Mitigating Foreign Social Media Influence Campaigns in U.S. Elections

by

Daniel Wade Provaznik II

B.S. Systems Engineering
United States Military Academy at West Point, 2018

SUBMITTED TO THE INSTITUTE FOR DATA, SYSTEMS, AND SOCIETY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Science in Technology and Policy
at the
Massachusetts Institute of Technology

September 2020

© 2020 Massachusetts Institute of Technology. All rights reserved.

Signature of Author: ...........................................................................................................

Institute for Data, Systems, and Society
August 17, 2020

Certified by: ...............................................................

Joel F. Brenner
Senior Research Fellow, MIT Center for International Studies
Thesis Co-Supervisor

Certified by: ...............................................................

Cagri K. Dagli
Technical Staff, MIT Lincoln Laboratory
Thesis Co-Supervisor

Accepted by: .............................................................

Noelle E. Selin
Director, Technology and Policy Program
Associate Professor, Institute for Data, Systems, and Society
and Department of Earth, Atmospheric, and Planetary Science
Mitigating Foreign Social Media Influence Campaigns in U.S. Elections

by

Daniel Wade Provaznik II

B.S. Systems Engineering
United States Military Academy at West Point, 2018

SUBMITTED TO THE INSTITUTE FOR DATA, SYSTEMS, AND SOCIETY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN TECHNOLOGY AND POLICY
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Abstract

The 2016 U.S. presidential campaign was rife with scandal, the greatest of which the Department of Justice exposed in detail in a 2018 indictment that charged a shadowy Russian organization known as the Internet Research Agency (IRA) with organizing thousands of fictitious individuals and organizations across virtually every social media platform to manipulate the beliefs of real American voters. The goal of this manipulation was to elect then-candidate Donald J. Trump as the 45th President of the United States.

This thesis performs a deep dive analysis into the IRA’s influence campaign on one social media platform: Twitter, and identifies worrying trends in account creation, tweet volume, and tweet content that indicate growing investment into IRA operations. This marked expansion of Twitter activity likely signals growing Kremlin enthusiasm behind social media propaganda and confidence in its ability to affect the beliefs of American citizens.

This data analysis and a full review of the public and private policy landscapes before and after the reveal of IRA operations aims to inform the next round of proposed election security legislation following the 2020 U.S. elections. I conclude by calling upon the upcoming 117th Congress to take immediate action and fulfill its duty to protect the integrity of U.S. democratic institutions in light of Russia’s past attempted interference and chilling reports that the Kremlin has learned from its past mistakes and continues to refine the art of laundering fabricated narratives to undermine democracies around the world.

Thesis Co-Supervisor: Joel F. Brenner
Title: Senior Research Fellow, MIT Center for International Studies

Thesis Co-Supervisor: Cagri K. Dagli
Title: Technical Staff, MIT Lincoln Laboratory
The final few months of my MIT experience did not go as I expected. In December of 2019, I developed the first symptoms of a medical issue known as chronic idiopathic urticaria and angioedema that would radically change the course of my final semester (and my outlook on life). This condition is still poorly understood and has no current cure, but thankfully almost always resolves itself with time. Over the short term, however, the only solution is to manage the symptoms which would vacillate between mildly uncomfortable and completely debilitating. The arrival of COVID-19 and the subsequent move to virtual coursework proved to be a blessing in disguise, as I could still attend classes and finish my last final exam despite feeling so unwell. With the help of an incredible group of Boston medical professionals and the miracle of modern medicine, I’m happy to say that at the time of this writing, I have been symptom free for the last six weeks. I’m grateful for every day of continued good health, and while my future in the Army remains unclear, I’m confident that I can maintain a positive outlook through whatever comes next.

Throughout my time at the Institute, I have been fortunate to build relationships with so many incredible individuals who have helped me more than I deserved:

First, I’d like to thank Dr. Joel Brenner who agreed to serve as my on-campus thesis adviser despite only spending half his time in Cambridge between trips home to Washington, D.C. His legal and academic background combined with his experience as Senior Counsel at the National Security Agency, head of U.S. counterintelligence under the Director of National Intelligence, and NSA Inspector General made him uniquely suited to advising a thesis that tries to make sense of and respond to a foreign threat that thrives in the space between routine statecraft and open warfare.

I’d also like to thank Cagri “Charlie” Dagli of the Artificial Intelligence Technology and Systems Group at MIT’s Lincoln Laboratory. Charlie personally advocated for my admission to the Lincoln Laboratory Military Fellowship program which ultimately made my MIT degree possible. He introduced me to the world of data analysis and weathered my repeated, exasperated venting over the seriousness of this threat to democracy, while also beating back bureaucratic tuition-related morass. Charlie, thank you for your unwavering support and optimism—it’s meant a lot.

Thank you also to the Technology and Policy Program which continuously forced me to reevaluate my views on life, policy, and politics and for surrounding me with the smartest, most passionate friends that made every day interesting. Special thanks to Barb DeLaBarre for always lending an ear and to Frank Field for his timely advice and sense of fashion.

I would be especially remiss if I did thank my wife, Anna, for her continued love and support over the last two years and especially throughout the last 8 months. She singlehandedly put me back together whenever the symptoms and uncertainty broke me apart. She helped me find the silver linings in every situation and stayed strong for me even in her lowest points. And I should mention, she did all of this while pregnant with our first child, a boy, who will be here literally the day after I submit this thesis. I wouldn’t want anyone else by my side in the upcoming journey that is parenthood. I love you, Anna, and thank you.

Finally, this thesis is dedicated to the grand experiment that is American democracy. While the right to vote was not initially universal in the United States, more than 200 years of progress has yielded a living system built on the principles of representation, inclusion, and individual contribution that ensures every American can make their voice heard. Foreign attempts to manipulate that voice or invalidate its conclusions must be stopped at any cost to preserve the integrity of democracy and its decisions in America.
# Table of Contents

1 Introduction .............................................................................................................................................. 11

2 Foundation: What Happened during and after the 2016 U.S. Presidential Election .............................................. 12
   2.1 The 2016 U.S. Presidential Election ........................................................................................................ 13
   2.2 Russian Involvement in the 2016 U.S. Presidential Election ........................................................................ 19
   2.3 Goals of Russian Involvement .................................................................................................................. 25

3 Data Analysis ............................................................................................................................................... 29
   3.1 Twitter’s Decision to Release Data to the Public ......................................................................................... 29
   3.2 What Twitter Included in Its Release ......................................................................................................... 32
   3.3 Trends in IRA Operations and Perceived Investment .................................................................................. 35
      3.3.1 Trends in IRA Accounts ...................................................................................................................... 35
      3.3.2 Trends in IRA Account Creation ........................................................................................................ 44
      3.3.3 Trends in English IRA Tweets ............................................................................................................ 50
   3.3 Broader Trends in Social Media-based Information Operations .................................................................... 57

4 Policy Review .............................................................................................................................................. 61
   4.1 Policy Landscape Prior to the Exposure of Russian Influence Efforts ....................................................... 61
      4.1.1 Social Media Policies Prior to the Exposure of Russia’s Influence Campaign .................................... 62
      4.1.2 Federal Policies Prior to the Exposure of Russia’s Influence Campaign .......................................... 63
   4.2 Policy Changes Following to the Exposure of Russian Influence Efforts .................................................. 66
      4.2.1 Action Taken by Social Media Platforms ............................................................................................ 66
      4.2.2 Action Taken by the Federal Government .......................................................................................... 71
   4.3 Proposed Policy Responses and Legislation .............................................................................................. 76
      4.3.1 Legislation Proposed in the U.S. House of Representatives ............................................................... 77
      4.3.2 Legislation Proposed in the U.S. Senate .............................................................................................. 89
      4.3.3 Sources of This Legislative Quagmire ............................................................................................... 96

5 Policy Recommendations ........................................................................................................................... 98
   5.1 With a Split Legislature ............................................................................................................................. 98
   5.2 With a United Congress ........................................................................................................................... 100

6 Conclusion and Call to Action ...................................................................................................................... 102
Figures

Figure 1: States with the Smallest Popular Vote Differentials in the 2016 Presidential Election

Figure 2: Twitter Profile of @Crystal1Johnson, an IRA-Controlled Twitter Account

Figure 3: Tweet from @wokeluisa, an IRA-Controlled Twitter Account

Figure 4: Twitter Profile of @TEN_GOP, an IRA-Controlled Twitter Account

Figure 5: Tweet from @Pamela_Moore13, an IRA-Controlled Twitter Account

Figure 6: IRA Twitter Account Creation over Time

Figure 7: Account Creation Language Proportions

Figure 8: Account Creation by Language over Time

Figure 9: English IRA Account Creation over Time

Figure 10: Tweet Language Proportions

Figure 11: English Tweets over Time

Figure 12: Map of IRA Tweets with Location Information

Figure 13: The Cross-Platform IRA Activity Monthly Totals (Twitter on Right Axis)

Tables

Table 1: Top 25 IRA-Controlled Twitter Accounts, Ranked by Follower Count

Table 2: Top 25 IRA-Controlled Twitter Accounts Ranked by Following Count

Table 3: Accounts Opened with Each Creation Language

Table 4: Tweets with Location Information by Language

Table 5: Increase in IRA Activity in the Six-Month Period after the 2016 U.S. Election
1 Introduction

The 2016 U.S. presidential election seemed to offer different versions of America over the next four years, the first: more or less a continuation of President Barack Obama’s administration including active leadership in the international community, the second: a revived prioritization of U.S. domestic affairs with a smaller international footprint. More Americans in the most electorally crucial states desired the latter, electing Donald Trump on November 8th, 2016. However, this diminished American role in the international community apparent appealed to more than just the necessary Americans.

The Russian government, in an attempt to restore the geopolitical stature it maintained during the Cold War, launched a multifaceted campaign to get Donald Trump elected and allow the United States to reduce its own international involvement. In addition to hacking and releasing politically damaging material on then-candidate Trump’s Democratic opponent, Hillary Clinton, and probing the electronic election infrastructure of ___ states for potential vote manipulation and follow-on offensive cyber-attacks, Russian intelligence operatives at the Internet Research Agency waged a war against U.S. domestic opinion, flooding every major social media platform with propaganda designed to boost Donald Trump’s chances of assuming the presidency, while undermining support the rival Clinton campaign.

These social media-based influence operations have been the subject of significant scrutiny and analysis by U.S. government investigations and some independent researchers who have verified the tactics and motives described above. This thesis seeks to identify additional trends in the available data to better inform policies that can stop Russia or any other foreign power from violating the integrity of American democracy again.
2 Foundation: What Happened during and after the 2016 U.S. Presidential Election

The 2016 U.S. presidential election holds a unique place in modern U.S. political history. Following President Barack Obama’s second term, a wide field of candidates from both parties took the campaign trail. Current and former senators, representatives, governors, and others competed against each other for both parties’ nominations. Former Secretary of State Hillary Clinton became the front-runner for the Democratic nomination following a contentious primary against Senator Bernie Sanders. The race for the Republican nomination took an unusual turn when Donald J. Trump declared his intention to run for president. Mr. Trump, a businessman and former reality TV persona, slowly rose to the top of a crowded field, eventually securing the Republican nomination. Both candidates experienced multiple scandals that could have knocked them out of the running in a different race, however, after incriminating emails were leaked about the Clinton campaign, accusations began to swirl that the Russian government was responsible.\(^1\) Amidst this controversy, Americans elected Donald Trump as the 45\(^{th}\) President of the United States by incredibly slim margins.

Three years prior, Russia’s only independent investigative newspaper, \textit{Novoya Gazeta}, reported that it had infiltrated a Russian “troll farm” which “managed hundreds of freelance bloggers” that were paid to comment pro-Kremlin material on Russian-language sites.\(^2\) Several months later, Buzzfeed News published “emails leaked by a mysterious Russian hacker collective” that contained plans to recruit and train “a new cadre of online trolls...deployed to spread the Kremlin’s message on the comments section of top American websites.”\(^3\) Throughout the course of the 2016 U.S. presidential campaign, reports


\(^{3}\) Ibid.
continued to pop up, adding detail to this mysterious Russian organization known as the Internet Research Agency which was purportedly flooding American websites and social media platforms with content often clumsily designed to seem written by an average American.⁴

On July 31, 2016, the Federal Bureau of Investigation (FBI) opened an investigation called “Crossfire Hurricane” into possible Russian interference in the 2016 election.⁵ In February of 2018, the Department of Justice (DOJ) issued an indictment against the Internet Research Agency (IRA) and several associated Russian individuals which revealed a massive coordinated effort of hacking and social media propaganda that aimed to elect then-candidate Trump.

### 2.1 The 2016 U.S. Presidential Election

On June 16th, 2015, Donald J. Trump announced his candidacy for president of the United States.⁶ An unusual candidate, Mr. Trump had never before held an elected position, worked in government, or served in the military.⁷ Instead, his campaign pitched him as a Washington outsider and successful businessman that could shake up Washington, “drain the swamp,” and “Make America Great Again!”⁸ Over the next 13 tumultuous months, then-candidate Trump rose to the top of a crowded Republican field of 22 presidential candidates that included conservative heavyweights like Governors John Kasich and Jeb

---


Bush and Senators Marco Rubio and Ted Cruz. On July 21st, 2016, Donald Trump was formally nominated as the Republican Party’s presidential nominee at the Republican National Convention in Cleveland, Ohio.9

The next day (and only three days prior to the start of the Democratic National Convention), the controversial anti-secrecy organization, Wikileaks, published more than 20,000 emails stolen from the Democratic National Committee (DNC) that revealed apparent, systemic bias against Senator Bernie Sanders’ campaign in favor of Secretary Hillary Clinton’s candidacy.10 These emails exposed conversations in which senior DNC officials derided Senator Sanders and his supporters, conspired to target Senator Sanders’ religious beliefs to undercut his support among religious voters in Kentucky and West Virginia, and preemptively crafted a narrative describing Sanders’ failure to secure the Democratic nomination.11 While these instances of bias occurred late in the primary after Secretary Clinton was well on her way to securing the nomination, they belied “the national party committee’s stated neutrality” and incensed Senator Sanders’ campaign and supporters, deepening the political fractures within a Democratic party already largely divided between its most liberal and moderate members.12 DNC Chairwoman Debbie Wasserman Schultz resigned shortly after this news broke, and the DNC issued a formal apology to “Senator Sanders, his supporters, and the entire Democratic Party for the inexcusable remarks made” by DNC officials in the leaked emails.13, 14 Despite this controversy, Secretary Clinton went on to receive the Democratic presidential nomination

---


12 Ibid.


on July 26, 2016, becoming the first woman to receive a major party nomination in US history. While the chorus of “Bernie, Bernie!” occasionally punctuated the Democratic National Convention proceedings and several dozen Sanders delegates staged a walkout after the official roll call vote, Senator Sanders attempted to unify the Democratic party by calling on his supporters to rally behind Secretary Clinton and retain the White House for the Democratic party.

While both major party candidates had been nominated and an especially contentious primary had finally concluded, the scandals continued in the lead up to the general election. Just over a month before election day, the Washington Post published tapes recorded on the set of “Access Hollywood” in 2005 in which Donald Trump was caught on a hot microphone bragging “in vulgar terms about kissing, groping and trying to have sex with women...saying ‘when you’re a star, they let you do it.'” Bipartisan criticism quickly followed. Democrats immediately seized upon this revelation, framing Donald Trump as unfit for the presidency, and Republicans including Senate Majority Leader Mitch McConnell, Republican National Committee Chairman Reince Priebus, and Speaker of the House Paul Ryan condemned candidate Trump’s language and demanded further apologies. The Trump campaign issued several additional statements over the next few days; however, many of these combined apologies with concurrent attacks on former President Bill Clinton’s impeachment and Hillary Clinton’s previous statements regarding women that had accused her husband of sexual harassment and assault. Incredibly, support for candidate Trump remained firm, dropping only one percentage point according

16 Ibid.
18 Ibid.
to a POLITICO/Morning Consult poll conducted the day following the “Access Hollywood”
tape release.20

Scandal befell Secretary Clinton shortly thereafter. On the same day the Washington
Post revealed the “Access Hollywood” tapes, WikiLeaks published more than 20,000 pages
of emails, allegedly from John Podesta, the chair of Secretary Clinton’s campaign.21 These
e-mails exposed the inner workings of the campaign and kicked off controversy about
Hillary Clinton’s ties to Wall Street and the leak of several town hall questions to the
Clinton campaign by CNN contributor and interim DNC chair, Donna Brazile.22,23

This second round of Wikileaks emails turned out to be only the first of two scandals
to mire the Clinton campaign in the month before election day. On October 28th, 2016, the
director of the Federal Bureau of Investigation (FBI), James Comey, informed Congress that
the FBI had discovered emails potentially related to its previous investigation into Clinton’s
use of a private email server during her tenure as Secretary of State and would be
conducting an additional investigation into this new material.24 Director Comey made this
announcement despite notification from the U.S. Department of Justice that doing so would
violate the department’s policy to not comment on investigations close to an election to
avoid potentially influencing that election’s outcome.25 Public opinion polling showed that


support for Hillary Clinton cratered in the days following Comey’s letter to Congress, dropping an estimated three percentage points.\textsuperscript{26} Just over a week later—and only two days before election day—Director Comey sent a second letter to Congressional leadership that the Bureau “had seen no evidence...to change [the] conclusion that Hillary Clinton should face no charges over her handling of classified information” associated with her use of the private server.\textsuperscript{27} Democratic leadership regarded this follow up as too little, too late, and decried Director Comey’s initial decision to reveal information that was sure to impact the election only days before it occurred. Despite the FBI’s conclusion, the damage was done in what the New York Times described as “the kind of potential turnabout rarely if ever seen at this late stage of a presidential race.”\textsuperscript{28} Why support for Donald Trump remained stable and his campaign successfully shrugged off the “Access Hollywood” scandal as support for Hillary Clinton fell amidst her own October scandals remains hotly debated and beyond the purview of this thesis, but on November 8th, Americans headed to the polls.

In the early morning of November 9th, 2016, Donald Trump was elected the 45th president of the United States. After the votes were tallied nationwide, it was determined that President Trump had won the electoral college with 304 electoral votes to former Secretary of State Hillary Clinton’s 227, but had actually lost the popular vote by more than 2.8 million votes, making him the fourth U.S. President ever to do so.\textsuperscript{29} This result took much of the country by surprise as late polling gave Hillary Clinton a modest edge, and prominent media outlets broadcast almost absolute confidence in Secretary Clinton’s


victory with the New York Times claiming she could still “easily assemble the 270 electoral votes ...for a victory” despite the damage from the revived emails scandal.\textsuperscript{30}

The keys to Donald Trump’s electoral success were razor thin victories in Michigan, Pennsylvania, and Wisconsin, which he carried by 0.23\%, 0.72\%, and 0.77\% or 10,704, 46,765, and 22,177 votes, respectively—all states that President Barack Obama had secured in the 2008 and 2012 presidential elections.\textsuperscript{31, 32, 33} Had Secretary Clinton won these three states, she would have secured 274 electoral votes, enough to seal the presidency.\textsuperscript{34}

\textbf{Figure 1: States with the Smallest Popular Vote Differentials in the 2016 Presidential Election}

\textsuperscript{35}

\begin{itemize}
\item \textsuperscript{34} Tim Meko, Denise Lu, and Lazara Gamio. 2016. How Trump won the presidency with razor-thin margins in swing states. November 11. \url{https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/}.
\end{itemize}
2.2 Russian Involvement in the 2016 U.S. Presidential Election

On February 16th, 2018, the U.S. Department of Justice (DOJ) announced that a District of Columbia grand jury returned an indictment from Special Counsel Robert S. Mueller III who had been appointment to investigate possible “coordination between the Russian government and...the campaign of President Donald Trump.”36 This indictment charged thirteen Russian nationals and three Russian companies for seeking to interfere in the 2016 US Presidential election.37 These individuals and companies all supported an organization known as the Internet Research Agency LLC (IRA), which “engaged in operations to interfere with elections and political processes” in the United States through “impairing, obstructing, and defeating the lawful function of the government through fraud and deceit.”38 Specifically, the defendants were charged with Conspiracy to Defraud the United States, and the rest of the Special Counsel’s indictment revealed the full extent of that conspiracy authoritatively for the first time.39

As early as 2014, IRA operatives “began to track and study groups on U.S. social media sites dedicated to U.S. politics and social issues.” Their monitoring metrics included the group’s size, the frequency of which it published content, and the level of audience engagement estimated through the “average number of comments or responses to a post.”40 In June of 2014, two IRA agents even traveled to the U.S. “under false pretenses in


40 Ibid., Page 12.
order to collect intelligence” to further future interference operations, visiting Nevada, California, New Mexico, Colorado, Illinois, Michigan, Louisiana, Texas, and New York with another agent visiting Georgia later that year. To supplement this research, IRA operatives posed as U.S. persons to contact U.S. political experts and activists to learn what political issues and geographic areas they should focus their effort upon. Following this intelligence gathering, IRA employees created hundreds of “social media accounts that appeared to be operated by U.S. persons” that posted in the correct U.S. time zones, incorporated U.S. holidays, and wrote about U.S political and economic issues to generate “political intensity,” while also creating thematic social media pages that addressed issues from immigration, religion, the Black Lives Matter movement, and specific geographic regions of the United States. To maintain a steady stream of social media content for these IRA-owned accounts and expand to other US domestic political issues, the IRA employed hundreds of Russians (less than affectionately known as “trolls”) to create and operate fictitious U.S. personas, produce politically charged media, and troubleshoot technical and administrative issues. IRA operatives used “the social security numbers and dates of birth of real U.S. persons” to open social media accounts, purchase social media advertising, and register email accounts hosted by U.S. email providers and masked the fact that all of this was done from Russia by purchasing space on U.S. computer servers and setting up virtual private networks that allowed the IRA to appear as if it was operating from within the United States. The IRA used this apparent U.S. presence to coordinate with “unwitting members, volunteers, and supporters of the Trump Campaign,” organizing political protests within the U.S.; “to encourage U.S. minority groups not to vote in the 2016 U.S. presidential election or to vote for a third-party” candidate; and “to promote

41 Ibid., Page 13.
42 Ibid., Page 14.
43 Ibid.
44 Ibid.
allegations of voter fraud by the Democratic Party.”"46 While the effect of the latter two efforts cannot be easily estimated, the IRA did organize dozens of rallies within the US including protests in New York, North Carolina, and Pennsylvania as well as a particularly successful “state-wide Trump Flashmob” in Florida known as “Florida Goes Trump.”47

In 2015, the IRA began to amplify the dissemination of its content by purchasing social media advertisements to the tune of “thousands of U.S. dollars every month.”48 They closely monitored the impact of these social media operations by tracking the size of the U.S. audience their content reached and regularly audited IRA content “to ensure they appeared authentic—as if operated by U.S. persons.”49 As operations progressed through 2016, the IRA’s monthly budget ballooned to exceed 73 million rubles or more than $1.25 million U.S. dollars.50 The IRA received its funding from Russian companies called Concord Management and Consulting LLC and Concord Catering (collectively, “Concord”) which were both controlled by a Russian oligarch named Yevgeniy Viktorovich Prigozhin “who has been nicknamed ‘Putin’s chef’ because of his proximity to the Russian President Vladimir Putin.”51,52 While Concord has not been publicly connected to the Russian government, its election interference campaign certainly complemented the simultaneous U.S. email thefts and election interference operations conducted by Russian intelligence, and in early 2017, the U.S. intelligence community assessed that Russian President

46 Ibid., Page 17-18.
47 Ibid., Page 22.
48 Ibid., Page 15.
49 Ibid.
50 Ibid., Page 7.
51 Ibid., Page 3.
Vladimir Putin himself ordered the influence campaign that targeted the 2016 presidential election (although the evidence supporting this assessment remains classified).\textsuperscript{53,54}

In mid-December of 2018, the United States Senate Select Committee on Intelligence (SSCI) released two independent reports it had commissioned from third-party experts.\textsuperscript{55} These reports, “the first comprehensive analyses of their kind conducted by entities other than social media companies themselves,” fully exposed the sheer scale and scope of Russian social media-based operations.\textsuperscript{56} Shortly after the 2016 presidential election, the SSCI opened an investigation into IRA social media activities, and in March of 2018, “some of the social platform companies misused by the IRA (Twitter, Facebook, an Alphabet)” turned over data related to IRA operations including Tweets and associated media, Facebook Page posts and Instagram account content, and Google advertising and YouTube video and channel data.\textsuperscript{57} The report completed by the New Knowledge Organization (now known as Knology) and titled “Tactics and Tropes of the IRA” used this evidence to tie the IRA to “widespread activity on other popular social platforms including Vine, Gab, meetup, Vkontakte, and LiveJournal” as well as to several standalone websites “created to host original written content” that served as source material for IRA social media operations.\textsuperscript{58} IRA operatives also created crude video games, browser extensions, and music applications to expand their message to younger U.S. demographics and even incorporated the popular


\textsuperscript{56} Ibid.


\textsuperscript{58} Ibid., Page 5.
video game Pokémon Go into their operations. Several other social media sites including Reddit, Tumblr, Medium, and Pinterest were not included in the SSCI investigation but had previously turned over evidence to the U.S. Department of Justice. Overall, the data turned over to the SSCI consisted of more than 10.4 million tweets (of which more than 6 million were original) produced by 3,841 Twitter accounts, upwards of 1,100 YouTube videos from 17 account channels, over 116,000 Instagram posts from 133 accounts, and more than 61,500 unique Facebook posts published by 81 different Facebook Pages. Facebook users engaged with IRA content more than 77 million times while Instagram users did so more than 187 million times and Twitter users over 73 million times. Facebook estimated that more than 20 million unwitting Instagram users interacted with IRA content, while more than 126 million Facebook users were exposed, although these estimates appear conservative as Instagram lacks a “native sharing feature.” However, New Knowledge could not independently verify these estimates due to incomplete user interaction data (detailed later).

The IRA’s social media efforts represent only the first of three parallel assaults on U.S. popular opinion ahead of the 2016 presidential election. A separate SSCI report from May of 2018 revealed that cyber actors associated with the Russian government also targeted electronic state election systems in at least 21 states, scanning for vulnerabilities in state Secretary of State websites and voter registration infrastructure. In a handful of states, these Russian hackers “went beyond scanning and conducted malicious access attempts on voting related websites,” gaining “access to restricted elements of election

59 Ibid.
60 Ibid.
61 Ibid., Page 7.
62 Ibid.
63 Ibid.
64 Ibid., Page 7-8.
infrastructure.”66 These incursions gave Russian operatives the power to “alter or delete voter registration data,” although they could not “manipulate individual votes or aggregate vote totals.”67 While the SSCI found no evidence that Russian hackers changed any votes, the intent of this network penetration remains unclear.68 These cyber actors could have discovered these vulnerabilities and planned to exploit them in the 2016 presidential election before choosing not to take action, or perhaps they were laying the groundwork for a future attack on a different U.S. election.69 Either way, the SSCI report concluded that this “activity indicate[d] an intent to go beyond traditional intelligence collection.”70

Special Counsel Mueller released another indictment, United States v. Netyksho, later in 2018 that fully and authoritatively detailed the third prong of Russian interference in the 2016 election: the hacking and public release of sensitive emails from the DNC and Clinton campaign team described previously.71 The Russians charged in this indictment were identified as agents from Units 26165 and 74455 of the Russian military intelligence agency, the Main Intelligence Directorate of the General Staff (GRU).72 These units specialized in “targeting military, political, governmental, and non-governmental organizations with spear phishing emails and other computer intrusion activity.”73 As early as March of 2016, these intelligence operatives successfully hacked “the email accounts of [hundreds of] volunteers and employees of the” Clinton campaign, including that of the campaign chairman, John Podesta.74 By April of 2016, they had also managed to hack the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the

66 Ibid.
67 Ibid., Page 1-2.
68 Ibid., Page 2.
69 Ibid.
70 Ibid.
72 Ibid., Page 1.
73 Ibid., Page 3.
74 Ibid., Page 2.
DNC while also implanting “hundreds of files containing malicious computer code” and stealing emails from the DCCC and DNC.\textsuperscript{75} They then published more than 50,000 of these stolen emails through dcleaks.com (a website which they had previously created) and through the anti-secrecy organization, Wikileaks.\textsuperscript{76} GRU operatives then obscured the Russian government’s role through an alias, Guccifer 2.0, a supposed lone Romanian hacker who claimed responsibility for the email leaks and stated ‘the intrusions and release of stolen documents had “totally no relation to the Russian government.”’\textsuperscript{77,78} The devastating effect to the Clinton campaign of these releases and their strategic timing has been previously described, but confirmation that these releases were orchestrated by a foreign government again shook the U.S. political landscape.

Clearly, the fact of Russian involvement is well established. But the question remains: What were the IRA and the Russian government that supports it trying to achieve?

### 2.3 Goals of Russian Involvement

After news of this months-long campaign of election interference broke, the Russian government’s motive behind it became hotly debated. The interpretation publicly broadcast by the United States Government changed over time. On December 9th, 2016, news broke that a classified Central Intelligence Agency (CIA) assessment concluded that Russia intervened in the 2016 presidential election to help Donald Trump win the presidency, rather than just to undermine domestic confidence in the U.S. electoral system.\textsuperscript{79} Just under a month later on January 6th, 2017, the US Office of the Director of

\textsuperscript{75} Ibid.
\textsuperscript{76} Ibid., Page 3.
\textsuperscript{77} Ibid., Page 14.
\textsuperscript{78} Ibid., Page 17.
National Intelligence (ODNI) published a declassified report titled “Assessing Russian Activities and Intentions in Recent US Elections” which combined analysis from the CIA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) and concluded that the influence campaign against the 2016 election was directly ordered by Russian President Vladimir Putin and aimed to “help President-elect Trump’s election chances...by discrediting Secretary Clinton” thereby “harm[ing] her electability and potential presidency.” Following this report’s release, the intelligence community’s conclusion came under fire from Republicans of the House Intelligence Committee who “accused intelligence agencies of failing to employ proper ‘tradecraft’ when they concluded Russia came to support Trump’s candidacy.”

Over the next year, journalists, researchers, and political pundits debated the veracity and the importance of this assessment and the impact any Russian influence might have had on American voting behavior. Evidence remained limited until February of 2018 when Special Counsel Robert Mueller’s investigation indicted 13 Russian operatives connected to the Internet Research Agency for conspiracy to defraud the United States. Critically, the indictment charged that these operatives were tasked “to communicate derogatory information about Hillary Clinton...and to support Bernie Sanders and then-candidate Donald Trump” through a network of thousands of social media accounts and fictitious U.S. personas. Three months later in May of 2018, “Republican and Democratic leaders of the Senate Intelligence Committee...endorsed the U.S. intelligence community’s

---


assessment” in a powerful bipartisan show of support for Special Counsel Mueller’s investigation and the nation’s beleaguered intelligence professionals.\textsuperscript{83}

Later that year in October of 2018, the Senate Intelligence Committee released two independent reports analyzing Russia’s social media influence operations. The first report completed jointly by the University of Oxford’s Computational Propaganda Project and Graphika, a U.S. social network analysis firm, stopped short of analyzing the intent behind Russian social media information operations, but the second report completed by the social issue analysis firm, the New Knowledge Organization (now known as Knology), concluded that the “IRA had a very clear bias for then-candidate Trump” that began early in the campaign and endured through the 2016 election and also identified comprehensive operations conducted against then-candidate Hillary Clinton.\textsuperscript{84} IRA operatives circulated anti-Hillary Clinton political content through both liberal and conservative leaning IRA-created communities.\textsuperscript{85} On Facebook, the IRA promoted a single event promoting support for Clinton’s candidacy, while on Twitter, the vast majority of “developed Left-wing Twitter personas were still largely anti-Clinton and expressed pro-Bernie Sanders and pro-Jill Stein sentiments.\textsuperscript{86} The IRA also “targeted a wide range of Republican leaders, including Senators Ted Cruz, Marco Rubio, Lindsay Graham,...and Dr. Ben Carson”--all of whom were candidates that challenged President Trump during the 2016 Republican primary--to support “the pro-Trump portion of the operation.”\textsuperscript{87} While the bias in IRA efforts to influence domestic public opinion in favor of then-candidate Trump is evident, it is worth noting again that IRA actions were limited to influence and propaganda and did not include direct manipulation of voter registration information or votes themselves, as specified by the SSCI.


\textsuperscript{85} Ibid.

\textsuperscript{86} Ibid.

\textsuperscript{87} Ibid.
Just over 80,000 votes across Michigan, Pennsylvania, and Wisconsin decided the 2016 presidential election.\textsuperscript{88} IRA-generated content reached a combined 147.4 million Americans across Facebook, Instagram, and Twitter alone.\textsuperscript{89} An unknown number of other unwitting Americans interacted with IRA propaganda on YouTube, Reddit, Tumblr, Pinterest, Gab, Vine, Meetup, and IRA-owned websites. While the impact of those interactions on individual U.S. citizens’ voting preferences can never be quantified, the sheer \textbf{possibility} that foreign social media influence efforts could actually affect the outcome in incredibly close elections justifies the need to better understand how foreign actors structure and operate their manipulation campaigns. That possibility and the conclusions that additional understanding provide should also galvanize U.S. political leaders to take every action necessary to preserve the integrity of American democracy.


\textsuperscript{89} Ibid., Page 6.
3 Data Analysis

To inform potential legislative action, this thesis seeks to unpack the trends and tactics associated with IRA activity. While most of the data concerning the IRA’s presence on social media remains closely guarded by many social media platforms, Twitter made the trailblazing decision to make this data open to independent researchers (like the author). This analysis will look for trends in IRA activity, including: the volume and timing of IRA network creation and content production, the focus and timing of IRA-manufactured content, the sophistication of and associated perceived enthusiasm behind IRA activity, and the real and implied investment into IRA operations, among others. The results of this analysis will drive an evaluation of proposed legislation and that legislations’ potential effectiveness in preventing future foreign election interference.

3.1 Twitter’s Decision to Release Data to the Public

On October 17th, 2018, Twitter published a blog post entitled: “Enabling further research of information operations on Twitter,” that coincided with the public release of the data Twitter had provided to the SSCI to aid in the committee’s investigation into IRA social media activity during the 2016 presidential election. Twitter made the unprecedented decision to make all accounts, Tweets, and related media available to enable independent academic research and investigation, like this master’s thesis. This new repository included substantially more data than had any previous information operation disclosure, and it presented that data in a machine-readable format that enables seamless data analysis. This release followed Twitter’s earlier commitment to the United States Congress and the public to disclose the results of its investigation into foreign interference in political conversations on the platform as well as Twitter’s decision to notify users if

---

they had interacted with accounts involved in known information operations. This voluntary disclosure of easily manipulable data set the standard for transparency concerning the role social media played in enabling online influence campaigns. Twitter’s conclusion that “[i]ndependent analysis of this activity by researchers is a key step toward promoting shared understanding of these threats” is wholeheartedly shared by the author.

Unfortunately, Twitter’s embrace of transparency proved to be the exception. Other social media companies showed obvious reluctance in facilitating the Senate Intelligence Committee’s investigation and have still resisted adopting a transparency-oriented stance. Facebook and Google, in particular, made it exceedingly difficult for researchers to access their data, refusing to turn over complete datasets to the SSCI. New Knowledge (now Knology) researchers provided further evidence of this resistance by publicizing that “[s]ome of what was turned over was in PDF form; other data sets contained extensive duplicates.” Google, perhaps the worst offender, provided non-machine-readable PDF screenshots of data in spreadsheets instead of the spreadsheets themselves. More importantly, the datasets provided “lacked core components that would have provided a fuller and more actionable picture” of Russian activity. The platforms (including Twitter

91 Ibid.
95 Ibid.
in this case) failed to include their “methodology for identifying the accounts,” forcing SSCI researchers to assume “the provenance and attribution [was] sound for the purposes of [their] analysis.”\textsuperscript{98} Social media companies also failed to “include anonymized user comments” and didn't include any conversion pathway data to elucidate how individuals came to follow the accounts," both of which eliminated key paths to gauge IRA impact.\textsuperscript{99} Minimal metadata was provided which hamstrung further analysis, and “[o]ne dataset failed to include any user engagement data at all.”\textsuperscript{100} Additionally, during the course of the SSCI investigation, Facebook disabled the application programming interface (API), access for third-parties to gather and interpret data, for public posts and has never offered an Instagram API both of which would have allowed SSCI researchers to fill gaps in the datasets provided by Facebook.\textsuperscript{101} Researchers stated that this loss of access would only prevent “further public understanding of the latest trends in computational propaganda.”\textsuperscript{102} Instead, Facebook trumpeted greater advertisement transparency, but researchers from the joint Oxford-Graphika team found that organic post activity received far more user engagement than political ads, was much greater in volume than political ad activity, and that ad activity did not substantially increase over time as IRA organic content did.\textsuperscript{103}

New Knowledge researchers also decried some of the other platforms’ apparent misrepresentation of the nature of Russian activity and the evasion in answering questions

\textsuperscript{98} Ibid.

\textsuperscript{99} Ibid.


from Congress.\textsuperscript{104} Regrettably, one unnamed “platform claimed that no specific groups were targeted” which was only true if speaking of social media advertisements purchased by the IRA,\textsuperscript{104} while another dissembled about whether or not the Internet Research Agency created content to discourage voting,” which it undeniably did.\textsuperscript{105} These researchers stop short of accusing these social media platforms of obstructing the SSCI’s investigation, but do question “whether these answers were the result of faulty or lacking analysis, or a more deliberate evasion.”\textsuperscript{106}

\subsection*{3.2 What Twitter Included in Its Release}

In the October 17th release, Twitter identified 3,841 accounts affiliated with Russia’s Internet Research Agency (although 228 of these were later more confidently linked to a Venezuelan information operations campaign), nearly 10 million tweets, and 274GB of associated media (pictures, memes, gifs, etc.).\textsuperscript{107} This data was the same that Twitter provided to the SSCI to inform the committee’s investigation into Russian social media information operations, and included the “earliest on-Twitter activity from accounts connected with these campaigns, dating back to 2009.”\textsuperscript{108}

The accounts data set includes the ten following categories of information for each account: “userid,” the identification number assigned to that account by Twitter;


\textsuperscript{105} Ibid.


\textsuperscript{107} Vijaya Gadde, and Yoel Roth. 2019. Enabling further research of information operations on Twitter. October 17. \url{https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html}.

\textsuperscript{108} Ibid.
“user_display_name,” the chosen name of the account (changed at the user’s convenience); “user_screen_name,” the Twitter handle of that account (starting with the “@” symbol and followed by any series of characters, e.g. “@jack”); “user_reported_location,” the optional geographic location of the account’s user, described by the user; “user_profile_description,” the optional, brief description of the account authored by the account’s user (can include almost any series of phrases, hashtags, etc.); “user_profile_url,” an optional link to a website designated by the account’s user; “follower_count,” the number of followers an account has; “following_count,” the number of accounts the account’s user follows; “account_creation_date,” the date and time which the user created the account; and “account_creation_language,” the user-designated language for the account (required during setup).

Twitter users can change their user display name, reported location, profile description, and profile URL at any time and can also leave these categories entirely blank. User ID, screen name, follower count, following count, account creation date, and account language are designated upon account creation and cannot subsequently be changed; every account in the dataset has these six pieces of information associated with it. Information on display name, reported location, profile description, profile URL, follower count, and following count was gathered at the time of suspension, so this dataset represents a snapshot in time as IRA operatives could have (and commonly did) change this information throughout the lifetime of each account.

The tweet data set includes twenty-two information descriptors for each tweet: “tweetid,” the tweet identification number designated by Twitter; “userid,” the user identification number assigned by Twitter; “tweet_language,” the language of the tweet text (as determined through Twitter’s language identification software); “tweet_text,” the

---


110 Of note: account_creation_language simply controls the language that all menus and interfaces are presented to the user in; this does not control what language the account’s user Tweets in.


112 Ibid.
actual body of text that makes up a tweet; “tweet_time,” the time when the tweet was published; “tweet_client_name,” the name of the client application used to publish the tweet; “in_reply_to_tweetid,” the tweetid of the original tweet a tweet is in reply to; “in_reply_to_userid,” the userid of the original tweet that a tweet is in reply to; “quoted_tweet_tweetid,” the tweetid of the original tweet that a tweet is quoting; “is_retweet,” a binary true or false variable for whether a tweet is a retweet; “retweet_userid,” the userid of the author of the original tweet; “retweet_tweetid,” the tweetid of the original tweet; “latitude,” the geo-located latitude; “longitude,” the geo-located longitude; “quote_count,” the number of tweets quoting a tweet; “reply_count,” the number of tweets replying to a tweet; “like_count,” the number of likes a tweet received; “retweet_count,” the number of retweets that a tweet received; “hashtags,” a list of hashtags used in a tweet; “urls,” a list of web addresses used in a tweet; “user_mentions,” a list of userids who are mentioned in a tweet; and “poll_choices,” the choices available in a tweet poll (only if a tweet is a poll).

The tweet media dataset included 300 separate digital archives that contained hundreds of thousands of pictures, videos, memes, gifs, and Periscope broadcasts. Twitter grouped these archives according to three categories: Twitter profile media, tweet media, and Periscope media while also including lists that detail which media came from which user. The profile media archives included all the profile photos and banners of all IRA accounts except those with the default twitter profile picture and/or banner, while the tweet media archives contained the lion’s share of videos, memes, and gifs. Finally, the

113 Ibid.
116 Ibid.
117 Ibid.
Periscope broadcast archives contained the full livestream broadcasts by Twitter users with Periscope accounts.\textsuperscript{118}

No content was entirely redacted, although, for accounts with fewer than 5,000 followers, Twitter “hashed” (i.e. anonymized) certain identifying fields like user ID and screen name “to ensure there [were] no false positives in these datasets” and to protect the privacy of those potential accounts accidentally included.\textsuperscript{119} Twitter found this anonymization necessary “to reduce the potential negative impact” on genuine users “while still enabling longitudinal research, network analysis, and assessment of the underlying content created by these accounts.”\textsuperscript{120} In the spirit of full transparency, Twitter later made unhashed versions of all its datasets available to specialist researchers under a data use agreement that ensures “the data is used within appropriate legal and ethical parameters.”\textsuperscript{121}

\textbf{3.3 Trends in IRA Operations and Perceived Investment}

Breaking down Twitter’s release by accounts and tweets reveals trends that point to various tactics the IRA employed in its covert assault on U.S. opinion. Overall, these trends signify remarkable advances in IRA sophistication over time, signaling growing enthusiasm for IRA efforts which likely translated to millions of additional Rubles galvanizing current operations and paving the way for the attempted manipulation of future elections.

\textbf{3.3.1 Trends in IRA Accounts}

\textsuperscript{118} Ibid.


\textsuperscript{120} Ibid.

\textsuperscript{121} Ibid.
Of the 3,641 Twitter accounts linked to the IRA, many developed significant followings, with more than twenty-five accounts gaining over 50,000 followers (shown in Table 1). Five of those top twenty-five had more than 100,000 followers, and one other had over 250,000. Seventeen of the top twenty-five focused on predominantly Russian topics, and ten of those seventeen acted as purported Russian news sites. (The Russian word “novosti” translates to “news” in English.) Eight of the top twenty-five focused on predominantly U.S. issues.
<table>
<thead>
<tr>
<th>Rank</th>
<th>User_Screen_Name</th>
<th>Follower Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NovostiMsk</td>
<td>257,638</td>
</tr>
<tr>
<td>2</td>
<td>NovostiSPb</td>
<td>149,672</td>
</tr>
<tr>
<td>3</td>
<td>TEN_GOP</td>
<td>147,767</td>
</tr>
<tr>
<td>4</td>
<td>MaxDementiev</td>
<td>134,805</td>
</tr>
<tr>
<td>5</td>
<td>KadirovRussia</td>
<td>123,989</td>
</tr>
<tr>
<td>6</td>
<td>NovostiCrimea</td>
<td>106,462</td>
</tr>
<tr>
<td>7</td>
<td>NovostiKrsnrsk</td>
<td>85,293</td>
</tr>
<tr>
<td>8</td>
<td>LavrovMuesli</td>
<td>84,642</td>
</tr>
<tr>
<td>9</td>
<td>NovostiPermi</td>
<td>84,167</td>
</tr>
<tr>
<td>10</td>
<td>Jenn_Abrams</td>
<td>79,152</td>
</tr>
<tr>
<td>11</td>
<td>Pamela_Moore13</td>
<td>72,121</td>
</tr>
<tr>
<td>12</td>
<td>TodayNYCity</td>
<td>66,980</td>
</tr>
<tr>
<td>13</td>
<td>NovostiNsk</td>
<td>60,869</td>
</tr>
<tr>
<td>14</td>
<td>NovostiKzn</td>
<td>59,724</td>
</tr>
<tr>
<td>15</td>
<td>ELEVEN_GOP</td>
<td>59,279</td>
</tr>
<tr>
<td>16</td>
<td>NovostiEkb</td>
<td>59,021</td>
</tr>
<tr>
<td>17</td>
<td>NovostiINN</td>
<td>58,060</td>
</tr>
<tr>
<td>18</td>
<td>wokeluisa</td>
<td>57,295</td>
</tr>
<tr>
<td>19</td>
<td>Crystal1Johnson</td>
<td>56,581</td>
</tr>
<tr>
<td>20</td>
<td>VestnikTula</td>
<td>56,526</td>
</tr>
<tr>
<td>21</td>
<td>LuganskNovosti</td>
<td>54,266</td>
</tr>
<tr>
<td>22</td>
<td>SouthLoneStar</td>
<td>53,999</td>
</tr>
<tr>
<td>23</td>
<td>coldwar20_ru</td>
<td>53,175</td>
</tr>
<tr>
<td>24</td>
<td>NovostiRnD</td>
<td>52,288</td>
</tr>
<tr>
<td>25</td>
<td>Mechtateli_</td>
<td>51,964</td>
</tr>
</tbody>
</table>

Table 1: Top 25 IRA-Controlled Twitter Accounts, Ranked by Follower Count

These U.S. centric accounts span both U.S. conservative and liberal political ideology and represent the IRA’s dual approach of advocating for then-candidate Trump and driving more liberal voters away from Hillary Clinton. Within the top twenty-five accounts, however, they skewed more conservative with only @wokeluisa and @Crystal1Johnson focusing on left-leaning issues. @wokeluisa tweeted almost 2,300 times and was retweeted

---

122 Table created by the author with data from Twitter’s election integrity initiative.
more than 1.3 million times while @Crystal1Johnson published over eight thousand tweets and was retweeted more than 3.7 million times. These left-leaning accounts predominantly focused on issues of race and immigration including the Black Lives Matter movement. Figure 2 and Figure 3 provide examples of their usual content.

Figure 2: Twitter Profile of @Crystal1Johnson, an IRA-Controlled Twitter Account

---


124 archive.today. n.d. @Crystal1Johnson. https://archive.is/p1EpK.
The top IRA accounts tasked with publishing conservative content include the most popular U.S oriented account, @TEN_GOP, which cast itself as the unofficial voice of conservatives in the state of Tennessee. @TEN_GOP tweeted more than eleven thousand times and was retweeted more than six million times. IRA trolls also established two backup accounts for @TEN_GOP, @ELEVEN_GOP and @realTEN_GOP, in case Twitter closed the original account. Other popular conservative accounts include @Jenn_Abrams and @Pamela_Moore13 which both pretended to be conservative women that commonly target political correctness and Democratic politicians. @Jenn_Abrams tweeted over twenty-two thousand times and was retweeted more than 550,000 times, while @Pamela_Moore13 tweeted over six thousand times and was retweeted more than 2.2 million times. Figure 4 and Figure 5 depict examples of these accounts’ typical content.

---


127 Ibid.

128 Ibid.
Figure 4: Twitter Profile of @TEN_GOP, an IRA-Controlled Twitter Account

---

Figure 5: Tweet from @Pamela_Moore13, an IRA-Controlled Twitter Account[^130]

When the same 3,641 accounts are ranked according to the number of accounts they follow as in Table 2, significantly more U.S. oriented accounts appear in the top twenty-five accounts. Twenty-four of these IRA accounts focus on U.S. domestic political issues while

---

Table 2: Top 25 IRA-Controlled Twitter Accounts Ranked by Following Count

<table>
<thead>
<tr>
<th>Rank</th>
<th>User_Screen_Name</th>
<th>Following Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TEN_GOP</td>
<td>74,664</td>
</tr>
<tr>
<td>2</td>
<td>Wokeluisa</td>
<td>50,746</td>
</tr>
<tr>
<td>3</td>
<td>SouthLoneStar</td>
<td>49,272</td>
</tr>
<tr>
<td>4</td>
<td>USA_Gunslinger</td>
<td>45,382</td>
</tr>
<tr>
<td>5</td>
<td>Pamela_Moore13</td>
<td>42,080</td>
</tr>
<tr>
<td>6</td>
<td>KaniJJackson</td>
<td>34,395</td>
</tr>
<tr>
<td>7</td>
<td>Crystal1Johnson</td>
<td>31,117</td>
</tr>
<tr>
<td>8</td>
<td>ELEVEN_GOP</td>
<td>30,227</td>
</tr>
<tr>
<td>9</td>
<td>BlackNewsOutlet</td>
<td>29,659</td>
</tr>
<tr>
<td>10</td>
<td>TheFoundingSon</td>
<td>29,429</td>
</tr>
<tr>
<td>11</td>
<td>Jenn_Abrams</td>
<td>22,607</td>
</tr>
<tr>
<td>12</td>
<td>Tpartynews</td>
<td>22,407</td>
</tr>
<tr>
<td>13</td>
<td>PigeonToday</td>
<td>21,336</td>
</tr>
<tr>
<td>14</td>
<td>Politweecs</td>
<td>20,288</td>
</tr>
<tr>
<td>15</td>
<td>Nevnon_ru</td>
<td>16,588</td>
</tr>
<tr>
<td>16</td>
<td>WashingtonOnline</td>
<td>14,404</td>
</tr>
<tr>
<td>17</td>
<td>Blackmatterus</td>
<td>14,112</td>
</tr>
<tr>
<td>18</td>
<td>Rf_choice</td>
<td>14,029</td>
</tr>
<tr>
<td>19</td>
<td>ScreamyMonkey</td>
<td>13,851</td>
</tr>
<tr>
<td>20</td>
<td>ChicagoDailyNew</td>
<td>13,665</td>
</tr>
<tr>
<td>21</td>
<td>Atlanta_Online</td>
<td>13,575</td>
</tr>
<tr>
<td>22</td>
<td>GiselleEvns</td>
<td>13,442</td>
</tr>
<tr>
<td>23</td>
<td>OaklandOnline</td>
<td>13,099</td>
</tr>
<tr>
<td>24</td>
<td>TrayneshaCole</td>
<td>12,977</td>
</tr>
<tr>
<td>25</td>
<td>AndyHashtagger</td>
<td>12,966</td>
</tr>
</tbody>
</table>
only one account, @Nevnon-ru, targeted Russia-related issues. These significantly higher following counts likely indicate a common strategy to rapidly increase the reach of a social media account’s online presence known as “follow for follow” behavior. This behavior occurs when an account publicly agrees to follow all accounts that follow it, resulting in a mutual increase in followership.\textsuperscript{132} This artificial increase in followers then allows IRA accounts to reach more Twitter users with their manufactured content.

According to analysis published by researchers at the online security company Symantec (now known as NortonLifeLock and part of Broadcom, Inc.), IRA accounts played one of two primary roles: main accounts that published new content and auxiliary accounts that amplified the main accounts messaging by retweeting content published by those main accounts.\textsuperscript{133} Symantec characterized main accounts as having at least 10,000 followers and followed substantially fewer accounts, while auxiliary accounts had less than 10,000 followers and followed a similar or often greater number of other accounts.\textsuperscript{134} Main accounts generally masqueraded as regional news accounts (both in Russia and the U.S.) or political organizations, while most auxiliary accounts purported to be American individuals.\textsuperscript{135} At the time Twitter took down these IRA-linked accounts, the IRA appears to have been attempting to create more English main accounts to amplify its ability to impact U.S. public opinion. Additionally, all IRA Twitter accounts roughly fit into three broad categories: “Black-targeted, politically Left-targeted, and politically Right-targeted.”\textsuperscript{136} While the IRA did target other racial minority groups, if focused overwhelmingly on Black

\textsuperscript{132} Dictionary.com. n.d. F4F. \url{https://www.dictionary.com/e/acronyms/f4f/}. \\
\textsuperscript{134} Ibid. \\
\textsuperscript{135} Ibid. \\
Americans, urging them to vote for a third party candidate instead of Secretary Clinton or discouraging them from voting altogether.137

3.3.2 Trends in IRA Account Creation

Visualizing when the IRA created their accounts reveal interesting and troubling trends suggesting significant premeditation and strategy. Figure 6 shows that the lion’s share of IRA accounts went online in the roughly eighteen-month period from mid-2013 to early 2015, just before the 2016 presidential campaign season. IRA operatives seemed to take special care when creating main accounts, setting them up “individually or in small batches.”138 However, they created auxiliary accounts in much larger batches, sometimes creating hundreds on the same day.139


139 Ibid.
IRA operatives opened accounts in at least eleven different languages, including: English, Russian, Spanish, German, Arabic, British English, French, Italian, Chinese, Ukrainian, and Indonesian. These languages roughly correspond with many of the Russian government’s chief domestic and foreign policy concerns: maintaining a compliant domestic population, eroding the influence of an increasingly isolationist U.S. maintaining a foothold in the Middle East through Syria, and diminishing German leadership in the European Union, although the minimal investment into Ukrainian accounts stands at odds with past and ongoing Russian involvement there. The vast majority of accounts--more than 2,300 were opened in English, representing over 62% of total accounts in the dataset, while the second most numerous language was Russian with more than 1,000 accounts,

140 Chart created by the author with data from Twitter’s election integrity initiative.

representing over 27%. Interestingly, the largest main accounts (as defined previously) were “always either English or Russian.” Spanish was the third most common account language with 234 IRA accounts, and German the fourth most common with 111 accounts. The other seven languages had fewer than 50 accounts each. Table 3 summarizes the number and approximate proportion of total accounts for each language, while Figure 7 visualizes the disparity in account totals.

<table>
<thead>
<tr>
<th>Account Creation Language</th>
<th>Number of Accounts</th>
<th>% of Total Accounts*</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>2,384</td>
<td>62.7</td>
</tr>
<tr>
<td>Russian</td>
<td>1,039</td>
<td>27.1</td>
</tr>
<tr>
<td>Spanish</td>
<td>234</td>
<td>6.1</td>
</tr>
<tr>
<td>German</td>
<td>111</td>
<td>2.9</td>
</tr>
<tr>
<td>Arabic</td>
<td>28</td>
<td>0.7</td>
</tr>
<tr>
<td>English-Great Britain</td>
<td>15</td>
<td>0.4</td>
</tr>
<tr>
<td>French</td>
<td>11</td>
<td>0.3</td>
</tr>
<tr>
<td>Italian</td>
<td>7</td>
<td>0.2</td>
</tr>
<tr>
<td>Chinese</td>
<td>3</td>
<td>0.1</td>
</tr>
<tr>
<td>Ukrainian</td>
<td>2</td>
<td>0.1</td>
</tr>
<tr>
<td>Indonesian</td>
<td>2</td>
<td>0.1</td>
</tr>
</tbody>
</table>

* Rounding error prevents the percentages from adding to 100%.

Table 3: Accounts Opened with Each Creation Language


143 Table created by the author with data from Twitter’s election integrity initiative.
When graphed over time as in Figure 8, patterns in IRA account creation language also emerge. These patterns are most evident in the five most common account languages: English, Russian, Spanish, German, and Arabic. IRA agents opened Arabic accounts primarily from early 2014 and into 2015 with another burst in 2017, German accounts in late 2015 through 2016 and into 2017, Spanish accounts almost all in the second half of 2017, and Russian accounts as early as 2009 all the way through 2018 with a large concentration of account creation from mid-2013 to mid-2014. Notably, the IRA became more sophisticated in its operations over time by expanding to other account languages. Before 2015, the IRA opened accounts in only four languages: Arabic, Russian, English, and Indonesian. In 2015, it expanded to German, French, Mainland Chinese, and British English, and by 2018, it had opened accounts in eleven languages.

---

144 Chart created by the author with data from Twitter’s election integrity initiative.
The trends in English account creation displayed in Figure 9 merit special discussion. The vast majority of English account creations came during two primary spikes during the eighteen-month period from the second half of 2013 to the beginning of 2015. Account creation continued in smaller numbers through 2015 and 2016 with another small spike during the middle of 2017. The IRA created most of their accounts prior to the 2016 presidential campaign and election, laying the groundwork for their influence efforts. IRA trolls used this time to gather additional information concerning U.S. politics, even sending operatives to the U.S. to gather intelligence as described previously. They also began to test the reception of various messaging strategies concerning different U.S. political issues and developed an extensive network of affiliated Twitter accounts that would soon reference each other, publish similar (or conflicting) content, and mutually link separate IRA-

---

Figure 8: Account Creation by Language over Time\textsuperscript{145}

\textsuperscript{145} Chart created by the author with data from Twitter’s election integrity initiative.
controlled media like YouTube videos and longer form blog posts. SSCI researchers likened this interlinked network of social media accounts to a professional digital marketing strategy in which the IRA created “media mirages,” or “interlinked information ecosystems designed to immerse and surround targeted audiences.” IRA accounts tended to operate in “‘teams’ of co-mentioners” that shared a similar fictional online identity. These team members would then commonly mention each other “forming a number of coherent communities of interaction.” Notably, the average time between account creation and that account’s first tweet was 177 days, suggesting that IRA operatives meticulously crafted their network of teams and their first wave of content before beginning their influence campaign in earnest.


147 Ibid., Page 42.


149 Ibid.

3.3.3 Trends in English IRA Tweets

Of the more than nine million IRA tweets released by Twitter, IRA trolls published more than 5.1 million or 57% in Russian, and more than 3.2 million or 36% in English. Ukrainian represented the next most common tweet language, but only accounted for less than 3% of the IRA’s total tweets. The IRA tweeted in 37 other languages ranging from Arabic to Czech to Japanese as seen below in Figure 10, but these other languages represented less than 1% of total IRA tweets.

Figure 9: English IRA Account Creation over Time\textsuperscript{151}

\textsuperscript{151} Chart created by the author with data from Twitter’s election integrity initiative.
As described previously, IRA operatives engaged in a coordinated effort to amplify misinformation narratives. Looking at the number of re-tweets present in the data set help corroborate this conclusion. Retweets constituted more than 1.8 million of the English tweets, representing more than 33% of all English IRA activity. However, IRA operatives only created 1.9 million unique blocks of text used in their tweets. Since many of the same retweets were shared by multiple IRA-connected accounts, this means that a significant proportion of the remaining 3.6 million English IRA tweets were duplicates as well. This implies that IRA-run accounts independently published identical tweets as purportedly original content. Additional research analyzing when identical and nearly identical tweets occurred could provide a proxy for the number of IRA operatives running these networks of accounts. Viewed over time, this could provide insight into the overall expansion of IRA operations and inform the overall scope of the IRA’s disinformation dissemination.

Analysis performed by SSCI-contracted researchers showed that “the early focus of the IRA’s Twitter activity was the Russian public” who were “targeted with messages in

---

152 Chart created by the author with data from Twitter’s election integrity initiative.
Russian from fake Russian users,” but this focus shifted to U.S-focused activity in 2013 which corresponds well with the dramatic increase in English tweets depicted in Figure 11.\footnote{Philip N. Howard, Bharath Ganesh, Dimitra Liotsou, John Kelly, and Camille François. 2018. The IRA, Social Media, and Political Polarization in the United States, 2012-2018. Oxford: Computational Propaganda Research Project - University of Oxford, Page 25.} Clearly, English tweet volume skyrocketed through the end of 2014 and remained high through to the 2016 election. Notably, the number of IRA English tweets spiked again in the months after the presidential election. English tweet volume finally overtook the IRA’s production of Russian language tweets in mid-2017 “shortly before Twitter suspended the majority of accounts.”\footnote{Ibid.} In total, IRA accounts published more than 771,000 tweets in English during the ten months prior to the 2016 U.S. presidential election.\footnote{Gillian Cleary. 2019. Twitterbots: Anatomy of a Propaganda Campaign. June 5. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation.} This sustained level of activity and surge in English tweet volume likely indicate increased Kremlin enthusiasm in the IRA’s influencing efforts and potentially signal the allocation of additional resources necessary to maintain and expand these operations (which would parallel the IRA’s increased expenditure on social media advertising leading up to and continuing after the 2016 election).\footnote{Philip N. Howard, Bharath Ganesh, Dimitra Liotsou, John Kelly, and Camille François. 2018. The IRA, Social Media, and Political Polarization in the United States, 2012-2018. Oxford: Computational Propaganda Research Project - University of Oxford, Page 3.}
Figure 11: English Tweets over Time

Surprisingly, IRA trolls almost always directed Twitter users to reasonably reliable external websites and resources, including legitimate news outlets. In fact, of the tweets that included external website links, only 6% linked to junk news sites (defined as “websites that publish false or misleading news”). While this is about 50% higher than the rate that normal Twitter users link to junk news, the absolute number of links to junk news remains very low. That said, IRA tweets sharply increased the number of links to junk news just before the election, with more than 2,000 junk news links in a single week in

---

157 Chart created by the author with data from Twitter’s election integrity initiative.


159 Ibid.
September and October of 2016. While the absolute number of tweets with junk news links was low, the proportion of IRA accounts that published at least one of these tweets was high at 51%. Interestingly, this also means that “almost half of all IRA-run accounts only spread reliable information on Twitter.”

Digging deeper into the content of IRA tweets further exposes the IRA’s preference for then-candidate Trump. IRA accounts used the hashtag of the abbreviated Trump campaign slogan “Make America Great Again!,” #MAGA “massively — over 300,000 times in posts and biographies between 2015 and 2017.” On election day itself and echoing the Trump campaign’s unfounded accusations of widespread election fraud, “the trolls pushed the hashtag #riggedelection almost 100 times,” and throughout the campaign, “they posted on rigging [the election] almost 1,500 times...and #voterfraud 290 times.” These accusations reached massive audiences after “@TEN_GOP posted two claims of voting machines rejecting votes for Trump” that “scored a combined 31,847 retweets and 15,857 likes, a significant figure on such a crucial day.” To underscore Russian support for then-candidate Trump, accusations and supposed evidence supporting election fraud died away almost immediately after news organizations announced Trump’s victory.

Prior to this thesis, researchers had paid little attention to the IRA tweets that contained geographic location information. More than 4,400 of these tweets (less than 1% of all IRA tweets) included the latitude and longitude at which the Tweet was published. Figure 12 shows the locations of tweets that did. Table 4 shows that Twitter identified more than 95% of tweets that did as written in Russian. The vast majority of tweets written

---

160 Ibid., Page 4.
161 Ibid.
162 Ibid.
165 Ibid.
166 Ibid.
in Russian were also located in Russia. It remains unclear whether the inclusion of this location data was due to poor operational security or was an intentional effort to add legitimacy to IRA tweets in other languages purported to be from other countries. The Mueller indictments show the IRA used U.S. servers and VPNs to mask their location of origin and took other precautions to conceal their activity, so it is not surprising that so few tweets include location data. However, some English and German accounts that did include location data were registered from U.S. and German IP addresses, respectively.\textsuperscript{167} If IRA agents did intentionally include location data in select tweets, the small scale of these inclusions could hint that this tactic remained in its infancy, although tweets with location data did appear from at least 2013 to 2017.

Figure 12: Map of IRA Tweets with Location Information

Map created by the author with data from Twitter’s election integrity initiative. An interactive version is available here: https://chart-studio.plotly.com/~dwpro/7/#/.

168 Map created by the author with data from Twitter’s election integrity initiative. An interactive version is available here: https://chart-studio.plotly.com/~dwpro/7/#/.
Table 4: Tweets with Location Information by Language\textsuperscript{169}

<table>
<thead>
<tr>
<th>Language</th>
<th>Number of Tweets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bosnian</td>
<td>1</td>
</tr>
<tr>
<td>Bulgarian</td>
<td>25</td>
</tr>
<tr>
<td>Croatian</td>
<td>1</td>
</tr>
<tr>
<td>Czech</td>
<td>5</td>
</tr>
<tr>
<td>Danish</td>
<td>2</td>
</tr>
<tr>
<td>English</td>
<td>63</td>
</tr>
<tr>
<td>Estonian</td>
<td>2</td>
</tr>
<tr>
<td>Finnish</td>
<td>3</td>
</tr>
<tr>
<td>French</td>
<td>8</td>
</tr>
<tr>
<td>German</td>
<td>2</td>
</tr>
<tr>
<td>Greek</td>
<td>4</td>
</tr>
<tr>
<td>Hindi</td>
<td>1</td>
</tr>
<tr>
<td>Icelandic</td>
<td>1</td>
</tr>
<tr>
<td>Indonesian</td>
<td>1</td>
</tr>
<tr>
<td>Italian</td>
<td>1</td>
</tr>
<tr>
<td>Norwegian</td>
<td>3</td>
</tr>
<tr>
<td>Romanian</td>
<td>6</td>
</tr>
<tr>
<td>Russian</td>
<td>4193</td>
</tr>
<tr>
<td>Serbian</td>
<td>11</td>
</tr>
<tr>
<td>Slovak</td>
<td>2</td>
</tr>
<tr>
<td>Slovenian</td>
<td>3</td>
</tr>
<tr>
<td>Spanish</td>
<td>2</td>
</tr>
<tr>
<td>Swedish</td>
<td>1</td>
</tr>
<tr>
<td>Turkish</td>
<td>1</td>
</tr>
<tr>
<td>Ukrainian</td>
<td>65</td>
</tr>
<tr>
<td>Welsh</td>
<td>1</td>
</tr>
</tbody>
</table>

\textsuperscript{169} Table created by the author with data from Twitter’s election integrity initiative.

3.3 Broader Trends in Social Media-based Information Operations
Unfortunately, IRA operatives did not limit their manipulation efforts to Twitter. As described previously, the IRA took advantage of almost every major social media platform to push its messaging, and this cross-platform campaign did not end after the 2016 U.S. presidential election. In fact, Russian activity skyrocketed after election day. Table 5 shows the IRA received 45% more Facebook Ad clicks, published 59% more Facebook Posts, tweeted 52% more often, and created 238% more Instagram posts in the six-month period following the 2016 election than the six months before the election.

<table>
<thead>
<tr>
<th>Social Media Platform (Activity Metric)</th>
<th>Increase in Activity (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instagram (Number of Posts)</td>
<td>238</td>
</tr>
<tr>
<td>Facebook (Number of Posts)</td>
<td>59</td>
</tr>
<tr>
<td>Twitter (Number of Tweets)</td>
<td>52</td>
</tr>
<tr>
<td>YouTube (Number of Citations on Twitter)</td>
<td>84</td>
</tr>
<tr>
<td>Facebook (Number of Ad Clicks)</td>
<td>45</td>
</tr>
</tbody>
</table>

Table 5: Increase in IRA Activity in the Six-Month Period after the 2016 U.S. Election

As is evident in Figure 13, most IRA social media activity peaked in the twelve months following election day. IRA Facebook operations expanded to more than 5,000 Posts in the first months of 2017, while its Instagram activity climbed to more than 9,000 Instagram posts throughout the first few months of 2017. Interestingly, IRA Twitter activity actually peaked in the latter half of 2017 at almost 190,000 tweets in a single month before declining dramatically (after Twitter took down the IRA’s network in late 2017).

---

170 Ibid., Page 10.
Russia's repeated attempts to manipulate U.S. public opinion are only the first of an ongoing, global wave of state-run disinformation efforts that use social media to influence voter behavior. Following its initial disclosure in August of 2018, Twitter redoubled its efforts to expose information operations on its platform, publishing seven more data releases and ultimately exposing 28 information operation campaigns linked to 15 different countries across four continents. (Of note, Twitter did not explicitly attribute these identified campaigns to any state government or other entity, aside from the first release's association with the Internet Research Agency; instead, these campaigns were identified solely by the country in which they occurred.)

Similarly, Facebook has had to drastically increase its election protection efforts and has taken down more than 50 networks of accounts around the world, many before major elections.

---

171 Ibid., Page 11.


The same researchers from the University of Oxford’s Computational Propaganda Project that authored one of two reports for the SSCI have since found evidence of social media manipulation campaigns “in 70 countries [in 2019], up from 48 countries in 2018 and 28 countries in 2017.” Authoritarian regimes seem to especially favor these campaigns “to suppress fundamental human rights, discredit political opponents, and drown out dissenting opinions” domestically, while the most sophisticated state actors: China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela, “have used these platforms to influence global audiences.”

---


175 Ibid.
4 Policy Review

The revelation of Russian attempts to manipulate U.S. public opinion exposed glaring inadequacies in the internal policies of social media platforms and federal law alike. Social media executives received tremendous external pressure to close many of these loopholes and pursued admirable initiatives to improve their platforms’ transparency while cooperating (at varying degrees) with federal investigations into Russia’s exploitation of their social network spaces. The executive branch of the federal government weathered the same public pressure, but responded with contradicting messaging and actions as President Trump continuously derided the intelligence community’s conclusions and dismissed Russia’s efforts while the DOJ investigated possible connections between his campaign team and the Russian government, issuing multiple indictments in the process. While the Trump administration did escalate the tit-for-tat expulsion of Russian intelligence officers in the U.S. that had begun under President Obama, any other executive action proved symbolic, toothless, and begrudgingly pursued. Congress, however, accomplished even less during the last four years, successfully passing a single bill that prevented President Trump from removing the sanctions applied to Russia by his predecessor. The hyper partisan political environment fomented by the Oval Office doomed dozens of other promising bills designed to improve various facets of U.S. election security and deter future foreign manipulation, creating a legislative graveyard in both the House and Senate.

4.1 Policy Landscape Prior to the Exposure of Russian Influence Efforts

Before Donald Trump declared his candidacy and well before most Americans had heard about Russian trolls impersonating Americans online, social media platforms stuck to their own Silicon Valley bubble, preferring to maximize their platform’s reach and advertising income while attempting to steer clear of Washington politics. Decades old legislation allowed them to police their own platforms, moderating content as they deemed
necessary, provided they abided by federal laws against pornography. Various government institutions and agencies governed and facilitated federal elections, and political advertising on social media was still in its infancy. This hands-off approach to social media regulation and these anachronistic election laws created the ideal environment in which to launch a covert effort to manipulate political discussion in the United States.

4.1.1 Social Media Policies Prior to the Exposure of Russia’s Influence Campaign

Prior to the exposure of Russia’s coordinated influence campaign, social media platforms and the United States federal government had extensive private and public policies backed by decades-old legislation that aimed to prevent inappropriate activity on their platforms or in government, respectively, but neither the technology’s designers in Silicon Valley nor policy makers in Washington D.C. imagined that a foreign power might abuse both to conduct a full scale information operations campaign via social media to attempt to influence the outcome of the 2016 U.S. presidential election.

Section 230 of the Communications Decency Act of 1996 (CDA) provides the foundation for online content moderation through its “Protection for ‘Good Samaritan’ Blocking and Screening of Offensive Materials.” Originally passed to prevent the spread of pornography on the Internet, this provision removed civil liability for any action voluntarily taken “in good faith” by social media platforms to remove material uploaded to their platforms by third parties that was considered obscene, violent, or otherwise objectionable. While subsequent legislation including the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 mandated that interactive computer services like social media platforms remove content related to child pornography or sex trafficking, social media companies still maintain remarkable latitude to control the content on their platforms.

Most social media companies including Facebook, Twitter, and Snapchat define the content and user behavior they deem objectionable through internally developed terms of service, the formal agreement between users and companies that all users must agree to in order to access the platform. Prior to the 2016 election, most social media companies' terms of service included policies against impersonation and inauthentic coordinated activity (common amongst spam networks) on their platforms, and they routinely banned and deleted Tweets, Posts, Pages, and accounts for violating these community guidelines. Despite these rules and their associated enforcement, social media companies had not imagined that a cyber savvy geopolitical adversary might covertly violate these policies to push propaganda within the United States. This lack of imagination persisted in social media political advertising which lacked sufficient confirmation mechanisms to verify that the individual or organization purchasing those advertisements was, indeed, American.

4.1.2 Federal Policies Prior to the Exposure of Russia’s Influence Campaign

Similarly, the U.S. federal government maintains an extensive series of policies governing foreign involvement in elections, political fundraising, lobbying, and more generally, the flow of foreign individuals into the country, but these proved just as easily exploitable by a determined foreign power. The indictment issued by Special Counsel

---


Mueller’s team against the IRA and associated Russians succinctly identifies the roles played by the Federal Election Commission, the Department of Justice, and the Department of State in limiting foreign influence in U.S. elections, but these organizations had not yet considered the feasibility of conducting a full scale influence campaign from half a world away.

The Federal Election Commission administers the Federal Election Campaign Act of 1971 (FECA) which “prohibits foreign nationals from making any contributions, expenditures, independent expenditures, or disbursements for electioneering communications” and “also requires that individuals or entities who make certain independent expenditures in federal elections report those expenditures to the Federal Election Commission.”¹⁸³ These obligatory disclosures “permit the Federal Election Commission to fulfill its statutory duties” but also force it into a reactive role, able to respond only when an individual or organization voluntarily submits evidence of their own wrongdoing.¹⁸⁴

Similarly, the “Department of Justice administers the Foreign Agent Registration Act (FARA)...which establishes a registration, reporting, and disclosure regime for agents of foreign principals”--which critically “includes foreign non-government individuals and entities.”¹⁸⁵ This inclusion defends against Russian government attempts to claim plausible deniability in this instance, given the IRA’s positioning within Concord businesses. FARA mandates that individuals “subject to its requirements submit periodic registration statements containing truthful information about their activities and the income earned from them.”¹⁸⁶ Again, the federal government relies on the disclosure of required information by foreign agents to monitor those same foreign agents, paving the way for bad actors who wish to conceal their political activity to easily do so.


¹⁸⁴ Ibid.

¹⁸⁵ Ibid.

¹⁸⁶ Ibid.
The U.S. Department of State controls “the issuance of non-immigrant visas to foreign individuals who need a visa to enter the United States,” and again the decision making behind who receives a visa is dependent on information provided by foreign individuals “about their employment and the purpose of their visit to the United States.”

This presents another example of an easily exploitable regulation that facilitates all kinds of information operations and intelligence gathering activity. In the context of the IRA’s election influencing campaign, sending agents to the U.S. to gather intelligence on domestic politics wasn’t even necessary. The insight into target swing states like Michigan is not epiphanic and represents one of the most fundamental strategies of campaigning in presidential elections and could have been found easily online. Similarly, the racial and religious tensions present within the U.S. have also been the long-time targets of political and commercial advertising campaigns. The utility of IRA intelligence collection within the U.S. remains dubious at best, especially when the divisions reported back to IRA content teams already thrived on the social media platforms the IRA sought to exploit.

Similar to the policies guiding social media, the law governing elections created an election system ripe for foreign exploitation. The Federal Election Campaign Act of 1971 failed to obligate political campaigns to report suspected foreign information operations to US law enforcement. Coordination between law enforcement, the intelligence community, and social media companies remained in its infancy, confined to isolated incidents and counter terrorism efforts; established information sharing did not exist. Federal law also neither designated responsibility for the investigation of possible election interference nor establish a reporting mechanism or timeline for the results of those investigations. Finally, no penalties existed for the intentional spread of material designed to prevent others from voting. Together, these oversights facilitated a permissive operating environment suited for foreign manipulation.

---

187 Ibid., Page 11-12.
4.2 Policy Changes Following the Exposure of Russian Influence Efforts

While some social media platforms (e.g. Facebook) took significantly more time to roll out new measures aimed at ensuring the integrity of domestic debate and elections, these platforms made immensely more progress than the United States Congress.

4.2.1 Action Taken by Social Media Platforms

Following the 2016 U.S. presidential election and the reveal of Russian interference efforts, social media companies pursued various strategies to stop coordinated inauthentic behavior on their platforms.

Twitter arguably adopted the most activist strategy, first making the data provided to the SSCI available to the public—a step towards transparency that no other social media platform has matched—and then releasing updated policies that forbade many of the tactics the IRA used to build a presence on the platform and use that presence to impact U.S. public opinion. In September of 2019, Twitter expanded its terms of service to include policies against the use of its service “to artificially amplify or suppress information or engage in behavior that manipulates or disrupts people’s experience on Twitter.” This policy explicitly prohibited “inauthentic engagements, that attempt to make accounts or content appear more popular or active” and “coordinated activity, that attempts to artificially influence conversations through the use of multiple accounts, fake accounts, [or] automation.”

Just one month later in October, Twitter CEO Jack Dorsey announced (via tweet) that Twitter had “made the decision to stop all political advertising on Twitter globally.”


189 Ibid.

190 Jack Dorsey. 2019. "We’ve made the decision to stop all political advertising on Twitter globally. We believe political message reach should be earned, not bought. Why? A few reasons...." Twitter.com. October 30. https://twitter.com/jack/status/1189634360472829952.
Twitter grounded this decision to ban all political advertising in the justification that political messaging “earns reach” when people choose to interact with and spread it themselves, and therefore should not require artificial distribution through paid targeted ads.\textsuperscript{191} Twitter CEO Jack Dorsey also indirectly acknowledged the fact that Twitter cannot feasibly monitor all political content due the prevalence of dubious or misleading information, the increasing sophistication of that messaging, and the “overwhelming scale” of political speech and advertising.\textsuperscript{192} This decision received praise from liberal lawmakers including Representative Alexandria Ocasio-Cortez of New York who stated that: “if a company cannot or does not wish to run basic fact-checking on paid political advertising, then they should not run paid political ads at all.”\textsuperscript{193} However, the impact this voluntary ban has had remains in doubt as “Twitter ads make up [only] a small fraction of what the presidential candidates have spent on digital advertising over all, with more money going toward Facebook and Google ads” in the 2018 midterm election than ever before.\textsuperscript{194}

In May of 2020, Twitter took additional steps to prevent the use of its platform to impact democratic elections with the roll out of its civic integrity policy.\textsuperscript{195} This new policy expressly prohibited the use of “Twitter’s services for the purpose of manipulating or interfering in elections or other civic processes,” including “posting or sharing content that may suppress participation or mislead people about when, where, or how to participate in a civic process”—all tactics employed by the IRA.\textsuperscript{196} Twitter defined civic processes as political elections, censuses, major referenda, and ballot initiatives, and specifically identified voter suppression and intimidation and the creation of fake accounts that

\textsuperscript{191} Ibid.
\textsuperscript{192} Ibid.


\textsuperscript{194} Ibid.


\textsuperscript{196} Ibid.
“misrepresent their affiliation, or share content that falsely represents its affiliation, to a candidate, elected official, political party, electoral authority, or government entity” as bannable offenses.197

Facebook, while initially reluctant, made significant strides of its own to prevent the use of its platform in election influence campaigns by nation states and non-state actors. Following the 2016 presidential election, Facebook grudgingly cooperated with the SSCI’s investigation into IRA influencing efforts (described previously). In April of 2017, Facebook announced initial efforts to stop misinformation and false news on its social media platforms, but these steps narrowly focused on disrupting economic incentives behind inauthentic behavior on Facebook and improving its ranking and reporting methodologies.198 None of these steps directly tackled the issue of a foreign power influencing domestic political opinion in the U.S. Finally, in April of 2018, Facebook announced it had taken down a network of 70 Facebook accounts, 138 Pages and 65 Instagram accounts linked to the IRA.199 For the first time, Facebook directly acknowledged that the “IRA has no place on Facebook.”200 In September of 2018, Facebook announced the creation of a “war room” that gathered Facebook employees “focused on rooting out disinformation, monitoring false news and deleting fake accounts that may be trying to influence voters before” the 2018 midterm elections.201 Shortly thereafter, it formally institutionalized this war room as its Election Operations Center and subsequently expanded operations to oversee the 2019 prime minister elections in India and the

197 Ibid.
200 Ibid.
European Union’s parliamentary election in 2019.\textsuperscript{202,203} One month later, Facebook expanded its voter suppression policies to ban “misrepresentations about how to vote” including the ability to vote via text or app and false “statements about whether a vote will be counted” or not, foreshadowing growing ideological agreement over the role of social media in preserving the integrity of elections with Twitter.\textsuperscript{204}

Over the next year Facebook announced the removal of 50 networks of coordinated inauthentic behavior worldwide ahead of major democratic elections which included at least one Russian network conducting “proactive work ahead of the [2020] U.S. elections.”\textsuperscript{205} In October of 2019, Facebook updated its inauthentic behavior policy to clarify how Facebook deals with deceptive practices on its platform, “whether foreign or domestic, state or non-state.”\textsuperscript{206} Importantly, Facebook committed that coordinated inauthentic behavior “conducted on behalf of a government entity or by a foreign actor” will merit “the broadest enforcement measures including the removal of every on-platform property connected to the operation itself and the people and organizations behind it.”\textsuperscript{207} Facebook simultaneously launched Facebook Protect, a service designed to “secure the accounts of elected officials, candidates, their staff and others who may be particularly vulnerable to targeting by hackers and foreign adversaries” interested in influencing the outcome of various elections.\textsuperscript{208}


\textsuperscript{207}Ibid.

\textsuperscript{208}n.d. Facebook Protect. \url{https://www.facebook.com/gpa/facebook-protect}. 
Facebook also increased the transparency of political advertising, making political ad data more accessible across its social media platforms including Facebook, Messenger, and Instagram. This included the roll out of a U.S. presidential candidate spend tracker that publicly showed how presidential candidates spent their advertising dollars on the platform, but Facebook stopped short of committing to identify political advertising purchased by foreign nations. Instead, Facebook focused on expanding the overall transparency of Page provenance by requiring individuals and organizations behind Facebook Pages to confirm their Page’s ownership and verify their organizations legal name, city, phone number, and website. A state intelligence service could still covertly overcome these additional transparency measures via manufactured or stolen identities, but these requirements provide another financial and logistical hurdle in doing so.

Facebook partially addressed the issue of foreign political advertising in January of 2020, when it required all advertisers to assign a Page Owner “in order to continue running issue, electoral, or political ads in the U.S.” However, coordinated covert activity could still circumvent these additional safeguards.

In February of 2020, Facebook took steps toward more complete transparency associated with its handling of foreign networks by starting to issue monthly reports on the networks of coordinated inauthentic behavior it had identified and removed. However, while Facebook includes some summary statistics describing these networks including the number of pages and accounts involved, it still has not made data on these networks fully available to the public as Twitter has done. Still, this trend towards transparency and accountability marks legitimate progress and shows that social media platforms have

---


210 Ibid.

211 Ibid.

become notably more serious about protecting the integrity of elections in the U.S. and around the world. Unfortunately, the same cannot be said of the U.S. federal government.

4.2.2 Action Taken by the Federal Government

Following the revelation that a foreign power attempted to mold domestic public opinion to influence the election, then-President Barack Obama issued Executive Order No. 13694 which expanded federal power to respond to cyber activity that seeks to interfere with U.S. elections or institutions. Using this new authority, President Obama issued sanctions against nine entities and individuals including agents of the GRU and the Federal Security Service of the Russian Federation (FSB) and ordered the Department of State both to shut “down two Russian compounds, in Maryland and New York, used by Russian personnel for intelligence-related purposes” and to declare 35 Russian intelligence agents operating in the U.S. under diplomatic cover “persona non grata,” thereby expelling them and their families from the country. Several months later, after then President-elect Trump made several comments questioning these sanctions during his campaign and continued this questioning after he assumed office, Congress passed the Countering America’s Adversaries Through Sanctions Act of 2017 (CAATSA) which limited President Trump’s ability to rescind the sanctions issued by President Obama by requiring the President to provide evidence to Congress that Russia had reduced the number and


intensity of its cyberattacks against the U.S.\textsuperscript{216,217} Days after Congress reaffirmed these sanctions, Russian President Vladimir Putin announced that the American diplomatic mission in Russia had to reduce its staff by 755 employees to only 455 in a tit-for-tat response.\textsuperscript{218} In retaliation, the State Department “ordered Russia...to close its consulate in San Francisco and two diplomatic annexes...in New York and Washington.”\textsuperscript{219}

Despite these initial responses and the sanctions ordered in the two previously described indictments from Special Counsel Mueller, President Trump’s administration took few additional steps to hold Russia accountable or to defend against foreign interference in future U.S. elections.\textsuperscript{220}

On September 12th, 2018, President Trump signed Executive Order No. 13848, titled “Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election,” which established an interagency process for determining if foreign election interference occurred and set the stage for sanctions to be applied directly against those “who actually interfered and their facilitators.”\textsuperscript{221} However, this order did not establish truly automatic sanctioning as proposed by legislators on Capitol Hill.\textsuperscript{222}

\begin{itemize}
  \item \textsuperscript{217} Ibid., Sec. 216. Congressional Review of Certain Actions Relating to Sanctions Imposed with Respect to the Russian Federation.
  \item \textsuperscript{222} Ed Stein. 2018. What’s in the Executive Order on Election Interference? September 19. \url{https://www.lawfareblog.com/whats-executive-order-election-interference}.\end{itemize}
No. 13848 tasked the Department of Treasury to identify specific individuals responsible for interference attempts, but did not implement any broader sanctions against the interfering country, instead reserving the decision to implement additional sanctions for the White House. Additionally, Section 1 of the Order focuses “almost exclusively on disruptions to ‘election infrastructure’” which it narrowly defines as:

[I]nformation and communications technology and systems used by or on behalf of the Federal Government or a State or local government in managing the election process, including voter registration databases, voting machines, voting tabulation equipment, and equipment for the secure transmission of election results.

The Order does manage to include the type of concerted, information operations-based influence campaign in its definition of foreign interference:

[A]ny covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions...

But ultimately, the Order fails to explicitly cite social media or internet-based disinformation efforts, “which reportedly had been included in an earlier draft.”

223 Ibid.
225 Ibid., Section 8. (f).
227 Shane Harris, Josh Dawsey, and Ellen Nakashima. 2018. White House drafting sanctions order to punish foreign interference in U.S. elections. August 8. https://www.washingtonpost.com/world/national-
striking exclusion and largely discretionary sanctioning took the teeth out of what could have been strong signaling and enforcement mechanisms that made it clear the U.S. would not tolerate additional influence campaigns in future elections.

Isolated sanctioning continued when the Department of Justice released a criminal complaint titled, United States of America v. Elena Alekseevna Khusyaynova, on October 19th, 2018 that charged a Russian national, Elena Alekseevna Khusyaynova “for her alleged role in a Russian conspiracy to interfere in the U.S. political system, including the 2018 midterm election.”228 Ms. Khusyayova served as the chief accountant for the IRA’s “Translator Project” and personally oversaw all financial activity associated with the production and dissemination of IRA-generated content and advertising during the 2016 U.S. presidential election in other IRA disinformation campaigns around the world.229

Just days after the DOJ filed charges against Ms. Khusyayova, news broke that the United States Cyber Command (CYBERCOM) had begun to target individual Russians in an attempt to deter them from “spreading disinformation to interfere in [U.S.] elections.”230 CYBERCOM reportedly alerted Russian oligarch-funded hacking groups and Russian intelligence operatives who were part of Moscow’s disinformation campaign that they are known to and under surveillance by the US intelligence community.231 Several months later after the 2018 U.S. midterm elections, the White House again issued a handful of additional sanctions against “four entities, seven individuals, three aircraft, and a


231 Ibid.
yacht...all associated with the Internet Research Agency and its financier, Yevgeniy Prigozhin.”

In February of 2018, the Washington Post reported that CYBERCOM had conducted a cyber-attack that blocked internet access to the Internet Research Agency on the day of the 2018 U.S. midterm elections. President Trump later confirmed the United States' involvement in an interview with Washington Post columnist Marc Thiessen to demonstrate his toughness on Russia, but sources for the New York Times and other media claim that he did personally order the operation. While this use of offensive U.S. cyber capabilities was the first of its kind, it was too little, too late. The effects of a concerted Russian influence campaign would have occurred in the months and weeks before election day. Foreign policy experts characterized the CYBERCOM operation as “more of a pinprick that is more annoying than deterring in the long run,” but defense officials countered that “grand strategic deterrence’ is not always the goal,” and lauded the attack for showing Russian what the U.S. could do.

In August of 2020, the Trump administration made another unusual attempt to prevent foreign influence in the upcoming 2020 U.S. presidential election. The U.S. Department of State sent text messages to an unknown, but reportedly large number of Russians and Iranians offering up to $10 million USD for information about people “trying
to attack American voting systems.” This messaging campaign drew immediate derision from Russian and Iranian social media users who joked about starting their own influence efforts to report on themselves for the reward. A Russian government spokesperson responded less humorously, calling it an American hybrid attack on Russian daily life.

While these actions taken together represent a start toward preventing foreign influence in U.S. elections, they remain more symbolic than anything. Expelling Russian intelligence officers and closing consulates will undoubtedly hurt Russia’s intelligence collection within the U.S., but the IRA’s influence campaign was undertaken remotely, aside from the brazen decision to send a handful of operatives to the U.S. Issuing targeted sanctions against those involved might have more of a deterrent effect by minimizing the enthusiasm of those conducting these operations (similar to the potential deterrent effect of notifying IRA operatives that they are under surveillance), symbolically knocking out power for a single day and soliciting information with a monetary reward fail to demonstrate the U.S. will take every necessary action to preserve the integrity of our democratic process.

4.3 Proposed Policy Responses and Legislation

While social media companies (some more reluctantly than others) scrutinized and improved their own policies to better prevent future election influence campaigns and the federal government made some halting progress in doing the same, the United States Congress failed to take any substantive action. Aside from CAATSA in 2017 which only ensured that President Trump could not remove Obama-era sanctions against Russian

---


238 Ibid.

239 Ibid.
individuals, both chambers of Congress failed to pass any election protecting legislation despite a dozen attempts to do so.

4.3.1 Legislation Proposed in the U.S. House of Representatives

In the U.S. House of Representatives, legislators introduced more than a dozen pieces of legislation that aimed to deter foreign influence through a variety of approaches including: mandating the report of foreign assistance during a campaign, reinforcing U.S. election infrastructure, and guaranteeing sanctions in response to foreign interference. However, despite these efforts, no legislation on this topic passed both chambers of Congress to become law. Among this multitude of failed proposals, very few even directly acknowledged foreign attempts to manipulate domestic public opinion, and even fewer enumerated how they would deter such covert foreign influence from happening again.

_H.R.5011 - Election Security Act of 2018_

On February 14th, 2018, Democratic Congressman Bennie Thompson from Mississippi introduced the first piece of election security-oriented legislation following the 2016 presidential election aptly titled the “Election Security Act of 2018.” Fairly narrow in scope, H.R.5011 primarily focused on the security of election infrastructure, establishing grant programs to support state voting system security, state audits of federal election results, and further research and development into election infrastructure security. However, H.R.5011 also required “the President to develop a national strategy to protect against attacks on U.S. democratic institutions, and...establishe[d] the National Commission to Protect U.S. Democratic Institutions.” The first of their kind, these last two points


\[241\] Ibid.

\[242\] Ibid.
indirectly acknowledged Russia’s interference in the 2016 U.S. presidential election and sought to prevent a recurrence in subsequent elections. After its introduction, H.R.5011 was referred to the Committee on House Administration, and in addition to the Committees on Homeland Security, Intelligence (Permanent Select), the Judiciary, and Foreign Affairs before being referred to the Subcommittee on Cybersecurity and Infrastructure Protection where it remained unaddressed through the end of the 115th Congress.

H.R.6436 - To direct the Director of National Intelligence to submit to State election officials and Congress annual reports on pre-election threats for general elections for Federal office.

Several months later, Representative Kathleen Rice from New York introduced a related bill entitled “To direct the Director of National Intelligence to submit to State election officials and Congress annual reports on pre-election threats for general elections for Federal office” which, as evident, aimed to identify “threats to election infrastructure and make recommendations to address those threats.” H.R.6436 was referred to the House Committee on Intelligence (Permanent Select) where it similarly stalled. While the provisions of this bill did not directly address the IRA’s social media influence operations, its affiliation with federal elections and subsequent “death by committee” would become the hallmark of most election security legislation proposed over the next four years.

H.R.1 - For the People Act of 2019

Following the 2018 midterms and subsequent transfer of power to the Democratic party in the House, the first piece of legislation of the 116th Congress, the “For the People Act of 2019,” was introduced by Representative John Sarbanes of Maryland on January 3, 2019. H.R.1 contained dozens of wide-ranging provisions including several that


primarily addressed “voter access, election integrity, election security, political spending, and ethics for the three branches of government.”

H.R.1 provided numerous policies that would harden U.S. federal elections against traditional election interference by requiring paper ballots, mandating cyber threat intelligence sharing, and funding improvements to outdated election infrastructure, and it also attempted to minimize foreign influence in future elections through banning certain campaign contributions from foreign nationals, mandating the compilation and public release of political advertisements on social media, and ensuring the enforcement of current regulations governing contact with foreign agents.

H.R.1 also included several more politically contentious provisions, including mandatory tax return release from U.S. presidential candidates, non-partisan redistricting commissions, and federal matching for small contributions to cash poor candidates.

When taken together, H.R.1 policies sought to make attempted foreign election influence unlikely to be successful, thus undermining a foreign power’s motivation to invest in an influence campaign. The 2016 presidential election and subsequent reported global influence campaigns provided reasonable exigency for these proposals, and House Democrats introduced them early enough to take effect before the 2020 U.S. presidential election, but the inclusion of the previously noted politically charged provisions meant that despite the passage of H.R.1 by the Democrat-controlled House, it was dead on arrival in the Republican-controlled Senate. H.R.1 quickly transitioned to a symbolic gesture by House Democrats against foreign meddling and the perceived indifference from the White House.

This remains unfortunate as the policies included in H.R.1 would have hardened the U.S. democratic process against foreign influence for years to come, raising the level of risk and investment required to interfere in U.S. elections. However, H.R.1 still lacked proposals that would directly deter the primary method of previous Russian influence:

---

245 Ibid.

246 Ibid.

247 Ibid.

covertly created and disseminated social media content designed to further divide the already polarized American political environment.

*H.R.378 - Safeguarding Election Infrastructure Act of 2019*

Almost a week later on January 9th, 2019, Representative Debbie Dingell of Michigan introduced the “Safeguarding Election Infrastructure Act of 2019.” H.R.378 included measures to increase the security of federal elections, including: “requiring paper ballots, requiring audits of election results, and providing support for voting system security improvements.” H.R.378 was referred to the Committee on House Administration, and to the Committee on Science, Space, and Technology where it was internally referred to the Subcommittee on Research and Technology where it remained. Again, these safeguards would have undoubtedly hardened federal election infrastructure, but they fail to deter against coordinated influence campaigns that target public opinion rather than ballot machines or vote tallies.

*H.R.2424 - Duty to Report Act of 2019*

On April 30th, Representative Eric Swalwell, a Democrat from California, proposed the “Duty to Report Act of 2019,” which sought to “amend the Federal Election Campaign Act of 1971 to require reporting to the Federal Election Commission and the Federal Bureau of Investigation of offers by foreign nationals to make prohibited contributions, donations, expenditures, or disbursements, and for other purposes.” After H.R.2424’s introduction, it was referred to the Committee on House Administration and the Committee on Science, Space, and Technology where it was internally referred to the Subcommittee on Research and Technology where it remained.

---


250 Ibid.

251 Ibid., Actions.

on the Judiciary where it was referred to the Subcommittee on the Constitution, Civil Rights, and Civil Liberties, where it remained, although its key provisions were later incorporated into H.R.4617. H.R.2424 directly addressed foreign interference akin to Russia’s reported attempts to notify the Trump campaign of the impending release of the “Podesta emails.” However, it too failed to address influence campaigns conducted through social media.

H.R.2660 - Election Security Act of 2019

The following month, Representative Bennie Thompson introduced a new version of his previous bill titled the “Election Security Act of 2019.” H.R.2660 expanded on H.R.5011, adding federal requirements for state voting systems that mandated the use of paper ballots made in the U.S., required states to make voter’s ballots available for inspection by the voter before election day, and ensured Americans with disabilities could vote via paper ballot. In addition to the grant requirements in H.R.5011, it also directed the National Science Foundation to award grants to develop accessible voter-verified paper ballots. H.R.2660 called for information sharing between the federal government regarding threats to election infrastructure and required the Department of Homeland Security to “issue a national strategy to protect against cyberattacks, influence operations, disinformation campaigns, and other activities that could undermine the security and integrity of democratic institutions.” This last provision serves as the first legislative

253 Ibid., Actions.


257 Ibid.

258 Ibid.
proposal to try to tackle the foreign manipulation of public opinion. H.R.2660 never progressed after its referral to the Committees on House Administration; Homeland Security; Intelligence (Permanent Select); Science, Space, and Technology; Foreign Affairs; and the Judiciary and following internal referral to the Subcommittees on Research and Technology; Cybersecurity, Infrastructure Protection, and Innovation; and the Constitution, Civil Rights, and Civil Liberties.259 On this occasion, the lion’s share of H.R.2660’s provisions were subsumed in another garnered more support, H.R. 2722.


That same month, Democratic Representative Zoe Lofgren of California introduced the “Securing America’s Federal Elections Act of 2019” better known as the “SAFE Act.”260 H.R.2722 incorporated much of H.R.2660 verbatim, but originally excluded the requirement for DHS to develop a national strategy and allowed a separate provision for states to use election related funding on election security efforts.261 Ultimately, the Democrat-controlled House passed a version of the SAFE Act that included the original provisions and added the requirement that voting systems “meet specified cybersecurity requirements, including the prohibition of the connection of a voting system to the internet.262 Unfortunately, the SAFE Act failed to gain traction in the Republican-controlled...
Senate despite two separate introductions by Senator Amy Klobuchar from Minnesota as S.2053 on June 28, 2019 and as S.2238 on July 23, 2019.263,264,265

_H.R.3281 - Deceptive Practices and Voter Intimidation Prevention Act of 2019_

On June 13, 2019, Democratic Representative Donald McEachin of Virginia introduced the “Deceptive Practices and Voter Intimidation Prevention Act of 2019” which prohibited

> [A]ny person, within 60 days before an election, from communicating, causing to be communicated, or producing for communication certain information on voting, if the person (1) knows such information to be materially false, and (2) has the intent to impede or prevent another person from exercising the right to vote in an election.266

H.R.3281 also made it illegal “to issue false statements regarding public endorsements and hindering, interfering with, or preventing voting or registering to vote” and established criminal penalties for violations.267 It also charged the DOJ to identify such violations as materially false and communicate accurate information in response.268 After its introduction to the House, H.R.3281 was referred to the House Committee on the Judiciary and then internally to referred to the Subcommittees on Crime, Terrorism, and Homeland Security; on the Constitution, Civil Rights, and Civil Liberties; and on Courts, Intellectual

263 Ibid., Actions.


267 Ibid.

268 Ibid.
Property, and the Internet before being almost entirely incorporated into H.R.4617, the SHIELD Act.269

**H.R.3412 - Election Security Assistance Act**

On June 21, 2019, Republican Representative Rodney Davis of Illinois proposed the first of few GOP-sponsored election security bills, the “Election Security Assistance Act.”270 This bill included the majority of provisions as H.R.2722, but removed the federal requirements called for in the SAFE Act and reduced “the appropriated funds to just $380 million for the 2020 elections” as opposed to the $600 million championed by House Democrats.271 H.R.3412 was referred to the Committees on House Administration and Intelligence (Permanent Select) and subsequently dropped.272

**H.R.3442 - Defending Elections against Trolls from Enemy Regimes Act**

Three days later, Republican Representative Doug Collins of Georgia introduced the “Defending Elections against Trolls from Enemy Regimes Act” which aimed to “amend the Immigration and Nationality Act to provide that aliens who engage in improper interference in a United States election are inadmissible and deportable.”273 H.R.3442 served as the companion bill to S.1328 of the same name which had passed the Senate

---


without amendment by Unanimous Consent. House Democrats subsequently referred H.R.3442 to the House Committee on the Judiciary which referred it to its Subcommittee on Immigration and Citizenship where it has remained since.

H.R.3873 - Foreign Influence Reporting in Elections Act

On June 22, 2019, Democratic Representative Elissa Slotkin of Michigan proposed the “Foreign Influence Reporting in Elections Act” which called for an amendment to the Federal Election Campaign Act of 1971 to “clarify the obligation to report acts of foreign election influence and require implementation of compliance and reporting systems by Federal campaigns to detect and report such acts.” Following its introduction H.R.3873 was referred to the house Committee on House Administration where it remained after H.R.4617 incorporated its primary provisions. Like other bills before it and H.R.4617 after it, H.R.3873 helped deter foreign contacts with U.S. election campaigns akin to reported Russian contact with the Trump campaign, however, it did not address social media centric influence campaigns.

H.R.4114 - Stop Supporting Foreign Interference in Our Democracy Act of 2019

Later that month, Democratic Representative Chrissy Houlahan of Pennsylvania introduced the “Stop Supporting Foreign Interference in Our Democracy Act” which aimed to amend the Federal Election Campaign Act of 1971 to make it explicitly illegal for an American individual to assist a foreign national to make a political contribution or donation.


277 Ibid., Actions.
to any U.S. election campaigns or political organizations. After referral to the House Committee on House Administration, a more specific version of H.R.4114 banning foreign contributions “to campaigns related to ballot initiatives and referenda” and “certain internet activity referring to a candidate or a political issue” was included in the SHIELD Act.

**H.R.4612 - Firewall Act of 2019**

Later that year, Democratic Representative from Minnesota Dean Phillips introduced the “Firewall Act” which contained a provision to prohibit “foreign nationals from making disbursements for digital political advertising” entirely. Similarly to H.R.4114, after H.R.4612 was referred to the House Committee on House Administration, House Democrats incorporated the “Firewall Act’s” central provision into the SHIELD Act.

**H.R.4617 - Stopping Harmful Interference in Elections for a Lasting Democracy (SHIELD) Act of 2019**

In October of 2019, Democratic Representative Zoe Lofgren introduced new legislation, the “Stopping Harmful Interference in Elections for a Lasting Democracy

---


279 Ibid., Actions.


282 Ibid., Actions.

(SHIELD) Act of 2019. H.R.4617 incorporated H.R.3281: Deceptive Practices and Voter Intimidation Prevention Act of 2019 almost in its entirety and contained a companion bill to Senator Amy Klobuchar’s S.1356, the Honest Ads Act of 2019. As previously described, the “SHIELD Act” included several amendments that incorporated key provisions from H.R.2424, H.R.3873, H.R.4114, H.R.4612, and H.R.4703 to establish the duty for campaigns to report unlawful foreign election assistance to the FBI and FEC, prohibit foreign contributions to campaigns related to ballot initiatives and referenda, and ban foreign funding of internet activity (e.g. digital advertising) referring to a candidate or issue.

House leadership referred H.R.4617 to the Committee on House Administration and the Committee on the Judiciary before it was discharged and subsequently passed by the house on October 23, 2019. The Senate received it on October 28, 2019 and referred it to the Committee on Rules and Administration.

H.R.4703 - Defending Elections from Foreign Efforts to Negate Democracy (DEFEND) Act of 2019

On October 16, 2019, Democratic Representative Conor Lamb from Pennsylvania proposed the “Defending Elections From Foreign Efforts to Negate Democracy (DEFEND) Act” which sought to prohibit “foreign nationals from making disbursements for internet activity promoting, supporting, attacking, or opposing the election of a candidate for public office.”

284 Ibid.
285 Ibid.
286 Ibid.
288 Ibid.
office."289 After referral to the House Committee on House Administration, this prohibition was almost directly incorporated into the SHIELD Act.290,291

H.R.6088 - Deepfakes in Federal Elections Prohibition Act

On March 4, 2020, Democratic Representative Stephen Lynch of Massachusetts introduced the “Deepfakes in Federal Elections Prohibition Act” which sought to “amend the Federal Election Campaign Act of 1971 to prohibit the distribution of materially deceptive audio or visual media prior to an election for Federal office.”292 House leadership referred H.R.6088 to the House Committee on House Administration.293 The SHIELD Act likely accommodates this bill’s central provision in its prohibition of “certain deceptive audio or visual media within 60 days of an election.”294 H.R.6088 concludes the list of House legislation associated with preserving the integrity of U.S. elections from the influence of foreign powers.295


290 Ibid., Actions.


293 Ibid., Actions.


4.3.2 Legislation Proposed in the U.S. Senate

In the U.S. Senate, attempts to deter foreign election influence remained similarly deadlocked. Legislators from both sides of the aisle collectively introduced at least ten bills that aimed to deter foreign interference in U.S. elections through a variety of approaches similar to proposals in the House, including: establishing the obligation to report foreign assistance to a campaign, hardening election infrastructure, requiring post-election audits and guaranteeing sanctions in response to foreign interference. However, despite these efforts, no legislation developed in the Senate on this topic made it through discussion in the House (despite successive reintroductions in some cases). As in the House, only the minority of Senate proposals directly acknowledged foreign social media influence campaigns, let alone laid out the steps necessary to deter this modern manipulation from occurring again.

S.1989 - Honest Ads Act

On October 19, 2017, Senator Amy Klobuchar proposed one of the first bills designed to prevent foreign nations from influencing U.S. public opinion through digital political advertising: S.1989, the “Honest Ads Act.” S.1989 sought to expand source disclosure requirements for political ads by defining paid targeted advertisements as “public communications” or “electioneering communications” and imposing additional disclosure requirements on those types of communications. It also aimed to require social media companies “to maintain publicly available records about qualified political advertisements that have been purchased on their platforms.” Senate leadership referred it to the Committee on Rules and Administration which referred it to the Judiciary Subcommittee on Crime and Terrorism which held several hearings before leaving the


297 Ibid.

298 Ibid.
legislation locked in committee.\textsuperscript{299} Senator Klobuchar reintroduced the bill to the 116th Congress in 2019 as S.1356 under the same name, but Republican senate leadership left it unaddressed.\textsuperscript{300,301}

\textit{S.2261 - Secure Elections Act}

Later in 2017, Republican Senator James Lankford of Oklahoma introduced the “Secure Elections Act” which charged the primary responsibility “for sharing information about election cybersecurity incidents, threats, and vulnerabilities with federal entities and election agencies” to the Department of Homeland Security.\textsuperscript{302} S.2261 also required DHS to establish an advisory panel to develop election cybersecurity guidelines, award grants for modernization to states, and establish a national bug bounty program to safely identify vulnerabilities in U.S. election infrastructure.\textsuperscript{303} S.2261 was referred to the Committee on Rules and Administration which held hearings to discuss its provisions, but these hearings yielded no additional progress.\textsuperscript{304}

\textit{S.482 - Defending American Security from Kremlin Aggression Act of 2019}

In February of 2019, Republican Senator Lindsey Graham of South Carolina proposed an expansive bill titled the “Defending American Security from Kremlin Aggression Act of 2019.”

\textsuperscript{299} Ibid., Actions.


\textsuperscript{301} Ibid., Actions.


\textsuperscript{303} Ibid.

\textsuperscript{304} Ibid., Actions.
Aggression Act of 2019.” S.482 included a raft of provisions from limiting U.S. withdrawal from the North Atlantic Treaty Organization (NATO) to establishing an Office of Cyberspace and the Digital Economy in the Department of State to oversee international cybersecurity and internet freedom issues to requiring the president to impose sanctions on Russians associated with interference into democratic processes. After referral to the Senate Committee on Foreign Relations, S.462 was debated and subsequently placed on the Senate legislative Calendar without further action.

S.825 - Protect our Elections Act

On March 14, 2019, Democratic Senator Chris Van Hollen of Maryland proposed the “Protect our Elections Act” which mandated that state and local governments ensure that each election service provider validates its ownership information and complies with cybersecurity best practices, while reinforcing these measures with mandatory annual audits. The Republican-controlled senate referred S.825 to the Committee on Rules and Administration where it has remained since.

S.949 - For the People Act of 2019

On March 28, 2019, Democratic Senator Mark Udall of New Mexico introduced the Senate companion bill to the House’s “For the People Act of 2019.” As expected, Senate

---


306 Ibid.

307 Ibid., Actions.


309 Ibid., Actions.

leadership rebuffed this expansive and politically charged legislation, sending it to the Senate Committee on Finance with no intention to raise it again.\textsuperscript{311}

\textit{S.1060 - Defending Elections from Threats by Establishing Redlines Act of 2019}

Two weeks later, a bipartisan group of 12 senators proposed the “Defending Elections from Threats by Establishing Redlines Act of 2019” which required the Office of the Director of National Intelligence to report on foreign interference in U.S. elections and force the president to automatically impose sanctions on the foreign nation that perpetrated that interference.\textsuperscript{312} This bill aimed to dissuade future Russian election influence efforts through the imposition of guaranteed consequences. These sanctions mandated full asset blocks, effectively requiring the Secretary of the Treasury to block all property associated with the offending nation within U.S. jurisdiction, and unlike most sanction bills, S.1060 did “not include any presidential-waiver provision.”\textsuperscript{313} While S.1060 enjoyed bipartisan sponsorship, support was not universal with several Republican senators critical of the bill’s timing and limits on presidential power.\textsuperscript{314} Accordingly, Senate leadership referred it to the Committee on Banking, Housing, and Urban Affairs which held related hearings, but did not proceed further.\textsuperscript{315}

\textit{S.1247 - Duty to Report Act}

\begin{itemize}
  \item \textsuperscript{311} Ibid., Actions.
  \item \textsuperscript{314} Ibid.
\end{itemize}
Later that month, Democratic Senator Richard Blumenthal of Connecticut introduced the “Duty to Report Act” which served as the companion bill to Representative Swalwell’s H.R.2424.\textsuperscript{316,317} Senate leadership referred to the Committee on Rules and Administration, which pursued no further action.\textsuperscript{318}

\textit{S.1328 - Defending Elections against Trolls from Enemy Regimes (DETER) Act}

On May 6, 2019, another bipartisan group of senators introduced the “Defending Elections against Trolls from Enemy Regimes (DETER) Act” which defined improper interference in U.S. elections to include interference in any candidate campaigns or ballot measures and barred foreign nationals accused of such improper interference from entering the country while also empowering the federal government to deport those accused of such interference and already in the U.S.\textsuperscript{319} As previously described, this bill passed the senate without amendment by Unanimous Consent, however, its companion bill in the House, H.R.3442 remained locked in committee after its initial introduction.\textsuperscript{320,321}

\textit{S.1540 - Election Security Act of 2019}

Ten days later, Senator Klobuchar proposed the “Election Security Act of 2019” which included many of the same election security provisions contained in H.R.1, H.R.2660,


\textsuperscript{320}Ibid., Actions.

and H.R.2722, requiring paper ballots, awarding election related grants, mandating election audits, and ordering the president to develop a national strategy to protect U.S. democratic institutions. S.1540 was referred to the Committee on Rules and Administration where it remained locked in committee. S.1562 - Foreign Influence Reporting in Elections Act

Later in May of 2019, Democratic Senator Mark Warner of Virginia introduced the “Foreign Influence Reporting in Elections Act” which--like many other bills--sought to “amend the Federal Election Campaign Act of 1971 to clarify the obligation [of campaigns] to report acts of foreign election influence.” Unsurprisingly, Senate Republicans referred S.1562 to the Committee on Rules and Administration where it stalled, however, Senator Warner attempted to revive it, reintroducing it again in July of 2019 as S.2242.

Democrats in the Senate made a last ditch effort to resurrect multiple stalled legislative proposals in late October of 2019 by calling for unanimous consent votes to immediately address the Senate versions of the previously passed House SHIELD Act (S.2669) and House SAFE Act (S.949) as well as S.1562: the “Foreign Influence Reporting in Elections Act” (all which had not been substantively discussed since they were referred to

---


323 Ibid., Actions.


committee).\textsuperscript{326,327,328} However, a single Republican senator’s objection halted any further consideration.\textsuperscript{329}


4.3.3 Source of This Legislative Quagmire

The root of this inaction is quite simple and very cliché: politics. Donald Trump’s political calculus is quite straightforward: publicly acknowledging that Russia conducted a multifaceted interference campaign to get Mr. Trump elected threatens the very legitimacy of his presidency. Much of the rest of the Republican party remains understandably reticent and hesitant to take a strong stand to prevent future influence; it pays political dividends to have the White House in Republican hands and any provocation of the president would be met in kind—not great for a politician’s career.

This hyper-partisan environment manifested in other politically unpalatable ways. President Trump’s repeated characterization of Special Counsel Mueller’s investigation as a “witch hunt” tainted every associated investigation and polarized the outcome before Mueller had even completed his report.330 Unending calls for President Trump’s impeachment by various House Democrats stoked this partisanship further.331 Recent reporting supports the belief that the Trump administration has used this hyper partisanship to color subsequent intelligence community analysis. President Trump’s public disdain for and mistrust in the nation’s intelligence experts reportedly led administration aides to the water down the language used in a National Intelligence Estimate (the most authoritative intelligence document, reflecting the IC’s consensus on national security matters) that examined Russia’s ongoing efforts to influence U.S. presidential elections in 2020 and even 2024.332

Ultimately, it is understandably difficult to be the candidate that Russia threw its weight behind, but repeatedly denying the well documented fact that Russia interfered to his benefit and threatening to veto any legislation that implicitly or explicitly acknowledges


this interference by attempting to prevent it from happening again is dereliction of the duties of the president.333

5 Policy Recommendations

Given the obvious detrimental effect of hyper partisanship over the last four years and the impending 2020 U.S. presidential race, my proposals are dependent on the outcome of that race. The impact that my suggested legislation can have directly depends on the willingness of both parties to work together and which party controls which chambers of congress. Democrats and Republicans have showed isolated bipartisanship in some legislative proposals including __ and S.1328, however, this willingness to work together has remained the exception, not the rule. Assuming this trend of general political antagonism holds through the 2020 presidential election and control of the House and Senate remains split down the party line, proposed legislation with any chance of success in both chambers must remain as apolitical and financially and logistically feasible as possible. If the presumptive Democratic nominee in the 2020 race, former Vice President Joe Biden, manages to take the White House and the Democratic party consolidates control of both the House and Senate, then proposed legislation can expand to include those policies with the greatest potential defense of American democracy's integrity. If the Republican party manages to maintain control of the Senate and flip the House—even if Biden is elected—then the current legislative graveyard will only grow.

5.1 With a Split Legislature

In keeping with the recommendation strategy above, the first bill 2020 House Democrats should address is S.1328, the Defending Elections against Trolls from Enemy Regimes (DETER) Act which passed the Senate with unanimous support after its reintroduction in early 2019. The DETER Act shows the most bipartisan support and promise at success in the House at this point, however, the president’s ongoing refusal to acknowledge Russian interference, let alone approve legislation to address it (thereby acknowledging it) makes this option exceedingly unlikely to move forward under the current administration. If Vice President Biden were to secure the presidency in November,
however, the DETER Act could have a serious shot at becoming law. The only remaining threat against its viability would be a large-scale reversal of Republican support in either chamber of Congress, but this revolt seems unlikely if President Trump is no longer in the White House.

If Congress finds success with the DETER Act, I would then encourage Democrats in the Senate to reintroduce H.R.2722, the Securing America’s Federal Elections (SAFE) Act of 2019 and H.R.4617, the Stopping Harmful Interference in Elections for a Lasting Democracy (SHIELD) Act of 2019. Again, without the threat of a presidential veto, these pieces of legislation already approved by the House during the 116th Congress have the potential to quickly progress through both chambers upon reintroduction, barring new resistance from Republican senators. Such resistance would also appear unlikely without Mr. Trump in the White House, and especially if Congress had already successfully passed the DETER Act and either the SAFE or SHIELD Acts.
5.2 With a United Congress

If the Democratic party unexpectedly took the White House, flipped the Senate, and maintained control of the House, then Democrats should go big on election security. Congressional Democratic leadership should either reintroduce and immediately pass S.1328, H.R.2722, and H.R.4617 or, more appropriately, combine these bills into a comprehensive election security package and introduce it as the first piece of legislation to the 117th Congress. This symbolic move would signal to the international community that the United States will not tolerate external influence in its most sacred domestic institution, and also reflect a tone of humility on the part of the new administration, should reports of Chinese and Iranian support for Vice President Biden be substantiated by the intelligence community and confirmed by independent researchers’ analysis of publicly available social media data.

Democrats should also include a provision in this new bill that mandates that social media companies either make all data associated with foreign influence campaigns by hosting a universally accessible database or provide all of that data to a similar, but government-sponsored repository. This increased transparency would inform a subsequent raft of legislation that could be specially tailored to the most current trends and tactics foreign nations employ to advance their attempted influence. Additionally, this bill should formalize reporting and information sharing mechanisms between social media (and other technology companies) and federal law enforcement. To facilitate this information sharing, the federal government should also grant appropriate security clearances to a select few of the employees at these companies charged with liaising with the federal government. This increased information flow and removal of security classification barriers would theoretically greatly increase the speed at which lawmakers receive word that an influence campaign has been discovered, potentially granting near-real time understanding of how foreign actors structure and expand their influence campaigns.
Finally, legislators should ensure that states have the funds necessary to implement these new election security standards and guarantee the allocation and distribution of future funding through the next several presidential election cycles. This guarantee of funding over time, while expensive and likely unpopular with several Republican fiscal responsibility champions, would help remove the hyper-partisanship previously associated with election security legislation, making increased security and standardized precautions the new normal. Making this funding a mundane function of the federal government would help restore default bipartisan support for ensuring the integrity of American democracy for years to come.
6 Conclusion and Call to Action

be too late for legislation to ensure the integrity of the upcoming 2020 presidential election, legislators have no excuse not to take action before 2024. After all:

“Protecting our democracies now [requires] setting the rules of fair play before voting day, not after.”

---

Bibliography


archive.today. n.d. @Crystal1Johnson. https://archive.is/p1EpK.


Dorsey, Jack. 2019. "We’ve made the decision to stop all political advertising on Twitter globally. We believe political message reach should be earned, not bought. Why? A few reasons ...." *Twitter.com.* October 30. https://twitter.com/jack/status/1189634360472829952.


