survey of Research on the Arab Spring." *India Quarterly*, June 12.

Smith, Chris, Brian McGuire, Ting Huang, and Gary Yang. 2006. *The History of Artificial Intelligence.* Report, Seattle: University of Washington.

Soll, Jacob. 2016. "The Long and Brutal History of Fake News." *Politico Magazine*, December 18.

2018. "South United Screenshot." New York Times. *New York Times.*

Staats, Arthur W. 1975. *Social Behaviorism.* Homewood, IL: Dorsey.

Standage, Tom. 2014. *Writing on the Wall: Social Media — The First 2,000 Years.* Bloomsbury.

Thomas, Elise. 2020. "Qanon Deploys 'Information Warfare' to Influence the 2020 Election." *Wired*, Febrary 17.

Tolstrup, Jakob. 2014. "Black knights and elections in authoritarian regimes: Why and how Russia supports autthoritarian incumbents in post-Soviet states." *European Consortium for Political Research.*

—. 2013. *Russia vs. the EU: The Competition for Influence in Post-Soviet States.* Boulder, CO: Lynne Rienner Publishers.

Tracy, Abigail. 2017. "Washington's Russia circus comes for Jill Stein." *The Atlantic*, December 19.

2017. "TV News Broadcasters: Comparative Social Media Footprint." Intelligence Community. *Assessing Russian Activities and Intentions in Recent US Elections.*

Twitter. 2018. "Update on Twitter's review of tthe 2016 election." *Twitter Public Policy Blog*, January 19.

United States v. Internet Research Agency, et al. 2018. 1:18-cr-000320-DLF (D.D.C., February 16).

van Dijck, José. 2013. *The Culture of Connectivity: A Critical History of Social Media.* Oxford: Oxford University Press.

Wheeler, Tom, Phil Verveer, and Gene Kimmelman. 2020. "The need for regulation of big tech beyond antitrust." *Brookings Institute.*

Woolley, Samuel, and Douglas Guilbeault. 2017. *Computational Propaganda in the United States of America: Manufacturing Consensus Online.* Report, Oxford Internet Institute Computational Propaganda Research Project.

Yglesias, Matthew. 2019. "The push to break up Big Tech, explained." *Vox*, May 3.