NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**FIGHTING BEARS AND TROLLS:
AN ANALYSIS OF SOCIAL MEDIA COMPANIES AND U.S. GOVERNMENT EFFORTS TO COMBAT RUSSIAN INFLUENCE CAMPAIGNS DURING THE 2020 U.S. ELECTIONS**

by

Elvis M. Chan

September 2021

Co-Advisors: Christopher Bellavita (contractor)
Erik J. Dahl

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
FIGHTING BEARS AND TROLLS: AN ANALYSIS OF SOCIAL MEDIA COMPANIES AND U.S. GOVERNMENT EFFORTS TO COMBAT RUSSIAN INFLUENCE CAMPAIGNS DURING THE 2020 U.S. ELECTIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Elvis M. Chan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense, the FBI, or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This thesis seeks to evaluate the effectiveness of the Russian disinformation campaigns targeting the 2020 U.S. elections and the efforts taken by the U.S. government and social media companies to thwart them. To develop countermeasures for Russian interference activities targeting future American elections, this thesis asks the question:

What impact did the countermeasures taken by the American social media companies and the U.S. government have on Russian social media influence campaigns targeting the 2020 U.S. elections?

This thesis uses a framework developed by Thomas Wilhelm, a U.S. Army researcher, to evaluate Russian hybrid warfare, based on the principles of Andrei Kartapolov, a prominent Russian general. Accordingly, it is used to measure the qualitative impact of the Russian measures and American countermeasures during the 2020 U.S. elections.

This thesis finds that the Russians shifted their tactics from 2016 to 2020. Still, the U.S. government and social media companies effectively impeded their influence campaigns primarily through information sharing and account takedowns, respectively. Because the Russians will continue their influence campaigns to undermine the United States, this thesis provides recommendations to include standardized information sharing and the establishment of a national coordination center.

14. SUBJECT TERMS
propaganda, social media, information operations, information warfare, active measures, foreign influence, influence operations, democracy, social discourse, hybrid warfare, bots, trolls, cyber, psychological operations, Soviet Union, Russia, social media, Facebook, Twitter, Instagram, Google, YouTube, big data, data analytics, micro-targeting, 2020 presidential election

15. NUMBER OF PAGES
149

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

FIGHTING BEARS AND TROLLS: AN ANALYSIS OF SOCIAL MEDIA COMPANIES AND U.S. GOVERNMENT EFFORTS TO COMBAT RUSSIAN INFLUENCE CAMPAIGNS DURING THE 2020 U.S. ELECTIONS

Elvis M. Chan
Assistant Special Agent in Charge, Federal Bureau of Investigation
B.S. Che E., University of Washington, 1993
BS, University of Washington, 1993

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2021**

Approved by: Christopher Bellavita
Co-Advisor

Erik J. Dahl
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis seeks to evaluate the effectiveness of the Russian disinformation campaigns targeting the 2020 U.S. elections and the efforts taken by the U.S. government and social media companies to thwart them. To develop countermeasures for Russian interference activities targeting future American elections, this thesis asks the question: What impact did the countermeasures taken by the American social media companies and the U.S. government have on Russian social media influence campaigns targeting the 2020 U.S. elections?

This thesis uses a framework developed by Thomas Wilhelm, a U.S. Army researcher, to evaluate Russian hybrid warfare, based on the principles of Andrei Kartapolov, a prominent Russian general. Accordingly, it is used to measure the qualitative impact of the Russian measures and American countermeasures during the 2020 U.S. elections.

This thesis finds that the Russians shifted their tactics from 2016 to 2020. Still, the U.S. government and social media companies effectively impeded their influence campaigns primarily through information sharing and account takedowns, respectively. Because the Russians will continue their influence campaigns to undermine the United States, this thesis provides recommendations to include standardized information sharing and the establishment of a national coordination center.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DNC	Democratic National Committee
EBLA	Eliminating Barriers for the Liberation of Africa
FARA	Foreign Agent Registration Act
FSB	Federal Security Service
FS-ISAC	Financial Sector ISAC
GANS	generative adversarial networks
GEC	Global Engagement Center
GRU	Main Directorate of the General Staff of the Russian Armed Forces
HPSCI	U.S. House Permanent Select Committee on Intelligence
ICA	Intelligence Community Assessment
IRA	Internet Research Agency
ISAC	Information Sharing and Analysis
JAR	joint analysis report
NAEBC	Newsroom for American and European Based Citizens
NCSC	National Counterintelligence and Security Center
NDAA	National Defense Authorization Act
ODNI	Office of the Director of National Intelligence
SSCI	U.S. Senate Select Committee on Intelligence

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis uses a systematic framework to evaluate the qualitative effectiveness of the Russian disinformation campaigns and the countermeasures taken by the U.S. government and social media companies to combat the aforementioned campaigns targeting the 2020 U.S. elections. To develop effective countermeasures for Russian interference activities targeting future American elections, this thesis seeks to answer the following question: What impact did the measures taken by the American social media companies and the U.S. government have on Russian social media influence campaigns targeting the 2020 U.S. elections?

Russian operatives working under the auspices of a St. Petersburg-based organization, known as the Internet Research Agency (IRA), created a significant degree of the toxicity on social media during the 2016 U.S. elections.[1] The online social media influence campaign perpetrated by the Internet Research Agency aimed to fan the flames of existing divisive rhetoric, drive a wedge between the many demographic groups in America, and erode confidence in democracy.[2] Russia remains a committed adversary with influence operations continuing to this very day, posing an active threat to American democracy.[3]

Since the end of 2016, federal agencies and private sector organizations, specifically the major American social media companies, have been actively helping to safeguard political campaigns and election infrastructure from computer intrusions through increased cybersecurity and other security measures. To date, most research has focused on quantitative and qualitative analyses of the IRA's influence campaigns. However, this research has not analyzed how the Russian government perceived the effectiveness of its

[1] Robert Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: Department of Justice, 2019), 4, https://www.hsdl.org/?view&did=824221.

[2] Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency* (New York: New Knowledge, 2018), 4.

[3] Miles Parks and Philip Ewing, "Foreign Interference Persists And Techniques Are Evolving, Big Tech Tells Hill," National Public Radio, June 18, 2020, https://www.npr.org/2020/06/18/880349422/foreign-interference-persists-and-techniques-are-evolving-big-tech-tells-hill.

campaigns. Furthermore, the efficacy of the U.S governmental and private sector actions to defend against the IRA's influence campaigns has not been systematically analyzed.

The objectives of this thesis are three-fold: (1) examining the Internet Research Agency and other Russian social media campaigns ahead of the 2020 U.S. elections to determine whether its tactics have shifted since 2016; (2) critically analyzing the private sector and U.S. government's actions to counter the Russian influence activities; and (3) proposing recommendations to safeguard future U.S. elections. The first two objectives are assessed using an analytical framework proposed by Thomas Wilhelm, Director of the U.S. Army's Foreign Military Studies Office. The results of the first two objectives, inform the last objective as well as a review of current literature by scholars and subject matter experts in different fields.

To design a helpful framework for analyzing Russian influence operations, Thomas Wilhelm surveyed the published works and speeches of General Lieutenant Andrei V. Kartapolov. Wilhelm surmised Kartapolov was one of the key architects of current Russian military science and doctrine.[4] Wilhelm believed the framework provided a well-rounded understanding of Russian martial intent and objectives about hybrid warfare from a Russian perspective.[5] Specifically, Kartapolov advocates using asymmetric, non-violent methods to undermine the strengths of Russia's opponents to achieve their strategic goals.[6]

The relevant components of the Kartapolov Framework for analyzing Russian social media-based influence operations against the United States are: (1) spreading discontent in the population; (2) exerting political pressure; and (3) confusing the political leadership.[7] This thesis uses the Kartapolov framework to conduct a qualitative evaluation of the Internet Research Agency's impact and the effectiveness of social media companies and the U.S. government's countermeasures. Specifically, it analyzes American actions to

---

[4] Tom Wilhelm, "A Russian Military Framework for Understanding Influence in the Competition Period," *Military Review* (2020): 35.

[5] Wilhelm, 38.

[6] Rod Thornton, "The Russian Military's New 'Main Emphasis,'" *RUSI Journal* 162, no. 4 (2017): 18–28, https://doi.org/10.1080/03071847.2017.1381401.

[7] A. V. Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," *Journal of the Academy of Military Science* 51, no. 2 (2015): 36.

determine their effectiveness for countering the three influence-related components of the Kartapolov Framework.

Three main themes emerged from the 2020 U.S elections. First, the Russians continued their efforts to target the U.S. elections but shifted tactics to avoid detection. Second, the social media companies, along with news media and research organizations, successfully identified and disrupted the evolving Russian disinformation campaigns. Third, the U.S. government acted more forcefully in securing the elections, primarily through its information sharing with the social media companies, political organizations, and the American public.

Despite the best efforts of the Russians, social media companies, news media, and research organizations detected, exposed, and disrupted the activities of the Internet Research Agency and other Russian-affiliated online groups. Although America's private sector may have been caught unaware during the 2016 elections, it was on heightened alert ahead of 2020, with the noteworthy efforts of American news outlets and non-governmental organizations exposing Russian disinformation activities and paving the way for the social media companies to shut down their social media accounts.

The U.S. government's response to the Russian influence campaign appeared more robust before the 2020 elections than in the 2016 or 2018 elections. The most important actions taken by the U.S. government may have been the information sharing with the social media companies to expose Russia's different operations and shut down its accounts. In addition, the U.S. government's information-sharing may have helped the social media companies secure their platforms by identifying malign Russian influence activities. The U.S. government's other responses, such as economic sanctions and indictments, provided the American public with factual narratives of the crimes perpetrated by the Russian Federation.

It took the collaborative efforts of the private sector, in the form of social media companies, researcher organizations, and news media, and the public sector, in the form of the executive and legislative branches of the U.S. government, to turn back the Putin-

sanctioned disinformation operations which were targeting the 2020 U.S. elections.[8] Ultimately, the American actions appeared effective in mitigating the Russian online tactics because voters were undeterred and turned out in record numbers for the election.

The 2021 Intelligence Community's annual threat assessment named Russia as one of "the most serious intelligence threats to the United States" and warned that the Russian government would continue its efforts to propagate dissension in the American populace.[9] Based on the evaluation of the Russian actions and the effectiveness of the American responses in the 2020 U.S. elections, this thesis makes recommendations for protecting future elections that have been drawn from experts in the U.S. government, non-governmental organizations, and academic institutions. The three types of possible actions are broadly categorized as security, transparency, and resiliency measures.[10] The proposed security measures include enhanced cybersecurity, enhanced disinformation detection, economic sanctions, information sharing, and the establishment of a fusion center. The transparency measures proposed include a public communications strategy, content labeling standards, updated political advertising and campaign finance laws, and transparent reporting. The resiliency measures suggested include improved media literacy

---

[8] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution (*Washington, DC: Office of the Director of National Intelligence, 2017), 7, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[9] Office of the Director of National Intelligence, *2021 Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2021), 11, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2204-2021-annual-threat-assessment-of-the-u-s-intelligence-community.

[10] Gabriel Cederberg et al., *National Counter-Information Operations Strategy* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019), https://www.belfercenter.org/publication/national-counter-information-operations-strategy; Renée DiResta and Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019* (Palo Alto, CA: Stanford University, 2019), https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks; Angus King and Mike Gallagher, *Cybersecurity Lessons from the Pandemic*, CSC White Paper #1 (Washington, DC: U.S. Cyberspace Solarium Commission, 2020), https://www.solarium.gov/public-communications/pandemic-white-paper; *Report on Russian Active Measures* (Washington, DC: U.S. Congress. House, 2018), https://republicans-intelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf; *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts against Election Infrastructure with Additional Views*, Senate, 116th Cong., 1st Sess. (Washington, DC: U.S. Congress. Senate, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

and critical thinking for the American public.[11] Hopefully, incorporating the proposed measures with existing ones will help repair and strengthen the framework of American democracy for the 21st century.

[11] Michael McFaul, ed., *Securing American Elections* (Palo Alto, CA: Stanford University, Cyber Policy Center, 2019), 8, https://www.hsdl.org/?view&did=827251.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

As I write these acknowledgments, I feel a sense of relief for finishing the program, and sadness for it coming to an end. I am most grateful for all of the people who made this accomplishment possible. My primary reasons for participating in this master's program were to intellectually challenge myself and add academic rigor to all the on-the-job training I have received working on national security matters at the FBI. Both objectives were accomplished handily, thanks to the outstanding instructors and staff at the Naval Postgraduate School.

What I did not account for was undertaking this feat during a once-in-a-lifetime pandemic. While the pandemic has been an unmitigated disaster for the world, it has been a mixed blessing for me. On the one hand, I wonder how much more I would have learned from the instructors and cohort members if we were in person. Experience has taught me that some of the most valuable discussions happen between classes or during sidebar conversations. On the other hand, I have not had to travel for work since the start of the pandemic, which has allowed me to focus on my studies after work and on the weekends. I recognize these are first-world privileges and am thankful.

I was pleasantly surprised by how close I became with my cohort members though I had never met any of them physically. I am very thankful for a few of our colleagues who have helped me along this academic journey. They include Cassie, our president who has been guiding us along like a gaggle of unruly geese; the California contingent of Rich, Ben, and Heather, who have been my supportive teammates on many group projects; Rob, who is the congenial host of Not Quite the Trident Room and a steadying influence on me; Katie, who constantly challenges me and created the infamous Riesner Theory; Ron, who is my younger and intractable ideological twin; and Emily, whose youth belies her insight. To Cohort 2001/2002, I say to you, *satis esse fortis stultum*.

To the Naval Postgraduate School faculty and staff, I am filled with gratitude and thank you for your efforts during this difficult time. I can honestly say that every class challenged me, with some making me feel mentally stretched in ways I did not think were

possible. First and foremost, I want to give a hearty thank you to my thesis team. Dr. Erik Dahl's acumen and discernment have focused my writing and made my thesis better. I consider you a kindred spirit in the practice of intelligence analysis and homeland security. Dr. Chris Bellavita's steadfast faith in me and support of my thesis topic has been the wind at my back. I appreciate your advocacy and use of the Socratic method to strengthen my thinking. Marianne Taflinger had the unenviable task of being my writing coach and taking the first crack at shaping my drafts so that they would be presentable to my advisors. Thank you for your patience and constructive feedback. Other instructors who have made a lasting impression on me include Branders, who rolled into class looking like a couple of Hell's Angels but spurred some of the most profound conversations I have ever had, and Paul Smith, who is the old friend in the security business that I just met this year.

To my sisters and brothers at the Federal Bureau of Investigation, I am proud to stand next to you and represent our storied organization. I appreciate the support of my superiors in allowing me to participate in this program, our supervisors who have minded the office when I am away from work, and my colleagues back at headquarters who were in the trenches with me as we worked to protect the 2020 elections. Your fidelity, bravery, and integrity motivate me to continue striving to improve myself.

To my colleagues in the private sector, I am glad that we find common cause with protecting the elections from malign foreign influence and other online threats. I have learned a great deal from you and appreciate your continued efforts to safeguard your platforms. Hopefully, we will get to see each other in person soon.

To my family, I appreciate all of your unflinching support and hope my efforts have made the world a better place in some small way. To my mother and father, thank you for instilling me with my drive for academic excellence and work ethic. To the Ochikubo and Furuya families, thank you for supporting my family and me with all of your time and energy when I decided to make a drastic midlife career change. To both of my daughters, my heart bursts with pride as I watch you grow into independent, fierce, and outspoken women who will positively impact this world in ways I have not imagined. Most importantly, I want to give the deepest thanks to my wife for all of her love, unwavering support, patience, and grace. Without her, none of my accomplishments are possible.

I. RUSSIA RISES FROM THE ASHES OF THE COLD WAR

> Over the course of my career, I've seen a number of challenges to our democracy. The Russian government's effort to interfere in our election is among the most serious.
>
> —Robert S. Mueller III, July 24, 2019

This statement from the well-respected former FBI Director underscored the severity of the Russian actions to interfere with the 2016 U.S. elections. After the end of the Cold War and the fall of the Soviet Union in 1991, Russia appeared to have faded from America's collective memory as an adversary.[1] This attitude abruptly changed on June 14, 2016, when a U.S.-based cybersecurity firm named Crowdstrike announced it had investigated intrusions into the computer networks of the Democratic National Committee (DNC) by two Russian hacking groups, code-named "Fancy Bear" and "Cozy Bear."[2] Away from the news media scrutiny, Russian operatives working under the auspices of a St. Petersburg-based organization, known as the Internet Research Agency (IRA), created a significant portion of the toxicity on social media during the presidential campaign season.[3] The "sweeping and sustained" online social media influence campaign perpetrated by the Internet Research Agency aimed to fan the flames of existing divisive rhetoric, drive a wedge between the many demographic groups in America, and erode

---

[1] Jon Wiener, *How We Forgot the Cold War: A Historical Journey Across America* (Berkeley: University of California Press, 2012), 1, https://books.google.com/books?hl=en&lr=&id=w_Sa-F8DXhgC&oi=fnd&pg=PA1&dq=american+memory+of+the+cold+war&ots=kvRphYu1TG&sig=sVpOOZBAdl0fqcHCskio5uy7tiE#v=onepage&q=american%20memory%20of%20the%20cold%20war&f=false.

[2] Dmitri Alperovitch, "Our Work with the DNC: Setting the Record Straight," *Crowdstrike Blog* (blog), June 5, 2020, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[3] Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 4.

confidence in democracy.[4] Russia remains a committed adversary as its influence operations continue to this very day, posing an active threat to American democracy.[5]

A. PROBLEM STATEMENT

While "hack and dump" campaigns, such as the 2016 DNC attack and cyberattacks against election infrastructure, are broadly considered Russia influence operations, the Internet Research Agency's social media influence campaign directly targeted voter confidence in election integrity aimed to harm democracy.[6] As Philip Howard, an Oxford researcher, contends, a healthy democracy relies on trustworthy news media and a climate that allows for civil discourse and consensus-building.[7] The IRA's continued onslaught of fake news and amplification of inflammatory content sowed discord and confusion in the United States. For example, Hillary Clinton received damaging publicity during the campaign season in 2016 when the Main Directorate of the General Staff of the Russian Armed Forces (GRU) and Wikileaks continually leaked stolen content from the Democratic National Committee; the IRA magnified the negative image of her through its dissemination of memes and other negative content on social media platforms, which in turn politically damaged her heading into Election Day, and may have delegitimized her presidency had she been elected.[8] Russia understood that attacks against the elections

---

[4] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 4.

[5] Parks and Ewing, "Foreign Interference Persists And Techniques Are Evolving, Big Tech Tells Hill."

[6] Sarah Birch, "Perceptions of Electoral Fairness and Voter Turnout," *Comparative Political Studies* 43, no. 12 (December 1, 2010): 1601–22, https://doi.org/10.1177/0010414010374021; Kellie J. Weir, "Safeguarding Democracy: Increasing Election Integrity through Enhanced Voter Verification" (master's thesis, Naval Postgraduate School, 2018), https://www.hsdl.org/?view&did=811383.

[7] Philip N. Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018* (Oxford, UK: University of Oxford, Computational Propaganda Research Project, 2019), 39, https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs.

[8] Allon J. Uhlmann and Stephen McCombie, "The Russian Gambit and the U.S. Intelligence Community: Russia's Use of Kompromat and Implausible Deniability to Optimize Its 2016 Information Campaign against the U.S. Presidential Election," *Library Trends* 68, no. 4 (2020): 684, https://doi.org/10.1353/lib.2020.0017.

struck at the heart of American democracy because this process expresses the people's will and gives the U.S. government legitimacy.[9]

Since the end of 2016, federal agencies and private sector organizations, specifically the major American social media companies, have been actively helping to safeguard political campaigns and election infrastructure from computer intrusions through increased cybersecurity and other security measures.[10] To date, most research has focused on quantitative and qualitative analyses of the IRA's influence campaigns. However, this research has not analyzed how the Russian government itself perceived the effectiveness of the campaigns in achieving their goals. Furthermore, the efficacy of the aforementioned governmental and private sector actions to defend against the IRA's influence campaigns has not been studied much in a methodical fashion. This thesis seeks to use a systematic framework to evaluate the qualitative effectiveness of the Russian disinformation campaigns and the countermeasures taken by the U.S. government and social media companies to combat the aforementioned campaigns targeting the 2020 U.S. elections. In summation, Russian influence operations' continual assault will weaken American democracy over the long term if not effectively countered.

B. RESEARCH QUESTION

To develop effective countermeasures for Russian interference activities targeting future American elections, this thesis seeks to answer the following question: What impact did the countermeasures taken by the American social media companies and the U.S. government have on Russian social media influence campaigns targeting the 2020 U.S. elections?

---

[9] Gregory A. Miller et al., *Critical Democracy Infrastructure: Protecting American Elections in the Digital Age Threats, Vulnerabilities, and Countermeasures as a National Security Agenda*, 2nd ed. (Palo Alto, CA: OSET Institute, 2020), 9, https://trustthevote.org/wp-content/uploads/2020/05/01May20_CDI-2nd.pdf.

[10] Federal Bureau of Investigation, "Protected Voices," Federal Bureau of Investigation, accessed August 5, 2020, https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices; Facebook, "Facebook - Preventing Election Interference," About Facebook, 2020, https://about.fb.com/actions/preventing-election-interference/; Google Threat Analysis Group, "Google Safety & Security," *Google* (blog), accessed May 27, 2020, https://blog.google/technology/safety-security/; Twitter, "Elections Integrity: We're Focused on Serving the Public Conversation," About Twitter, 2020, https://about.twitter.com/en_us/advocacy/elections-integrity.html.

C. LITERATURE REVIEW

This literature review analyzes the leading scholarly and expert debates on the Internet Research Agency and other Russia-backed social media activities targeting the U.S. elections from 2014 to 2020, the countermeasures taken by American social media companies and the U.S. government, a framework for understanding the objectives of Russian hybrid warfare, and the recommendations to counter Russian influence activities provided by subject matter experts in a variety of fields. Russian influence campaigns, known as "active measures," have been in existence since the inception of the Soviet Union over 100 years ago.[11] Prior research in this topic drew primarily from the ranks of history, political science, public policy, and international studies. An extensive survey of the current academic literature indicates that the types of researchers drawn to the field of foreign influence campaigns have recently broadened due to the Internet Research Agency's success in employing social media platforms to conduct influence campaigns targeting the 2016 U.S. elections. Presently, scholarly analyses also come from researchers in the fields of computer science, data analytics, and communications. This thesis attempts to evaluate the efficacy of the aforementioned actions to determine if finetuning or a wholesale change in tactics is required to counteract future Russian influence campaigns.

The literature review will be comprised of four parts. The first part examines the studies of Russian online influence campaigns from 2014 to 2020. The sources for this topic include reports and papers by the U.S. government, think tanks, private research firms, academic researchers, and news media. The second part examines the documents which analyze or disclose countermeasures taken by the American social media companies, specifically Facebook, Google, and Twitter, and the U.S. government. The sources include government reports and statements, academic research papers, private research firm reports, think tanks papers, the social media companies' transparency reports, and news media reporting. The third part examines a framework for understanding the objectives of Russian hybrid warfare. The sources primarily include articles and research papers from academic and military institutions. The fourth part examines recommendations for

[11] *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel I: Hearing before the Select Committee on Intelligence*, Senate, 115th Cong., 1st sess., March 20, 2017, 10.

countering future Russian online influence campaigns. The sources for this topic include Congressional reports, think tank papers, academic research papers, and private research companies' reports. The literature review has revealed an abundance of source materials covering the activities surrounding the 2016 and 2018 U.S. elections. At the time of this thesis, there have not been many scholarly works published examining Russia's interference against the 2020 U.S. elections.

1. Russian Online Influence Activities from 2014 to 2020

Groups of investigators and scholars provide a critical review and analysis of Russian online influence activities and tactics vis-à-vis the 2016 U.S. election. The U.S. Intelligence Community Assessment (ICA) issued in January 2017 encapsulated the Executive Branch of the U.S. government's consensus judgment that the Russian Federation endeavored to erode public confidence in the U.S. elections and favor one presidential candidate over another.[12] Since that ICA was published, an abundance of literature into the IRA's 2016 to 2020 activities has been written by governmental entities, non-governmental organizations, and academic researchers.

Both the U.S. government's executive and legislative branches conducted investigations into the Russian interference in the 2016 U.S. elections, which included the IRA's social media campaigns. The foundational work detailing the IRA's actions during this timeframe may be the 2019 report from Robert Mueller III, the former FBI Director appointed by the Department of Justice as the Special Counsel to investigate Russian interference in the 2016 U.S. elections.[13] This report resulted from approximately two years of work by the Special Counsel's Office and the analysis of a multitude of evidence collected through legal processes and interviews.[14] Mueller and his team had two main findings regarding the Russian influence campaign. First, the report found that the IRA's

---

[12] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution* (Washington, DC: Office of the Director of National Intelligence, 2017), 7, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[13] Robert Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: Department of Justice, 2019).

[14] Department of Justice, "Special Counsel's Office," Department of Justice Special Counsel's Office, October 16, 2017, https://www.justice.gov/sco.

social media campaign aimed to sow discord in the U.S. elections but pivoted to favoring Donald Trump when it became apparent he would be the Republican presidential nominee.[15] Second, Mueller's team concluded that the hack and dump attack against the DNC was intended to harm Hillary Clinton's presidential campaign.[16]

The intelligence committees for both houses of Congress also issued reports regarding Russian interference in the 2016 U.S. elections. Of the two, the U.S. Senate Select Committee on Intelligence (SSCI) report had bipartisan approval from the committee members when it was published. Its findings coincided with the Special Counsel's report.[17] The U.S. House Permanent Select Committee on Intelligence (HPSCI) report was issued by the Republican majority over the Democratic committee members' dissent. The HPSCI majority and minority reports concluded that the Russians had interfered with the elections through the cyberattack against the DNC and the IRA's social media campaigns.[18] The majority report neglected to mention that these two operations were intended to damage the Clinton campaign and favor the Trump campaign, whereas the minority report highlighted the majority's omission and suggested partisan politics explained the omission.[19]

In August 2020, the State Department's Global Engagement Center published a report, which exposed Russia's current disinformation strategy and tactics.[20] Though the report did not address the Russian activities targeting the 2016 U.S. elections, it described

---

15 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 4.

16 Mueller, 4.

17 *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures, Campaigns, and Interference In the 2016 U.S. Election, Volume 2: Russia's Use Of Social Media With Additional Views*, Senate, 116th Cong., 1st Sess. (Washington, DC: U.S. Congress. Senate, 2019), 4, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

18 *Report on Russian Active Measures*, 98.

19 *Report of the House Permanent Select Committee on Intelligence on Russian Active Measures Together with Minority Views*, H.Rept 115–1110 (Washington, DC: Government Publishing Office, 2019), 257, https://www.congress.gov/115/crpt/hrpt1110/CRPT-115hrpt1110.pdf.

20 Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem* (Washington, DC: Department of State, 2020), https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

Russian online influence operations, the online ecosystem that Russia was aiming to cultivate, and framed the IRA's current activities as a continuation of the Russian active measures strategy.[21] The State Department and Special Counsel's Office reports, coupled with the Congressional intelligence committee reports, represented the U.S. government's understanding of Russian disinformation strategy in general and the IRA's role within the broader Russian influence enterprise.

In March 2021, the Office of the Director of National Intelligence (ODNI) issued an unclassified version of the intelligence community assessment summarizing foreign state-sponsored threats to the 2020 U.S. elections.[22] In particular, the ODNI's report provided a succinct but comprehensive overview of the Russian influence campaign, which focused on damaging the Biden presidential campaign and favoring the Trump campaign.[23] In April 2021, the ODNI issued an unclassified version of the Intelligence Community's annual worldwide threat assessment, highlighting Russian influence operations as a persistent threat to the United States.[24] Reporting from the ODNI represents the collective efforts of all 18 organizations which comprise the U.S. Intelligence Community.[25]

Another corpus of literature written by non-governmental and academic researchers tended to be more quantitively detailed in its findings of the IRA than governmental counterparts as they delved into statistical analyses of social media activities. Researchers from the New Knowledge private research firm, now known as Yonder, conducted a comprehensive analysis of the IRA's activities in 2016 and authored a report at the request

---

21 Global Engagement Center.

22 Office of the Director of National Intelligence, "Intelligence Community Assessment on Foreign Threats to the 2020 U.S. Federal Elections," Intelligence Community Assessment (Washington, DC, March 16, 2021), https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2192-intelligence-community-assessment-on-foreign-threats-to-the-2020-u-s-federal-elections.

23 Office of the Director of National Intelligence, 2–5.

24 Office of the Director of National Intelligence, *2021 Annual Threat Assessment of the U.S. Intelligence Community*, 11.

25 Office of the Director of National Intelligence, "Members of the IC," Office of the Director of National Intelligence, accessed April 27, 2021, https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

of the Senate Select Committee on Intelligence.[26] Renee DiResta and her colleagues conducted a highly detailed qualitative and quantitative analysis of all the social media data submitted to SSCI by Facebook, Google, and Twitter. The data encompassed the IRA's activities from about 2015 to 2018. Their findings regarding the intent of the IRA's social media campaign and the cyberattack against the DNC aligned with the Special Counsel's and SSCI's reports.[27] DiResta et al. go beyond the government reports' findings and conclude that the Russians actively attempted to suppress voter turnout, especially among black voters, and foment insurrectionist sentiment against different levels of American government.[28]

Philip Howard, a University of Oxford researcher, also had the opportunity to analyze the aforementioned social media data provided to SSCI. Howard and his colleagues conducted a statistical analysis of the social media data, to include an in-depth examination of the IRA's strategy and tactics.[29] Howard, who along with Samuel Woolley, had previously coined the phrase "computational propaganda" to describe the IRA's cyber covert operation activities, also found that the IRA's social media campaign was designed to interfere in the 2016 U.S. elections, specifically favoring Trump over Clinton.[30] Their report went further than prior research by describing the specific targeting of different demographic groups to elicit particular responses; i.e., promoting right-wing turnout for Trump, discouraging black voters from voting or civic engagement, and amplifying the differences between the ideologically progressive and conservative.[31]

---

[26] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*.

[27] DiResta et al., 4.

[28] DiResta et al., 8.

[29] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*.

[30] Samuel C. Woolley and Philip N. Howard, "Political Communication, Computational Propaganda, and Autonomous Agents," *National Science Foundation Public Access Repository*, September 3, 2016, 6; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3; Woolley and Howard, "Political Communication, Computational Propaganda, and Autonomous Agents," 3.

[31] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 18.

More recently, Robert Walker examined the IRA's online activities in his 2019 master's thesis at the Naval Postgraduate School.[32] His work's primary focus was to evaluate the purpose and impact of the IRA's social media content, coming to the same conclusions as his predecessors.[33] Unlike the previously mentioned researchers, Walker also examined the countermeasures taken by private sector companies and the U.S. government from 2016 to 2018 to assess their impact and found them to be partially effective.[34] These researchers did not have the same political considerations or constraints as governmental investigators to examine and make qualitative judgments about the intent of the IRA's activities and motivations.

Despite a broad agreement within the United States that the Russians attempted to interfere in the 2016 U.S. elections, some conservative American media have disputed the impact these efforts had on the election outcome. In a *New York Magazine* article, Margaret Hartmann, senior editor, stated, "the general consensus is that liberals are overstating the significance of Russia's alleged meddling in an effort to shift the blame for their loss from Hillary Clinton, and undermine Trump's presidency."[35] A 2018 poll taken by British marketing research firm YouGov found that only 37% of Republicans believed Russia interfered with the 2016 U.S. elections.[36] This researcher's extensive literature search could not find any scholars, private research organizations, or prominent conservative think tanks who had authored papers discussing the Russian interference in the 2016 U.S. elections, the Internet Research Agency's social media activities, or policy recommendations for countermeasures. The negative results of this query suggest that this topic did not rate as relevant to these organizations.

---

[32] Robert E. Walker, "Combating Strategic Weapons of Influence on Social Media" (master's thesis, Naval Postgraduate School, 2019), http://hdl.handle.net/10945/62826.

[33] Walker, 69–79.

[34] Walker, 89–100.

[35] Margaret Hartmann, "How Conservatives View Russia's Alleged Meddling in the U.S. Election," *New York Magazine*, December 16, 2016, https://nymag.com/intelligencer/2016/12/how-the-right-is-talking-about-russias-election-meddling.html.

[36] Kathy Frankovic, "Republicans Still Not Convinced of Russian Election Meddling," YouGov, August 10, 2018, https://today.yougov.com/topics/politics/articles-reports/2018/08/10/republicans-still-not-convinced-russian-election-m.

2. Countermeasures by the Private Sector and the U.S. Government

The Internet Research Agency appeared to conduct their influence activities undetected on the major social media platforms, specifically those belonging to Facebook, Google, and Twitter, before and during the 2016 U.S. elections.[37] Thus, the social media companies did not pursue any policy changes or take any actions to thwart the influence campaign. In October 2016, the Department of Homeland Security (DHS) and Office of the Director of National Intelligence publicly blamed the Russian Federation for hacking the Democratic National Committee.[38] Subsequently, the FBI and ODNI issued a joint analysis report (JAR), providing more details to the previously published joint statement.[39] The JAR attributed the 2016 DNC hack to two Russian hacking groups, known as APT28 and APT29, and provided technical details to allow organizations to safeguard themselves from these types of computer intrusions.[40] Typically, the U.S. government does not publicly disclose foreign actors' tradecraft because it can reveal sensitive sources and methods used to acquire this information. Likely, the significance of the DNC hack and public pressure prompted the U.S. government to supplement its initial October 2016 statement.[41]

During the time frame after the 2018 U.S. elections and before the 2020 U.S. elections, private research firms and academic research centers played a more prominent role as the social media companies decided to partner with them. These research

---

[37] Cecilia Kang, Nicholas Fandos, and Mike Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill," *New York Times*, October 31, 2017, https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html.

[38] Department of Homeland Security and Office of the Director of National Intelligence, *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security* (Washington, DC: Department of Homeland Security and Office of the Director of National Intelligence, 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[39] Department of Homeland Security and Federal Bureau of Investigation, *GRIZZLY STEPPE – Russian Malicious Cyber Activity* (Washington, DC: Department of Homeland Security and Federal Bureau of Investigation, 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

[40] Department of Homeland Security and Federal Bureau of Investigation, 5–10.

[41] Chris Strohm, "Russian Hacking Began as 'Grizzly Steppe,'" *Chicago Tribune*, December 30, 2016, sec. Nation & World, https://www.chicagotribune.com/nation-world/ct-russian-hack-grizzly-steppe-20161230-story.html.

organizations were pivotal in identifying the Internet Research Agency's activities and its various influence campaigns. The two noteworthy organizations were Graphika and the Stanford Internet Observatory. In 2020, Graphika issued a series of reports that exposed Russian influence operations' activities across different platforms. The organization coordinated with the social media companies that shut down IRA-controlled accounts. It discovered that the IRA had made fake left-wing and right-wing news sites to amplify the existing discourse on hot-button topics, such as governmental corruption, gun control, and racial discrimination.[42] The Graphika researchers concluded that the IRA made these sites to help them target people through their ideologies, similar to their tactics in 2016.[43] The Stanford Internet Observatory was led by Alex Stamos, formerly Facebook's Chief Security Officer, and Renee DiResta, one of the researchers retained by SSCI to investigate Russian interference in 2016. The Stanford Observatory collaborated with the social media companies to identify Russian influence campaigns, which the companies would subsequently disrupt through account takedowns and content removal.[44] The Stanford researchers identified influence operations conducted by the GRU and IRA in Africa, which mostly followed prior Russian influence campaign tactics.[45] These two instances showed the social media companies partnering with different research organizations to identify and disrupt various foreign influence campaigns, likely to avoid duplicating efforts and spread the workload.

---

[42] Ben Nimmo et al., "IRA Again: Unlucky Thirteen" (New York, NY: Graphika, September 2020), https://public-assets.graphika.com/reports/graphika_report_ira_again_unlucky_thirteen.pdf; Jack Stubbs, "Exclusive: Russian Operation Masqueraded as Right-Wing News Site to Target U.S. Voters - Sources," Reuters, October 1, 2020, https://www.reuters.com/article/usa-election-russia-disinformation-idUSKBN26M5OP.

[43] Nimmo et al., "IRA Again: Unlucky Thirteen," 24; Stubbs, "Exclusive."

[44] DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*; Stanford Internet Observatory, "Analysis of June 2020 Twitter Takedowns Linked to China, Russia, and Turkey," *Stanford Internet Observatory* (blog), June 11, 2020, https://cyber.fsi.stanford.edu/io/news/june-2020-twitter-takedown.

[45] DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*; Shelby Grossman, Daniel Bush, and Renée DiResta, "Evidence of Russia-Linked Influence Operations in Africa," *Stanford Internet Observatory* (blog), October 30, 2019, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf.

3. Framework for Understanding Russian Hybrid Warfare

The concept of Russian hybrid warfare was devised by Western experts around 2014 to describe Russia's use of conventional military force and unconventional means, specifically cyberattacks and information operations, in its incursions into Crimea, Eastern Ukraine, and Syria.[46] A review of current literature determined that the Russian military officers who are believed to have contributed the most to the Russian hybrid warfare concept were General Valery Gerasimov, Chief of the Russian Federation's General Staff, Lieutenant General S. A. Bogdanov, a retired General Staff officer, and Lieutenant General Andrei V. Kartapolov, currently Russia's Deputy Minister of Defense and the former head of the Russian General Staff's Main Operational Directorate.[47] Of these individuals, Gerasimov was most widely attributed to have created modern Russian hybrid warfare because of a heavily cited article he wrote in February 2013 to describe his thoughts on 21st-century wars.[48] In 2014, a British researcher, Mark Galeotti, coined the term "The

---

[46] Ofer Fridman, "On the 'Gerasimov Doctrine': Why the West Fails to Beat Russia to the Punch," *PRISM* 8, no. 2 (2019): 101.

[47] Viorel Barbu, "The Hybrid War in the East-West Paradigm," in *Strategic Changes in Security and International Relations*, ed. Dorin Corneliu Pleșcan et al., vol. XVI, Part 2 (16th International Scientific Conference, Bucharest, Romania: "Carol I" National Defence University, 2020), 101–12, https://www.strategii21.ro/A/2020-04.%20STRATEGIC%20CHANGES%20IN%20SECURITY%20AND%20INTERNATIONAL%20RELATIONS/FSA_2020_VOLUMUL%202.pdf#page=102; Elizabeth Bodine-Baron et al., *Countering Russian Social Media Influence* (Santa Monica, CA: RAND Corporation, 2018), https://doi.org/10.7249/RR2740; Sandor Fabian, "The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy," *Defense & Security Analysis* 35, no. 3 (2019): 308–25, https://doi.org/10.1080/14751798.2019.1640424; Fridman, "On the 'Gerasimov Doctrine'"; Mark Galeotti, "The Mythical 'Gerasimov Doctrine' and the Language of Threat," *Critical Studies on Security* 7, no. 2 (2019): 157–61, https://doi.org/10.1080/21624887.2018.1441623; Krisztian Jojart, "Russia Military Thinking and the Hybrid War," *Scientific Periodical of the Hungarian Military National Security Service*, no. 1 (2019): 82; Nina A. Kollars and Michael B. Petersen, "Feed the Bears, Starve the Trolls: Demystifying Russia's Cybered Information Confrontation Strategy," *The Cyber Defense Review* Special edition (2019): 145–60; Sarah O'Connor et al., *Cyber-Enabled Foreign Interference in Elections and Referendums*, Policy Brief Report No. 41 (Canberra, Australia: Australian Strategic Policy Institute, 2020), https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums; Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *Journal of Slavic Military Studies* 29, no. 4 (2016): 554–75, https://doi.org/10.1080/13518046.2016.1232541; Timothy Thomas, "The Evolving Nature of Russia's Way of War," *Military Review* 97, no. 4 (August 2017): 34–42; Thornton, "The Russian Military's New 'Main Emphasis'"; Wilhelm, "A Russian Military Framework."

[48] Valery Gerasimov, "The Value of Science in Prediction," *Military-Industrial Kurier*, February 27, 2013, https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf.

Gerasimov Doctrine" to encapsulate this evolution in Russian military thinking.[49] Over the next five years, the Gerasimov Doctrine was referenced or cited in hundreds of scholarly works.[50] In 2019, Galeotti gave a mea culpa when he clarified that the term was meant to be a placeholder for the changing thoughts about Russian military strategy.[51] Galeotti pointed out that Gerasimov was a career armored division officer and not considered a military science theoretician.[52] Other Russian experts also dismissed the Gerasimov Doctrine as a model for understanding how Russia incorporated information operations into its conventional warfare strategy.[53]

Like Gerasimov, Lieutenant General Bogdanov and a colleague wrote an article about hybrid warfare called the "New Generation War."[54] In this article published in February 2013, Bogdanov discussed the need for information technology and information operations superiority, as it perceived the United States and other Western countries were already using technology-enabled psychological warfare to target Russia.[55] Bogdanov believed these information operations could internally undermine a country's ability to govern and leave it vulnerable to conventional military force.[56] However, since the publication of that article, Bogdanov has not mentioned the term "New Generation War" in his subsequent articles.[57] Later on, Bogdanov would use a different term for hybrid warfare, popularized by Lieutenant General Kartapolov.[58]

---

[49] Galeotti, "The Mythical 'Gerasimov Doctrine' and the Language of Threat."

[50] Galeotti.

[51] Galeotti.

[52] Galeotti.

[53] Fridman, "On the 'Gerasimov Doctrine,'" 101; Fabian, "The Russian Hybrid Warfare Strategy," 311; Kollars and Petersen, "Feed the Bears, Starve the Trolls"; Thomas, "The Evolving Nature of Russia's Way of War."

[54] S.G. Chekinov and S.A. Bogdanov, "The Nature and Content of New Generation War," *Military Thought*, no. 4 (February 2013): 12–23.

[55] Chekinov and Bogdanov; Thomas, "The Evolving Nature of Russia's Way of War," 39.

[56] Kollars and Petersen, "Feed the Bears, Starve the Trolls," 147.

[57] Thomas, "The Evolving Nature of Russia's Way of War," 41.

[58] Thomas, 41.

In 2015, Lieutenant General Kartapolov published an article and gave a speech at the Russian Academy of Military Science about hybrid warfare, which he described as "New-Type Warfare."[59] Specifically, Kartapolov discussed using asymmetric means, such as cyber operations and other forms of political pressure, to weaken an adversarial state's military strength.[60] What differentiates Kartapolov from Gerasimov and Bogdanov was the specific manner in which he laid out the elements for successfully waging New-Type Warfare.[61] Multiple Western scholars consider Kartapolov's article and speech to be a roadmap for the current Russian military thought and practice of hybrid warfare.[62] Figure 1 shows a graphic from the Kartapolov article, which describes the tactics for conducting a New-Type War. In particular, Thomas Wilhelm, an American military scholar, has devised a framework for understanding Russian influence operations based on his analyses of multiple works by General Kartapolov, which will be discussed in further detail in the Research Design section of this thesis.[63]

[59] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods"; Thomas, "The Evolving Nature of Russia's Way of War," 38.

[60] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods"; Kollars and Petersen, "Feed the Bears, Starve the Trolls," 147.

[61] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 35.

[62] Barbu, "The Hybrid War in the East-West Paradigm," 109; Jojart, "Russia Military Thinking and the Hybrid War," 19; Kollars and Petersen, "Feed the Bears, Starve the Trolls," 147; Thomas, "The Evolution of Russian Military Thought"; Thomas, "The Evolving Nature of Russia's Way of War," 41; Thornton, "The Russian Military's New 'Main Emphasis,'" 23; Wilhelm, "A Russian Military Framework," 33.

[63] Wilhelm, "A Russian Military Framework," 33.

Figure 1. Kartapolov's Components for Conducting Hybrid Warfare.[64]

4. Recommendations for Countering Russian Influence Campaigns

Recommendations for countering Russian malign influence operations primarily come from three sectors: (1) the U.S. government, (2) non-governmental organizations such as think tanks, and (3) researchers affiliated with academic institutions. The intelligence committees for both houses of Congress provided recommendations in the reports, which summarized their investigations of Russian interference in the 2016 U.S. elections. The House Permanent Select Committee on Intelligence report's recommendations focused on information sharing between election-related stakeholders, improved cybersecurity for election information infrastructure, and potential legislative actions to enhance cybersecurity.[65] The Senate Permanent Select Committee on Intelligence report's recommendations discussed the Executive Branch using a suite of deterrents to dissuade foreign influence in U.S. elections, such as sanctions, diplomatic pressure, and cyber operations, enhanced cybersecurity measures for election

[64] Source: Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 35; Thomas, "The Evolution of Russian Military Thought," Appendix 1.

[65] H.R., *Report on Active Measures*, 120–22.

infrastructure, and replacing outdated election equipment.[66] All of these recommendations may broadly be characterized as security measures.

Like the Congressional reports, various policy think tanks have proposed a series of recommendations to counter Russian influence campaigns. The RAND Corporation suggested a three-pronged set of activities: (1) targeting the Russian government through sanctions, diplomacy, and pro-democracy programs; (2) identifying and disrupting the activities of the Internet Research Agency and other proxies through information sharing and improved detection technologies; and (3) disrupting the effectiveness of social media amplification channels through technology enhancements and policy changes.[67] Similar to the third prong of RAND's recommendations, the German Marshall Fund was highly focused on improved transparency through better information-sharing between companies and better labeling state-sponsored content.[68] Looking at the environment from a more holistic perspective than RAND or the German Marshall Fund, the Belfer Center advocated for a national strategy for countering information operations, to include increased transparency to attribute and reveal Russian influence operations, leveraging all facets of the U.S. government to disrupt these operations, increased engagement with allies to counter influence operations, and better cooperation between the U.S. government and social media companies.[69] In contrast to the other organizations, the Belfer Center also advocated for improved media literacy in the nation's education system.[70] In summary, the writers' consensus viewpoint from the literature review is that enhanced security, transparency, and resiliency are crucial to combating malign Russian influence in elections.

As another group of outside observers of social media influence campaigns, academic researchers provided practical proposals based on their analysis of the IRA's

---

66 *Russian Active Measures Campaigns: Volume 1*, 55–60.

67 Bodine-Baron et al., *Countering Russian Social Media Influence*, 12.

68 Bradley Hanlon, *A Long Way to Go - Analyzing Facebook, Twitter, and Google's Efforts to Combat Foreign Interference*, Policy Brief No. 41 (Washington, DC: German Marshall Fund of the United States, 2018), 1, https://securingdemocracy.gmfus.org/wp-content/uploads/2018/12/A-Long-Way-to-Go-Analyzing-Facebook-Twitter-and-Googles-Efforts-to-Combat-Foreign-Interference.pdf.

69 Cederberg et al., *National Counter-Information Operations Strategy*, 11–12.

70 Cederberg et al., 12.

tactics and activities. These proposals may have added weight because they are in peer-reviewed publications. Both DiResta and Howard's academic research teams, from Stanford University and Oxford University respectively, provided wide-ranging proposals involving collaboration between relevant stakeholders to counter current and future Russian influence campaigns.[71] These recommendations included information sharing between private sector companies and the government, better policing and content moderation by the social media companies, and critically thinking about how future technologies can influence campaigns.[72]

In contrast to DiResta and Howard's teams, researchers from the Harvard Kennedy School concentrated their recommendations on social media companies.[73] Specifically, the Harvard researchers focused on policy improvements for the social media companies concerning increased transparency for taking down content, better content moderation, labeling state-sponsored content, providing links to reliable sources of information, and focusing on their users' rights and privacy.[74] Kate Starbird, a University of Washington researcher, agreed on the critical nature of better content moderation by the social media companies but expressed concern about the potential curtailment of free speech.[75] In a completely different vein, Canadian researchers Barry Cartwright et al. believe advanced

71 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 101; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 40.

72 DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1–2.

73 Deen Freelon and Tetyana Lokot, "Russian Disinformation Campaigns on Twitter Target Political Communities across the Spectrum. Collaboration between Opposed Political Groups Might Be the Most Effective Way to Counter It.," *Harvard Kennedy School Misinformation Review* 1, no. 1 (2020): 2, https://doi.org/10.37016/mr-2020-003.

74 Freelon and Lokot, 2.

75 Kate Starbird, Ahmer Arif, and Tom Wilson, "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations," *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 2019): 19, https://doi.org/10.1145/3359229.

technology, specifically artificial intelligence, will be vital for detecting and combating foreign influence campaigns.[76]

A review of the literature revealed some trends among the different sectors, which provided recommendations. The Congressional recommendations focused on security measures such as enhanced cybersecurity, economic sanctions, and cyber operations.[77] The think tank recommendations ran the gamut from security measures similar to Congressional recommendations to transparency measures, such as promoting public communications about disinformation campaigns by the U.S. government, to resilience measures, such as improved media literacy.[78] Academic literature generally supported the same security, transparency, and resiliency measures favored by think tanks and public policy organizations.[79]

5. Conclusions from Literature Review

A review of all the relevant literature makes clear that Russia has and will continue to persist as an adversarial nation-state seeking to destabilize American democracy. The current online influence campaigns being conducted by Russian actors are an extension of Soviet-era psychological warfare operations, amplified by 21st-century social media platforms. The sources providing recommendations to counter these malign influence operations include academia, private sector, government, think tanks, and other non-

---

[76] Barry Cartwright, George Weir, and Richard Frank, "Fighting Disinformation Warfare with Artificial Intelligence: Identifying and Combatting Disinformation Attacks in Cloud-Based Social Media Platforms," in *CLOUD COMPUTING 2019 Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization*, ed. Bob Duncan et al. (Cloud Computing 2019, Venice, Italy: IARIA, 2019), 73–77, https://www.researchgate.net/publication/333024381_CLOUD_COMPUTING_2019_Proceedings_of_the_Tenth_International_Conference_on_Cloud_Computing_GRIDs_and_Virtualization.

[77] *Report on Russian Active Measures*, 121–27; *Russian Active Measures Campaigns: Volume 1*, 54–57.

[78] Cederberg et al., *National Counter-Information Operations Strategy*, 11–12; William Marcellino et al., *Foreign Interference in the 2020 Election: Tools for Detecting Online Election Interference* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RRA704-2.html.

[79] DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1–2; Darren L. Linvill and Patrick L. Warren, "Engaging with Others: How the IRA Coordinated Information Operation Made Friends," *Harvard Kennedy School Misinformation Review* 1, no. 2 (April 2020): 2, https://doi.org/10.37016/mr-2020-011.

governmental organizations. The variety of sources and input indicates that a whole-of-society approach utilizing a range of security, transparency, and resiliency measures will be necessary to combat Russian influence operations.

D. RESEARCH DESIGN

The objectives of this thesis are three-fold: (1) examining the Internet Research Agency and other Russian social media campaigns ahead of the 2020 U.S. elections to determine whether its tactics have shifted since 2016; (2) critically analyzing the private sector and U.S. government's actions to counter the Russian influence activities; and (3) proposing recommendations to safeguard future U.S. elections. The first two objectives will be assessed using an analytical framework proposed by Thomas Wilhelm, Director of the U.S. Army's Foreign Military Studies Office. The last objective will be informed by the results of the first two objectives, as well as a review of current literature by scholars and subject matter experts in different fields.

To design a useful framework for analyzing Russian influence operations, Thomas Wilhelm surveyed the published works and speeches of General Lieutenant Andrei V. Kartapolov. Wilhelm surmised Kartapolov was one of the key architects of current Russian military science and doctrine, specifically the aforementioned "New-Type War."[80] Wilhelm believed the framework provided a well-rounded understanding of Russian martial intent and objectives about hybrid warfare through a Russian perspective.[81] Specifically, Kartapolov advocates utilizing asymmetric, non-violent methods to undermine the strengths of Russia's opponents to achieve their strategic goals.[82] Kartapolov highlighted ten components for conducting hybrid warfare, herein referred to as the Kartapolov Framework: (1) spreading discontent in the population; (2) exerting political pressure; (3) confusing the political leadership; (4) use of new and advanced weaponry; (5) train and arm opposition forces; (6) utilization of special military forces

[80] Tom Wilhelm, "A Russian Military Framework for Understanding Influence in the Competition Period," *Military Review* (2020): 35.

[81] Wilhelm, 38.

[82] Thornton, "The Russian Military's New 'Main Emphasis.'"

behind enemy lines; (7) commit large scale subversive acts to destabilize to the enemy; (8) shift to conventional warfare after softening the enemy; (9) destroy the enemy and seize territory concurrently; and (10) use airstrikes and artillery to destroy any focal points of resistance to establish complete control of the territory.[83]

The relevant components of the Kartapolov Framework for analyzing Russian social media-based influence operations against the United States are: (1) spreading discontent in the population; (2) exerting political pressure; and (3) confusing the political leadership.[84] This thesis will use the Kartapolov framework to conduct a qualitative evaluation of the Internet Research Agency's impact and the effectiveness of social media companies and the U.S. government's countermeasures. To assess the social media companies and the U.S. government's actions to counter Russian influence activities, this thesis will also employ the Kartapolov framework. Specifically, the American actions will be analyzed to determine their effectiveness for countering the three influence-related components of the Kartapolov Framework. In particular, a qualitative analysis will evaluate American efforts to counter the spread of discontent in the American populace, defuse political pressure, and stop confusion in political leadership. The analysis will be dependent on publicly available information.

The review of the private sector countermeasures to the IRA's influence campaign will be based on examining three sources of information. Private sector actions, specifically those of the "Big Three" social media companies of Facebook, Google, and Twitter, are tracked and reviewed by academic researchers and non-governmental organizations.[85] These two groups write reports or papers based on their findings. An example of this type of information is a recently published paper examining Twitter's account suspensions related to the 2020 U.S. elections by researchers from the University of New Mexico and

[83] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 35.

[84] Kartapolov, 36.

[85] Ryan Robinson, "7 Top Social Media Sites in 2020," Adobe Spark, accessed July 21, 2021, https://www.adobe.com/express/learn/blog/top-social-media-sites.

the Georgia Institute of Technology.[86] The social media companies have also regularly made public announcements of their actions to combat foreign influence activities. These types of information will be used to assess the impact of the private sector's countermeasures.

The review of U.S. government countermeasures will rely only on publicly available, unclassified information. Although classified reporting on U.S. government actions likely exists, these sources will fall outside this thesis's scope. In certain instances, different facets of the U.S. Government generates unclassified reports, such as those produced by the different committees in Congress or various executive branch agencies. In other circumstances, the U.S. government will make public statements or unseal legal documents such as indictments or arrest affidavits. On occasion, the news media will also leverage their sources to reveal U.S. government actions. These types of information will be used to assess the impact of the U.S. government's countermeasures.

Recommendations for safeguarding future U.S. elections will be informed by the aforementioned analyses of actions taken by the private sector and the U.S. government and a review of advice provided by subject matter experts in various fields. These experts comprise academic scholars, researchers from non-governmental organizations, and U.S. government officials from both the legislative and executive branches. The diverse experiences and perspectives should provide a robust set of recommendations for a whole-of-society approach to secure elections.

In summation, the examination of the Internet Research Agency's social media campaigns ahead of the 2020 U.S. elections will rely primarily on exploring literature produced by four groups: academic researchers, non-governmental research organizations, reports from the social media companies, and U.S. government investigatory reports. Although offering different perspectives, these subject matter experts provide the most reliable analysis and assessment of the Russian influence activities.

---

[86] Farhan Asif Chowdhury et al., "Examining Factors Associated with Twitter Account Suspension Following the 2020 U.S. Presidential Election," *ArXiv* 2101, no. 09575 (January 23, 2021), https://arxiv.org/pdf/2101.09575.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

II. OPENING MOVES – SCOPE AND BACKGROUND

> We're all targets of a sophisticated and capable adversary and we must engage in a whole-of-government approach to combat Russian active measures.
>
> — Richard Burr, March 30, 2017

In the Russian Federation, President Vladimir Putin, who has been in power since 2000, makes every major decision.[87] As a former senior-level KGB officer, Putin holds antagonistic views of liberal democracies in general and the United States in particular.[88] Michael McFaul, former U.S. Ambassador to Russia, assessed that Putin sees the United States as "a hostile power and a serious threat to Russian national interests."[89] As such, Putin perceives himself to be in an ideological struggle "between conservative, Christian, sovereign values—which he embraces—and decadent, liberal, multilateral ideas championed by many Western governments, including first and foremost the United States."[90] Harkening back to Soviet-era information operations, Putin recognized the advent of online social media platforms as an avenue to target U.S. elections.[91] The Russian influence operations started before the 2016 U.S. elections and continued through the 2020 U.S. elections.

Before delving into the nuances of the Russian online social influence campaigns targeting the 2020 U.S. elections, this chapter outlines the scope of the issue to be studied in this thesis, the recent history motivating these influence campaigns, a review of Russian and American measures during the 2016 and 2018 U.S. elections, and an analysis of the effectiveness of these measures using the Kartapolov Framework.

---

87 Timothy J. Colton and Michael McFaul, "Russian Democracy under Putin," *Problems of Post-Communism* 50, no. 4 (July 2003): 13, https://doi.org/10.1080/10758216.2003.11656043.

88 S., *Russian Active Measures*, 14.

89 McFaul, *Securing American Elections*, 11.

90 McFaul, 11.

91 Starbird, Arif, and Wilson, "Disinformation as Collaborative Work," 4.

A. SCOPE OF THESIS

The current Russian information operations targeting U.S. elections can trace their roots to Soviet-era propaganda and disinformation campaigns.[92] Because of the immense longevity and scale of these Russian information operations, it is essential to frame what will be discussed within the confines of this thesis. The critical components to be bounded are time periods covered, types of influence operations, and the social media platforms to be examined.

1. Relevant Time Periods

On March 30, 2017, Eugene Rumer, Senior Fellow at the Carnegie Endowment for International Peace, testified before the Senate Select Committee on Intelligence and described active measures as a century-old suite of information warfare tools continuously being used by Russia to advance its ideological objectives and erode the stability of its liberal democratic rivals.[93] The use of disinformation campaigns, i.e., intentionally propagating false or misleading information, is one of the primary tools in their portfolio.[94] Soviet-era active measures evolved and are now "enabled by technology and adapted for a globalized world, their modern incarnations are much more sinister, with far greater range and speed – and, through the Internet, able to influence popular opinion on a scale never before possible."[95] However, it was only around the 2016 U.S. elections when the Russians deployed these large-scale online disinformation campaigns against the American democratic system.[96] Therefore, this thesis will focus on Russian activities from three distinct periods: (1) preceding and during the 2016 U.S. elections, (2) after the 2016 U.S. elections to preceding the 2018 U.S. midterm elections, and (3) after the 2018 U.S. midterm elections to the 2020 U.S. elections.

---

92 Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections: The Quarterly Journal* 15, no. 1 (2016): 8, https://doi.org/10.11610/Connections.15.1.01.

93 S., *Russian Active Measures*, 10.

94 S., *Russian Active Measures*, 10.

95 Abrams, "Beyond Propaganda," 8.

96 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 22.

2. Types Of Russian Influence Operations

The Russian influence operations directed at the 2016 U.S. Presidential elections are broadly divided into three categories, the last of which will be within the scope of this thesis.[97] The first category is "hack and dump," wherein Russian hackers breached the DNC computer networks, stole data, and then disseminated it via different online platforms such as WordPress, Twitter, and Wikileaks.[98] The second category is attempted hacks on the actual voting systems in each state. The systems include voter registration databases and online polling equipment. The last category, as described by researchers from New Knowledge, is the "sweeping and sustained" online social media influence campaign perpetrated by the Internet Research Agency "consisting of various coordinated disinformation tactics aimed directly at U.S. citizens, designed to exert political influence and exacerbate social divisions in U.S. culture."[99]

Online social media influence campaigns conducted by the Internet Research Agency and other Russian-backed organizations will be the focus of this thesis because they have a significant and continuing impact on Americans and democracy. In contrast, the other two types of Russian influence operations, focused on political campaigns and election infrastructure, are only germane to Americans every two years during election seasons. Since the 2016 election, federal agencies and private sector organizations have been actively helping to safeguard political campaigns and election infrastructure from computer intrusions through increased cybersecurity and other security measures. Arguably, campaigns and election systems are better protected now than they were in 2016. Though regularly occurring on a biennial basis, American engagement with the electoral process is little compared to their daily, and sometimes hourly, social media engagement.

In 2019, about 70 percent of all Americans had at least one social media account and used the Internet between 30 minutes to two hours per day.[100] This statistic means the

---

97 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 4.

98 DiResta et al., 4.

99 DiResta et al., 4.

100 J. Clement, "Social Media Usage in the United States," Statista, May 19, 2020, https://www.statista.com/topics/3196/social-media-usage-in-the-united-states/.

IRA has daily opportunities to reach out to Americans via social media newsfeeds or posts. Due to First Amendment constraints, federal agencies have little involvement in Americans' usage of social media. Couple this with the fact that social media companies have a vested interest in keeping American users on their platforms. For the most part, Americans are left to fend for themselves on social media platforms.

Research has shown mixed results regarding people's usage of social media. On the one hand, social media usage positively correlates with increased political engagement.[101] On the other hand, users tend to stay on social media platforms longer when engaged with content that conforms to their own opinions, whether factual or not.[102] The social media companies understand this phenomenon and finetune their algorithms to keep feeding content they think users want.[103] The IRA could take advantage of this behavior by inserting itself into the social media ecosystem and working to sow discord and erode the American public's trust in democratic institutions.

3. Targeted Social Media Platforms

Despite a vast array of social media platforms, Russians primarily targeted these three of the four most visited ones: #1 – YouTube, a Google subsidiary, #3 – Twitter, and #4 - Facebook.[104] Wikipedia is the #2 most visited website, but not a social media platform and heavily moderated, unlike the other sites.[105] Whereas previous studies focused on discrete periods around a single election (2016, 2018, or 2020), this thesis will review and analyze Russian activities across the entire time when the IRA and other Russian-backed groups have targeted the United States with its social media influence campaigns. The term,

---

101 Sebastián Valenzuela, "Unpacking the Use of Social Media for Protest Behavior: The Roles of Information, Opinion Expression, and Activism," *American Behavioral Scientist* 57, no. 7 (July 2013): 923, https://doi.org/10.1177/0002764213479375.

102 Armin A. Rad, Mohammad S. Jalali, and Hazhir Rahmandad, "How Exposure to Different Opinions Impacts the Life Cycle of Social Media," *Annals of Operations Research* 268, no. 1 (2018): 88, https://doi.org/10.1007/s10479-017-2554-8.

103 Rad, Jalali, and Rahmandad, 89.

104 DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 6.

105 Joshua Hardwick, "Top 100 Most Visited websites by Search Traffic (as of 2020)," *Ahrefs* (blog), May 12, 2020, https://ahrefs.com/blog/most-visited-websites/.

private sector companies, will refer to the three companies whose social media platforms were the most heavily used by the Russians for their influence operations. Understanding the IRA's activities across this period may reveal the efficacy of actions taken by the private sector companies and the U.S. government in response to the IRA's efforts.

B. RECENT HISTORY – THE CAMPAIGNS FROM 2016 TO 2018

Around 2014, Putin tapped his close ally Yevgeniy Prigozhin to conduct influence operations against the American public.[106] Prigozhin, recognized as "Putin's Chef," is a Russian oligarch who owns a conglomerate known as Concord Management, with subsidiaries in various businesses, including catering.[107] Project Lakhta is the umbrella term for Prigozhin-owned firms focused on domestic and overseas influence operations. By September 2016, the monthly operating budget of Project Lakhta was the equivalent of $1.25 million.[108] One of the businesses under Project Lakhta is the Internet Research Agency, founded around 2013 in St. Petersburg, Russia, to be a sophisticated marketing and influence firm. Organized like a legitimate business, its management group oversees various departments, including finance, information technology, search engine optimization, data analysis, and graphics.[109] Before targeting Americans, IRA employees engaged in around-the-clock influence operations directed at Russian and Ukrainian citizens.[110] In April 2014, a new department called the "Translator Project" was formed to conduct online activities against Americans on the American social media platforms of Twitter, Facebook, Instagram, and YouTube.[111] By July 2016, IRA assigned more than 80 employees to the Translator Project.[112] These machinations showed the Russian

106 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 5.

107 U.S. vs. Internet Research Agency LLC, No. 18-cr-00032-DLF (U.S. District Court for the District of Columbia February 16, 2018).

108 U.S. vs. Internet Research Agency LLC at 7.

109 U.S. vs. Internet Research Agency LLC at 5.

110 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

111 U.S. vs. Internet Research Agency LLC at 6.

112 U.S. vs. Internet Research Agency LLC at 6.

Federation's commitment of personnel and resources to pursue this type of covert online campaigning.

President Putin's initial strategy appeared to be inflaming the existing discord in the American populace and eroding public confidence in American institutions such as free speech and the electoral process. Still, that strategy evolved as it became clear who the nominees would be. By June 2016, Hillary Clinton was the presumptive Democratic nominee and frontrunner for president. Putin was known to despise Clinton during her tenure as Secretary of State during the Obama Administration.[113] She seemed to be the ideological opposite of Putin. Clinton believed in multilateral international cooperation, wanted to strengthen NATO, desired increased sanctions for Russia's occupation of Crimea, and advocated for fair elections and greater freedoms within Russia.[114] Putin may have sensed that Donald Trump's rise as a legitimate candidate offered an avenue to advance his anti-American agenda. Putin's strategy evolved as the presidential campaign season continued through the summer, supporting Trump as its centerpiece.[115] The Russian covert influence operation pivoted to helping the Trump campaign, in addition to its continued efforts to tear down the Clinton campaign.[116] An IRA-purchased political advertisement on Facebook reflected its efforts to target Clinton in Figure 2. This behavior showed the adaptability of the Russians to make use of contemporaneous events for their advantage.

---

113 McFaul, *Securing American Elections*, 14.

114 McFaul, 14.

115 Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions*, 7.

116 Mueller, "Report on The Investigation into Russian Interference in the 2016 Presidential Election," 5.

Figure 2. Facebook Political Advertisement Targeting Hillary Clinton.[117]

1. What Happened During the 2016 U.S. Elections?

The Russian influence campaigns utilizing American social media platforms started around 2013 and extended through the 2016 U.S. elections.[118] Reviewing the Russian measures and the countermeasures taken by the private sector companies and the U.S. government during this time sets up the baseline for comparison to the Russian and American activities during the 2020 U.S. elections. Moreover,

---

[117] Source: "HPSCI Minority Open Hearing Exhibits," Permanent Select Committee on Intelligence, accessed March 20, 2021, https://intelligence.house.gov/hpsci-11-1/hpsci-minority-open-hearing-exhibits.htm.

[118] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

examining these actions across three separate elections may reveal trends and evolutions in tactics by the Russians and Americans.

a. The IRA's Social Media Activities

Before the 2016 U.S. Elections, the Internet Research Agency's influence operations against the American public encompassed three lines of effort. First, IRA employees made and maintained fake user accounts and pages on social media platforms that covered a range of political issues.[119] For these accounts and pages, the IRA employees generated organic content to ingratiate themselves with online communities and amplify or steer the themes discussed in these communities. Second, IRA employees used social media bots, i.e., computer programs which control social media accounts, to amplify existing content.[120] Third, IRA employees covertly purchased online advertisements from social media companies to enhance their organic content and drive online traffic to sites controlled by them.[121] In the marketing world, advertisements are known as "paid content." In contrast, organic content refers to unpaid messaging generated by people that helped foster support for a product or brand through voluntary and spontaneous recommendations by users.[122] Although the IRA employees were being paid, they impersonated regular users on the social media platforms so their messaging could look authentic. Ironically, Russians masqueraded as Americans and weaponized free speech to foment division and corrode Americans' faith in such speech.

For the first line of effort, the IRA managed its influence operations like a digital marketing campaign.[123] It created false personas and imitated activist groups on the left and right sides of the political spectrum. These personas and groups extended across

---

[119] U.S. vs. Internet Research Agency LLC at 14.

[120] Dhiraj Murthy et al., "Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital," *International Journal of Communication* 10 (2016): 4.

[121] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 17.

[122] Nicole A. Buzzetto-More, "Social Media and Prosumerism," *Issues in Informing Science and Information Technology* 10 (July 2013): 75.

[123] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

multiple social media platforms.[124] Philip Howard, University of Oxford researcher, opined that "users were more likely to assume the credibility of the false organizations set up by the IRA with a presence across multiple platforms, operating websites, YouTube channels, Facebook pages, Twitter accounts, and even PayPal accounts set up to receive donations."[125] Viewers believed these were legitimate because of the extraordinary efforts the personas and groups had taken. To finetune its messaging, IRA employees visited the United States in 2014 to learn about American culture, gather intelligence, and take photographs later used to enhance the authenticity of their false online personas.[126] The care the IRA took showed its deep commitment and calculation in its endeavors to harness American-style free speech to undermine trust in democracy.

When reviewing the IRA-generated Facebook content, some themes emerge. First, on the left end of the political spectrum, the IRA's efforts targeted minority groups to suppress voter turnout.[127] Topics of messaging included anti-government rhetoric, boycotting the election, following the wrong voting procedures, and scaring voters from showing up at polling locations.[128] Figure 3 illustrates an example of IRA-purchased political advertisements on Facebook with anti-government messaging targeting black voters. Second, on the right end of the political spectrum, the IRA promoted conspiracy theories, stopping legal and illegal immigration, protecting gun rights and religious freedom, and other relevant issues for conservatives (see Figure 4).[129] Again, the efforts were presumably targeting conservatives to drive up voter turnout.

---

[124] F. Sattelberger, "Optimising Media Marketing Strategies in a Multi-Platform World: An Inter-Relational Approach to Pre-Release Social Media Communication and Online Searching.," *Journal of Media Business Studies* 12, no. 1 (2015): 66, https://doi.org/10.1080/16522354.2015.1027117.

[125] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 8.

[126] Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 14.

[127] Linvill and Warren, "Engaging with Others," 2.

[128] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3.

[129] Howard et al., 3.

Figure 3. Facebook Political Ads Targeting Black voters.[130]

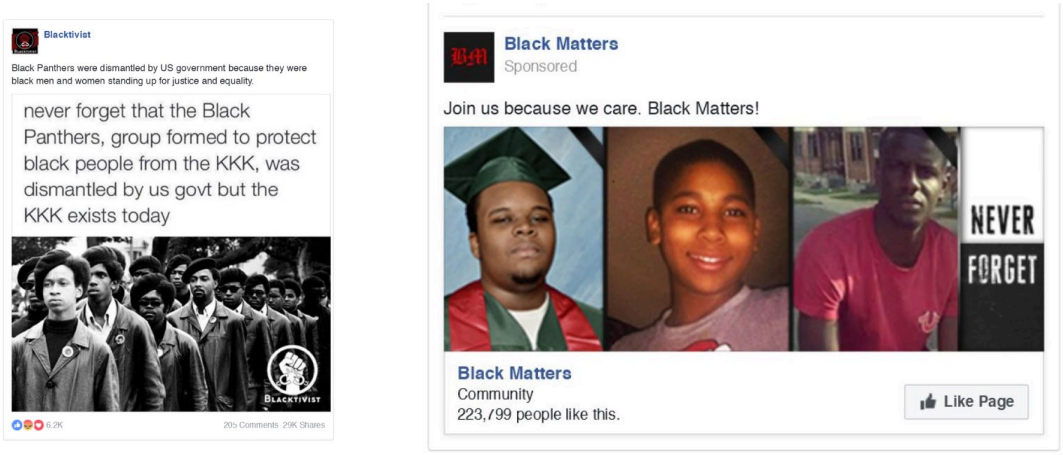
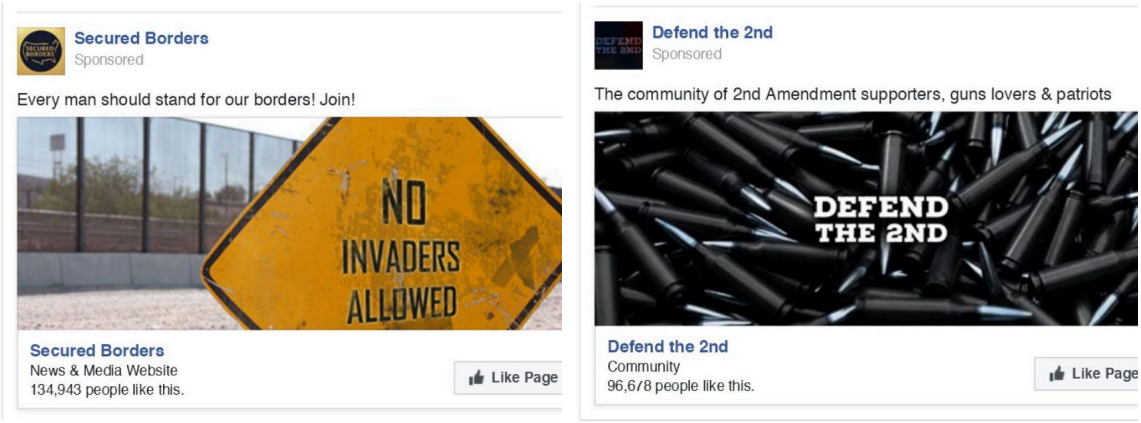


Figure 4. Facebook Political Ads Targeting Right-Wing Voters.[131]



The ratios of IRA-generated content on Facebook changed through the course of 2016. In the first half of 2016, over half of all the most active IRA-made Facebook accounts targeted right-wing audiences with posts discussing the topics referenced above.[132] This phenomenon happened before Trump had won the Republican presidential nomination. Explicit mentions of Trump increased by mid-2016 after he secured the nomination and

130 Source: "HPSCI Minority Open Hearing Exhibits."

131 Source: "HPSCI Minority Open Hearing Exhibits."

132 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 33.

focused on amplifying the anti-immigrant rhetoric, which was a hallmark of the Trump campaign.[133] Howard summed up his analysis by stating it was "clear that the IRA sought to energize conservatives around Trump's campaign and encourage the cynicism of other voters in an attempt to neutralize their vote."[134] Howard's examination concluded that the Russians sought to elicit specific behavior, namely encouraging right-wing voters to turn out for Trump and discouraging left-wing and minority voters from going to the polls.[135]

A review of Twitter activities in 2016 showed similar behavior to the IRA's activities on Facebook.[136] In further support of the idea that the IRA treated its influence operations as a marketing campaign, Josephine Lukito, a University of Wisconsin researcher, observed the IRA posting messages on Reddit before similar messages appeared on Twitter.[137] Lukito assessed that the IRA could have been using Reddit to test message resonance before deployment to Twitter.[138] From July 2, 2015 to May 31, 2017, there were about 1.9 million tweets but only 12,603 Reddit posts.[139] Lukita noted that "Twitter's centrality to the IRA's campaign may also explain why more content was produced on Twitter relative to Reddit."[140] Lukita suggested that Reddit's usage may have been a "trial balloon" and opined it could be evidence of the IRA treating their social media influence operation like a marketing campaign.[141] One of the campaign's central goals appeared to be influencing voter turnout during the elections, which was similar to what Philip Howard had concluded.[142]

---

[133] Howard et al., 33.

[134] Howard et al., 32.

[135] Howard et al., 3.

[136] Howard et al., 27.

[137] Josephine Lukito, "Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017," *Political Communication* 37, no. 2 (2020): 249, https://doi.org/10.1080/10584609.2019.1661889.

[138] Lukito, 249.

[139] Lukito, 249.

[140] Lukito, 249.

[141] Lukito, 238.

[142] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 19.

In contrast to the IRA activities on Facebook and Twitter, the YouTube videos provided by Google to the Senate Select Committee on Intelligence revealed that most of them were used to target African Americans.[143] It is unclear why the IRA chose this platform to target African Americans specifically. However, because Google provided only a limited amount of data for public research, making any general conclusions regarding IRA activities on Google's platforms is difficult.[144] YouTube is the most visited site in the United States, mainly used for broadcasting videos.[145] It does not facilitate two-way communications as quickly as the other two platforms.[146] As on the other two platforms, the Senate Intelligence Committee assessed the intent of the YouTube videos might have been to suppress black voter turnout since the YouTube videos were primarily targeted at African Americans.[147]

The sheer magnitude of the IRA's social media campaign targeting the United States was unparalleled in the digital age. Researchers retained by the SSCI estimated the IRA had uploaded over 1,000 videos on YouTube and reached a significant number of American users: 59 percent on Facebook, 19 percent on Instagram, and two percent on Twitter.[148] In table 1, the Special Counsel's Office estimated the number of people reached by a Facebook posting or a Twitter tweet. Although the ultimate number of individual American voters influenced by the IRA remains unclear, table 1 reveals the scale of the reach by the social media platforms.

---

143 Howard et al., 18.

144 Howard et al., 9.

145 Hardwick, "Top 100 Most Visited websites by Search Traffic (as of 2020)."

146 Hardwick.

147 *Russian Active Measures Campaigns: Volume 2*, 6.

148 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

Table 1. Reach of IRA-controlled Social Media Accounts[149]

Social Media Platform	Number of Accounts	Number of Users Reached
Facebook	470	126,000,000
Twitter	3,814	1,400,000

For the second line of effort, the IRA amplified real user accounts whose identities, behavior, and content aligned with the IRA's strategic goals.[150] Clemson University researchers discovered over 100,000 real user accounts amplified by IRA-controlled social media bots.[151] They noted the IRA-targeted accounts with fewer followers for amplification and speculated these types of accounts would generate less scrutiny from the social media companies or perhaps wanted to increase these accounts' prominence to serve their ends. Immediately before and after the 2016 U.S. elections, the IRA changed from generating its own original content to amplifying real users' messages. The IRA may have presumed that real users' posts would be more impactful and resonant with American viewers.[152] This shift showed the IRA's continued evolution to maximize its effectiveness.

For the third line of effort, the IRA purchased online advertisements from the social media companies to complement its other activities.[153] In 2016, the IRA spent about $100,000 on Facebook and $5,000 on Google.[154] Twitter noted that the Kremlin-controlled media site, Russia Today, spent about $274,000 in online advertisements to

149 Adapted from Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 15.

150 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 26.

151 Linvill and Warren, "Engaging with Others," 3.

152 Linvill and Warren, 3.

153 U.S. Congress. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns: Volume 2*, 7.

154 Patrick Savage, *Russian Social Media Information Operations: How Russia Has Used Social Media to Influence U.S. Politics* (Washington, DC: American Security Project, 2017), 1, https://www.hsdl.org/?view&did=808713.

promote over 1,800 tweets on its platform.[155] The IRA was very tactical in its advertising campaign. Using "race, ethnicity, and self-identity" as categories allowed it to use Facebook and Instagram to target specific demographic groups.[156] Then, it would run advertising targeting each of these demographic groups to drive users to IRA-created social media content.[157] The IRA employed different tactics for the purchase of Google online advertisements. In this case, Google ads guided users to various IRA-controlled websites and domains.[158] Marketing research indicates organic content has more resonance than paid content (i.e., advertisements).[159] Since the IRA's online advertising campaign primarily drove users to the organic content, evaluating its success is difficult. The Senate Select Committee on Intelligence concluded that the advertisements were not a vital component of the IRA's campaign.[160] However, the IRA used different techniques to further its social media influence operation, showing flexibility and adaptability.

b. Private Sector Countermeasures

In broad terms, organizations may take three categories of actions to counter influence operations: security, transparency, and resiliency. Security measures involve the monitoring, detection, and neutralization of threats. Transparency measures comprise information sharing to relevant stakeholders, whether between organizations, organizations and individuals, or the general public. Transparency measures also promote trust by allowing people to see what is going on. Finally, resiliency measures involve taking steps to be able to recover quickly from adverse situations.

During and immediately after the 2016 U.S. elections, the Big Three social media companies of Facebook, Google, and Twitter were utterly unaware of the IRA's massive

---

155 Savage, 1.

156 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 17.

157 Howard et al., 17.

158 Howard et al., 17.

159 Buzzetto-More, "Social Media and Prosumerism," 75.

160 S., *Russian Active Measures Campaigns: Volume 2*, 7.

influence campaign across all of their platforms.[161] The social media companies had no countermeasures in place to mitigate or disrupt the IRA's activities. Even if they had been aware, whether the social media companies would have taken any serious actions cannot be known for sure. Comments from Mark Zuckerberg, Founder and Chief Executive Officer of Facebook, on November 11, 2016, exemplified the companies' mindset when he famously said the notion that fake news would have any impact on the presidential elections was "a pretty crazy idea."[162] The social media companies took no security, transparency, or resilience measures. Ultimately, they offered no resistance to the IRA's malign activities during the 2016 U.S. elections.

c. U.S. Government Countermeasures

The private sector and U.S. government's efforts were disconnected ahead of the 2106 elections. Although U.S. government agencies, such as the FBI, monitored Russian influence operations, none of their acquired intelligence was relayed to the social media companies to protect their platforms.[163] Ambassador McFaul noted that cooperation between the technology companies and the U.S. government was "almost non-existent" before the 2016 U.S. Elections in the post-Snowden leak era.[164] This condition showed an almost complete lack of transparency between the two entities.

The U.S. government's attempts at security or transparency measures did not come until late into the presidential campaign season. The first official statement regarding the 2016 elections from the U.S. government came on October 7, 2016, when the Department of Homeland Security and Office of the Director of National Intelligence issued a one-page joint statement attributing the hack of the DNC and multiple hacking attempts against state election infrastructure to the Russian Federation.[165] However, the statement provided no technical details and only general cybersecurity guidance. The joint statement's intended

---

[161] McFaul, *Securing American Elections*, 43.

[162] Shahani, "Zuckerberg Denies Fake News on Facebook Had Impact on The Election."

[163] McFaul, *Securing American Elections*, 43.

[164] McFaul, *Securing American Elections*, 43.

[165] "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security."

effect may have been to inform the American electorate of malign actions being taken by Russia. Though such an effect was probably diminished because on the same day, the media was focused on the breaking news that Donald Trump had made lewd comments about women to Entertainment Tonight reporter Billy Bush in 2005 when the *Washington Post* released a video of their conversation.[166]

The second set of transparency and security-related actions from the U.S. government came on December 29, 2016, which was well after the elections. As an act of transparency, the FBI and DHS issued a joint action report titled "GRIZZLY STEPPE—Russian Malicious Cyber Activity." The report provided an overview of the Russian hacking activities ahead of the election and shared technical details.[167] If the U.S. government had provided this information ahead of the elections, especially the technical details, it could have helped political organizations and campaigns safeguard their computer networks and electronic devices. As another security and transparency action by the U.S. government, the Department of the Treasury publicly sanctioned nine Russians and two Russian intelligence agencies, the Federal Security Service (FSB) and the General Military Intelligence Directorate, for election-related cybercrimes.[168] It also sanctioned two Russian hackers for financial cybercrimes under the same executive order (E.O. 13694).[169] The purpose of these sanctions was to expose the American public to all of the Russian activities directed against the U.S. elections. Other sanctions such as those imposed by the Magnitsky Act have illuminated Russian oligarchs' and bureaucrats' corrupt financial dealings while relinquishing their ill-gotten funds.[170] Although these actions showed a proportional response from the U.S. government, the effect of such

---

166 THR Staff, "Donald Trump Caught on Hot Mic in 2005 Talking About Women: 'When You're a Star, They Let You Do It,'" News, Hollywood Reporter, October 7, 2016, https://www.hollywoodreporter.com/news/donald-trump-caught-hot-mic-936343.

167 Department of Homeland Security and Federal Bureau of Investigation, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*.

168 Dianne E. Rennack, *U.S. Sanctions on Russia: An Overview*, CRS Report No. IF10779 (Washington, DC: Congressional Research Service, 2018), https://www.hsdl.org/?view&did=813693.

169 Rennack.

170 Julia Ioffe, "Why Does the Kremlin Care So Much about the Magnitsky Act?," *The Atlantic*, July 27, 2017, https://www.theatlantic.com/international/archive/2017/07/magnitsky-act-kremlin/535044/.

actions as a deterrent for future Russian meddling in U.S. elections remains indeterminate. U.S. economic sanctions imposed after the annexation of Crimea did not deter Russia from its occupation of certain parts of Eastern Ukraine but may have curtailed further encroachment into Ukraine.[171]

During this period, the last transparency action from the U.S. government came on January 6, 2017, when the ODNI issued a supplemental report to the previously published GRIZZLY STEPPE report. This report aimed to lay out the U.S. government's analytical process and provide additional details justifying the attribution of election interference to the Russian Federation.[172] Unfortunately, whether this belated disclosure meaningfully affected public discourse or Americans' understanding of the activities surrounding the 2016 U.S. Elections is nebulous at best.

d. Using the Kartapolov Framework to Evaluate Russian & American Measures in 2016

As mentioned in the Research Design section, Thomas Wilhelm, Director of the U.S. Army's Foreign Military Studies Office, developed a framework to understand how asymmetric techniques fit within the Russian philosophy of warfare to achieve its goals. This framework was inspired by Wilhem's analysis of the writings and speeches of Russian Deputy Minister of Defense, Andrei V. Kartapolov.[173] Using the Kartapolov Framework offers an organized structure to evaluate the effectiveness of the Russian measures and American countermeasures. As a reminder, the relevant elements of the Kartapolov Framework for analyzing Russian social media-based influence operations against the United States are: (1) spreading discontent in the population; (2) exerting political pressure; and (3) confusing the political leadership.[174] These elements will be used to gauge the effectiveness of the Russian measures targeting the 2016 elections. In addition, the

---

171 Nigel Gould-Davies, "Russia, the West and Sanctions," *Survival* 62, no. 1 (January 2, 2020): 19, https://doi.org/10.1080/00396338.2020.1715060.

172 Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions*.

173 Wilhelm, "A Russian Military Framework," 35.

174 Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 36.

American countermeasures will be assessed in terms of their effectiveness in mitigating the aforementioned elements.

The critical elements of the Kartapolov Framework can easily be superimposed on the 2016 activities of the IRA's campaign in a step-by-step fashion.[175] The first element, spreading discontent in the population, described the IRA's precise method of targeting different demographic groups with fake content, amplifying actual user content, and purchasing advertising. Researchers concluded that IRA's tailored messaging aimed to motivate conservatives to vote while suppressing liberals, specifically black voters.[176] A record number of Americans voted in 2016, but Black voter turnout dropped from its 2012 levels.[177] Table 2 below illustrates the decreased Black voter turnout levels. The Pew Research Center said voter turnout percentages among the other racial demographics stayed about the same.[178]

Table 2. Comparison of Black Voter Turnout for Presidential Elections.[179]

Election Year	Black Voter Turnout
2012	66.6%
2016	59.6%
Change	**-7.0%**

A direct correlation between the IRA's activities and lower Black voter turnout cannot be determined within the scope of this thesis. American voters' motivations to vote

175 Wilhelm, "A Russian Military Framework," 35.

176 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 39.

177 Jens Manuel Krogstad and Mark Hugo Lopez, "Black Voter Turnout Fell in 2016, Even as a Record Number of Americans Cast Ballots," FactTank: News in the Numbers, May 12, 2017, https://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/.

178 Krogstad and Lopez.

179 Adapted from Krogstad and Lopez.

or not vote are myriad and not always easy to discern. Chryl Laird, Bowdoin College professor, suggested that Black voter turnout fell in 2016 because the Black community did not have the same incentives to vote as they did in 2008 and 2012 when there was a Black candidate for president.[180] It is still unclear whether the IRA's operation contributed to the record number of Americans voting or suppressing turnout among Black voters in 2016. What is clear is that the IRA deliberately intended to influence American voters' behavior regarding the elections and possibly eroded their faith in the electoral process.

For the second element of the framework, exerting political pressure, the IRA's efforts seemed to impact the U.S. government as its responses appeared delayed and muted. After the Senate Intelligence Committee issued its report reviewing the response of the Obama Administration to the Russian interference, Senator Richard Burr commented that they were "frozen by 'paralysis of analysis,' hamstrung by constraints both real and perceived; Obama officials debated courses of action without truly taking one."[181] In this report, the Senate Intelligence Committee noted that the FBI and DHS did not provide the general public or state and county election officials with notifications about the malicious cyber activities until the late summer of 2016.[182] Because the activities were not attributed to Russia, these notifications would not have drawn much scrutiny.[183] The third element of the framework, confusing political leadership, appeared in one of the SSCI report findings, which noted that government officials were conflicted about making public announcements for fear of feeding the political narratives about insecure or fraudulent elections.[184]

The social media companies were utterly caught by surprise and had no awareness of the malign Russian influence activities on their platforms. As such, they did not take any

---

[180] Chryl Laird, "Why Black Voter Turnout Fell in 2016," Vox, January 15, 2020, https://www.vox.com/mischiefs-of-faction/2018/1/15/16891020/black-voter-turnout.

[181] Tucker Higgins, "Obama Response to 2016 Russian Election Meddling Had 'many Flaws,' Senate Report Finds," CNBC, February 6, 2020, https://www.cnbc.com/2020/02/06/obama-response-to-2016-russian-meddling-had-many-flaws-senate-report.html.

[182] *Russian Active Measures Campaigns: Volume 1*, 4.

[183] S., *Russian Efforts against Election Infrastructure*, 4.

[184] S., *Russian Efforts against Election Infrastructure*, 4.

action against the Internet Research Agency's influence campaign in 2016. Instead, these companies allowed the IRA free rein to achieve the relevant elements of the Kartapolov Framework. However, later on, intense pressure from U.S. lawmakers and the media would eventually force the social media companies to examine what had taken place on their platforms and strive to ensure it did not happen in the future.[185]

Reviewing the U.S. government's countermeasures through the Kartapolov Framework revealed its ineffectiveness to counter the Internet Research Agency's efforts. For the first element of the framework, the IRA had an unfettered ability to conduct information operations on social media and spread discontent throughout the American population. Not until October 2016 did the U.S. government take any action. However, the one-page statement from DHS and the ODNI attributing election interference to Russia did not make an impression with Americans as news media reporting on the tawdry revelations of the Trump discussion on the Entertainment Tonight video and the hacked emails from John Podesta likely overwhelmed all other news coverage.[186]

For the second element, the Russian activities appeared to exert tremendous political pressure on the Obama White House. Multiple news media outlets reported that in the summer of 2016, President Obama was reluctant to take explicit actions because he did not want to appear to be influencing the election in favor of Clinton.[187] By the same token, the third element involved confusing the political leadership. Whether the IRA's tactics perplexed the Obama administration is moot because the delayed governmental

---

185 *Report on Russian Active Measures*; *Report of the House Permanent Select Committee*; March 20, 2017; *Russian Active Measures Campaigns: Volume 1*; *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, S.Rpt. 115–21 (Washington, DC: Government Publishing Office, 2018), https://www.hsdl.org/?view&did=806949; *Mass Violence, Extremism, and Digital Responsibility: Hearing before the Committee on Commerce, Science, and Transportation*, Senate, 116th Cong., 1st sess., September 18, 2019, https://www.commerce.senate.gov/2019/9/mass-violence-extremism-and-digital-responsibility.

186 Devlin Barrett and Damian Paletta, "FBI Suspects Russia in Hack of John Podesta Emails," *Wall Street Journal*, October 12, 2016, https://www.wsj.com/articles/top-russian-officials-shift-away-from-denying-dnc-hack-1476295233; THR Staff, "Donald Trump Caught on Hot Mic in 2005 Talking About Women."

187 Philip Ewing, "FACT CHECK: Why Didn't Obama Stop Russia's Election Interference In 2016?," National Public Radio, February 21, 2018, https://www.npr.org/2018/02/21/587614043/fact-check-why-didnt-obama-stop-russia-s-election-interference-in-2016.

response represented the result that the Russians would have desired. The U.S. government's actions in the form of the FBI/DHS joint report detailing Russian activities and the Treasury Department's economic sanctions did not come until well after the elections had already been decided. The U.S. Intelligence Community assessed that Putin and Russia perceived their ability to shape the American discourse and influence the outcome of the 2016 U.S. Elections to be at least a "qualified success" and that there would be little negative impact to continuing their online operations.[188]

Evaluating the Russian and American efforts using the Kartapolov Framework for this period revealed that Russia was the ultimate winner of the 2016 U.S. elections. The IRA's social media campaign had fulfilled the Kartapolov Framework's core tenets of spreading discontent in the population, exerting political pressure, and confusing political leadership.[189] The American efforts ranged from non-existent, in the case of the social media companies, to ineffective, in the case of the U.S. government.

2. What Happened During the 2018 U.S. Midterm Elections?

After the 2016 U.S. Elections, the Internet Research Agency's online operations continued unabated through the 2018 U.S. Elections.[190] Analyzing the IRA's activities and the countermeasures taken by the private sector companies and the U.S. government revealed how their tactics have evolved. The effectiveness of the Russian and American measures was evaluated using the Kartapolov Framework.

a. The IRA's Social Media Activities

Despite being outed by the media and the U.S. government in late 2016, the IRA appeared to operate without interruption at almost the same levels in 2017 and 2018. This success indicated that the IRA continued to be a well-financed organization and a

188 Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions*, 5.

189 Wilhelm, "A Russian Military Framework," 35.

190 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3.

seemingly worthwhile investment for Yevgeniy Prigozhin, Putin's close ally.[191] The IRA's financial strength is shown in Table 3. Given the power structure in Russia, Putin likely knew of and approved of these activities.[192] From his perspective, Putin had won the battle of 2016 and wanted to continue the social media campaign as part of the ideological struggle between Russia and the United States.[193]

Table 3. IRA Spending Plan for 2017 and 2018.[194]

Year	Budget
2017	$12,000,000
2018	$10,000,000 (January through June)

Oxford researcher Philip Howard observed the IRA taking advantage of prominent events by timing its online advertising purchases to coincide with events such as the announcement of the Trump tax plan and U.S. military strikes in Afghanistan and Syria.[195] This development may suggest the IRA had honed its skills to cater to the users it engaged. A second reason could be that the IRA shifted much of its social media activities from Facebook to Instagram. Because Instagram is more image-focused, it could be more conducive to the meme operations which the IRA appeared to favor. In addition, Instagram recognized the importance of meme campaigns and hired a manager focused solely on the

191 Peter Laurence, "Powerful 'Putin's Chef' Cooks up Murky Deals," *BBC News*, November 4, 2019, Online edition, sec. Europe, https://www.bbc.com/news/world-europe-50264747.

192 *Report on Russian Active Measures*, 1.

193 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 99.

194 Adapted from DiResta et al., *The Tactics & Tropes of the Internet Research Agency*; Department of Justice, "Russian National Charged with Interfering in U.S. Political System," United States Attorney's Office Eastern District of Virginia, October 19, 2018, https://www.justice.gov/usao-edva/pr/russian-national-charged-interfering-us-political-system.

195 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3.

meme community.[196] Lastly, DiResta stated that groups of low-paid workers, known as click farms, could have been used by the IRA to fraudulently make their Instagram accounts more prominent than they otherwise would have been through organic user engagement.[197]

An analysis of the IRA's Twitter activities from 2014 to 2018 uncovered the sophistication used to target distinct online communities. Specifically, the IRA targeted people from different demographic groups based on their political issues of interest[198] Approximately half of all the tweets from the IRA-controlled accounts happened in 2017.[199] This targeted approach indicated a certain mastery of the platform and seemed to be focused on fomenting dissension among the different groups identified by the IRA.

The IRA continued using online advertising through 2017 before social media companies adjusted their ad purchasing policies, effectively shutting them out.[200] Thus, at least through 2017, the IRA's tactics appeared to be relatively unchanged. Ostensibly, the IRA's continued social media activities on these platforms were meant to set the stage for influencing voter opinions and turnout ahead of the 2018 U.S. Midterm Elections and beyond.

b. Private Sector Countermeasures

Before the 2018 U.S. Midterm Elections, Facebook, Google, and Twitter announced they had taken substantive actions and policy changes to address malign foreign influence and election integrity issues on their platforms.[201] These actions seemed to be

196 Heather Leighton, "For Instagram's 10th Birthday, Experts Predict The Future Of Meme Culture," *Forbes*, October 7, 2020, https://www.forbes.com/sites/heatherleighton/2020/10/07/for-instagrams-10th-birthday-experts-predict-the-future-of-meme-culture/.

197 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 8.

198 Freelon and Lokot, "Russian Disinformation Campaigns on Twitter Target Political Communities across the Spectrum. Collaboration between Opposed Political Groups Might Be the Most Effective Way to Counter It.," 3.

199 Freelon and Lokot, 3.

200 Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security"; Twitter, "Elections Integrity."

201 Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security"; Twitter, "Elections Integrity."

focused on security and transparency measures. Facebook and Twitter appeared to be the most detailed in sharing their changes and the most public about account takedowns. A possible reason could be that Facebook and Twitter faced more Congressional scrutiny than Google as their senior executives testified before Congress on three separate occasions before the midterm elections.[202] In one of the hearings, Google was also in attendance but appeared more circumspect about account takedown notifications because it did not observe as many IRA-controlled accounts on YouTube.[203] In fact, Google only announced the takedown of one IRA-controlled YouTube account ahead of the 2018 midterm elections.[204]

Facebook stated it took a series of measures to protect its platform: (1) "better collaboration with governmental, non-governmental, and technology companies to identify and disrupt new threats; (2) hiring fact-checking organizations to review content and; (3) improved technological methods for detecting fake accounts."[205] Facebook also changed its advertising purchasing policies to make the buyers transparent and maintains a library of purchased political advertisements. Most notably, Facebook began to publicize its detection and takedowns of fake accounts and pages. In 2018, Facebook announced three takedowns totaling 597 Facebook pages, 287 Facebook accounts, and 99 Instagram accounts.[206] Thus, whether bowing to political pressure or genuinely wanting to reform, Facebook appeared to take tangible actions to combat foreign influence campaigns.

Google and Twitter also took countermeasures ahead of the 2018 U.S. midterm elections. For example, Google announced improved cybersecurity measures to protect

---

[202] Kang, Fandos, and Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill"; Tony Romm, "5 Things We Learned When Facebook, Google, and Twitter Testified to Congress About Russia's Election Meddling," Recode Daily, October 31, 2017, https://www.vox.com/2017/10/31/16588032/facebook-google-twitter-congress-russia-election-2016-tech-hearings-franken-cruz-graham; Katy Steinmetz, "Lawmakers Hint at Regulating Social Media During Hearing with Facebook and Twitter Execs," *Time*, September 5, 2018, https://time.com/5387560/senate-intelligence-hearing-facebook-twitter/.

[203] Kang, Fandos, and Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill."

[204] Google Threat Analysis Group, "Google Safety & Security."

[205] Facebook, "Facebook - Preventing Election Interference."

[206] Facebook.

political campaigns and their platforms.[207] During the same year, Twitter indicated its efforts included improving its algorithms to detect and takedown social media bots, establishing an internal cross-functional team to handle foreign influence threats, modifying its advertising policies to promote buyer transparency, updating its terms of service to ban all inauthentic behavior, and enhancing the security configuration settings for the application programming interface.[208] In addition, Twitter highlighted its intelligence sharing with Jigsaw, Google, other social media companies, and law enforcement agencies.[209] In October 2018, Twitter released an archive of foreign-influence-related account information so "members of the public, governments, and researchers can investigate, learn, and build media literacy capacities for the future."[210] In 2018, Twitter announced the takedown of 3,613 IRA-associated accounts.

On the one hand, Google's response to the Russian influence campaigns appeared to be subdued, likely because YouTube had not played a significant role in the IRA's playbook for 2016. For example, Howard noted that Google only provided 228 YouTube 2016 election-related videos to the Senate Intelligence Committee, and each video was viewed about 1,500 times or less.[211] On the other hand, Twitter's response was similar to Facebook's and made substantive efforts to combat malign foreign influence on its platform. As a result, the number of accounts taken down by Facebook and Twitter in 2018 was roughly commensurate with the number of accounts discovered after the 2016 U.S. elections. The reason for this disparity in the number of IRA accounts on each platform is indeterminate.

---

[207] Google Threat Analysis Group, "Google Safety & Security."

[208] Carlos Monje Jr., "2018 U.S. Midterm Elections Review," *Twitter Company* (blog), January 31, 2019, https://blog.twitter.com/en_us/topics/company/2019/18_midterm_review.html.

[209] Twitter, "Elections Integrity."

[210] Twitter, "Retrospective Review Twitter, Inc. and the 2018 Midterm Elections in the United States," Twitter, February 4, 2019, https://blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf.

[211] Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 7, 11.

c. U.S. Government Countermeasures

Before the 2018 U.S. midterm elections, the U.S. government took a series of public actions to address Russia's interference in the 2016 U.S. elections and put countermeasures in place to ensure better protection in subsequent elections. These actions comprised both transparency and security measures. Transparency-focused efforts aimed to inform the American electorate about what happened in 2016 and was still occurring. Jennifer Hochschild, a Harvard College professor, believed "democracies thrive best…if citizens have a broad education and some level of political knowledge."[212] Americans should have access to information that is free of corrupt foreign influence to inform their voting. The security-focused actions were intended to deter and punish Russian interference in the U.S. electoral process or safeguard their intended targets. These actions took the form of Congressional hearings, an FBI initiative, multiple indictments, economic sanctions, and other operations. Unlike in the lead-up to the 2016 U.S. elections, the U.S. government was very active and public in enacting countermeasures before the 2018 U.S. midterm elections. These actions are described below in chronological order.

On August 31, 2017, the State Department announced the closures of the Russian Consulate in San Francisco and annexes in New York City and Washington, D.C.[213] These closures were taken in response to Russia reducing the size of the American workforce at the U.S. Embassy in Moscow, which was perceived as a retaliatory measure for the United States sanctioning multiple Russians in December 2016 for their interference in U.S. Elections.[214]

On October 31, 2017, the Senate Judiciary Committee held a hearing with senior executives from Facebook, Google, and Twitter to discuss the extent of the Russian disinformation campaigns on their respective platforms.[215] This public hearing was one

---

[212] Jennifer Hochschild, "If Democracies Need Informed Voters, How Can They Thrive While Expanding Enfranchisement?," *Election Law Journal: Rules, Politics, and Policy* 9, no. 2 (2010): 111–23.

[213] Department of State, "Senior Administration Official on Russia," U.S. Department of State, August 31, 2017, https://2017-2021.state.gov/senior-administration-official-on-russia/.

[214] Rennack, *U.S. Sanctions on Russia*.

[215] Romm, "5 Things We Learned When Facebook, Google, and Twitter Testified to Congress About Russia's Election Meddling."

of America's first opportunities to hear about what happened from the U.S. social media companies. It also provided politicians with the occasion to exert pressure on the companies to make constructive changes to their platforms.

In December 2017, Congress reestablished the Global Engagement Center (GEC) as an agency within the State Department responsible for countering foreign state and non-state propaganda and disinformation operations.[216] Previously, the GEC was established under Executive Order 13721 in the Obama administration to counter foreign terrorist propaganda and online recruitment efforts.[217] It would later pivot to focusing on exposing foreign state disinformation campaigns.

On January 29, 2018, the FBI announced its Protected Voices Initiative. FBI Director Christopher Wray said it "provides tools and resources to political campaigns, companies, and individuals to protect against online foreign influence operations and cybersecurity threats."[218] Under the auspices of the initiative, the FBI provided cybersecurity briefings to, and stayed engaged with, the national-level political organizations. This security-based countermeasure was focused on protecting one of the primary targets for Russian information operations.

On February 16, 2018, the Special Counsel's Office indicted Yevgeniy Prigozhin and 12 employees of the IRA with eight criminal counts for their efforts to interfere in the 2016 U.S. Elections.[219] The unsealed indictment affidavit offered the first opportunity for the American public to learn about the extent of the scope and scale of the Russian influence operation. The unsealed indictment affidavit described in evidence-based detail what the IRA had propagated on social media against the American public. The accompanying arrest warrants showed the U.S. government's intention to bring these Russians to face justice at some point.

---

216 Matthew Weed, *Global Engagement Center: Background and Issues*, CRS Report No. IN10744 (Washington, DC: Congressional Research Service, 2017), 2, https://fas.org/sgp/crs/row/IN10744.pdf.

217 Weed, 2.

218 Federal Bureau of Investigation, "Protected Voices."

219 U.S. vs. Internet Research Agency LLC.

On March 28, 2018, the Department of Treasury levied sanctions against 16 Russian nationals for election interference-related activities. These included some of the individuals mentioned above whom the Special Counsel's Office previously indicted. In addition, on June 11, 2018, another eight Russian nationals were sanctioned for associated activities.[220] These were another set of measures likely designed to inflict punishment on the Russian actors and act as a deterrent for future activities targeting U.S. elections.

On April 10–11, 2018, the Senate Commerce Committee and Senate Judiciary Committee held hearings on consecutive days with Mark Zuckerberg to discuss Russia's influence campaigns on Facebook and its countermeasures to combat them.[221] This hearing provided the American public with the opportunity to listen to one of the primary architects of the current social media landscape in the United States. The Senate committees also used this as an opportunity to hold Facebook accountable for its actions and exert pressure for positive change.

On July 17, 2018, the House Judiciary Committee held a hearing with senior executives from Facebook, Google, and Twitter so they could provide updates on their companies' efforts for content filtering to stop foreign influence campaigns on their platforms.[222] On September 5, 2018, the Senate Intelligence Committee held a hearing with senior executives from Facebook and Twitter to discuss their companies' efforts to stop foreign influence campaigns and illegal transactions on their platforms.[223] Both of these hearings were additional occasions for Americans to learn about social media companies' progress in safeguarding the upcoming election.

---

220 Rennack, *U.S. Sanctions on Russia*.

221 Mike Snider, "What's at Stake for Facebook's Mark Zuckerberg as He Testifies for Day 2," *USA Today*, April 10, 2018, https://www.usatoday.com/story/tech/news/2018/04/10/whats-stake-facebooks-mark-zuckerberg-he-testifies-before-congress/503017002/.

222 *Facebook, Google, and Twitter: Examining the Content Filtering Practices of Social Media Giants, House of Representatives*, House of Representatives, 115th Cong., 1st sess., July 17, 2018, 2, https://www.hsdl.org/?view&did=821944.

223 Steinmetz, "Lawmakers Hint at Regulating Social Media During Hearing with Facebook and Twitter Execs."

On October 19, 2018, the IRA's chief accountant, Elena Alekseevna Khusyaynova, was indicted by the U.S. Attorney's Office for the Eastern District of Virginia because of her role in the conspiracy to interfere with the U.S. political system, to include the 2016 and 2018 U.S. elections.[224] Khusyaynova's unsealed indictment affidavit revealed the extent of the IRA's financial transactions as the group waged its influence campaign against the United States.[225] Moreover, as she is a regular Russian citizen without the privileges typical to Russian oligarchs or diplomats, her indictment may deter other Russians from working for the IRA or similar types of companies.

The Washington Post reported that U.S. Cyber Command conducted an offensive cyber operation on November 2, 2018, against the St. Petersburg-based IRA office, a day before the U.S. Midterm Elections.[226] This operation was believed to have knocked out the IRA's computer networks for days. If true, this operation showed that the U.S. government was willing to reveal and deploy its technical capabilities to safeguard the integrity of the electoral process.

On November 16, 2018, Congress enacted the Cybersecurity and Infrastructure Security Agency Act of 2018. This legislation created the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security.[227] In January 2017, DHS designated the election system infrastructure as the 17th critical infrastructure sector. CISA is the U.S. government agency charged with helping state and local governments secure America's election systems.[228] Both security-focused actions showed that the U.S.

---

224 Department of Justice, "Russian National Charged with Interfering in U.S. Political System."

225 Department of Justice.

226 Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

227 "Cybersecurity and Infrastructure Security Agency Act of 2018," Pub. L. No. 115–278, Public Law 20 (2018), https://www.hsdl.org/?view&did=829787.

228 Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Security," Cybersecurity and Infrastructure Security Agency, accessed June 3, 2020, https://www.cisa.gov/election-security.

government perceives elections are vital to national security and requires consolidating a host of protective cyber functions into one federal agency.

In contrast to the 2016 U.S. elections, the executive and legislative branches of the U.S. government were active ahead of the 2018 elections as it took a series of security measures to shore up vulnerabilities in the different facets of the democratic process, such as providing cybersecurity briefings for political organizations, and enhance transparency about governmental actions to inform the American public, through the many Congressional hearings, law enforcement actions, and economic sanctions.

d. Using the Kartapolov Framework to Evaluate Russian and American Measures in 2018

For the 2018 U.S. elections, the Kartapolov Framework was used to evaluate the effectiveness of the Russian actions, primarily through the efforts of the Internet Research Agency. It was also used to determine the efficacy of the American efforts, both private sector and governmental, to counter each element of the framework. As a reminder, the relevant elements of the framework for this evaluation are: (1) spreading discontent in the population; (2) exerting political pressure; and (3) confusing the political leadership.[229]

After the 2016 U.S. elections, multiple researchers determined that the Internet Research Agency continued at the same cadence and volume of activity as before, seemingly undeterred by being outed in the news media and through government communications.[230] The New Knowledge and Oxford University researchers noted that the Internet Research Agency used meticulous precision to identify different demographic groups by race and political affinities to amplify dissension with its online messaging.[231] Another purpose of the IRA's messaging was to promote right-wing voter turnout and

---

[229] Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," 36.

[230] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*; Freelon and Lokot, "Russian Disinformation Campaigns on Twitter Target Political Communities across the Spectrum. Collaboration between Opposed Political Groups Might Be the Most Effective Way to Counter It."; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*.

[231] DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 8–9; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 18.

suppress left-wing and Black voters.[232] The IRA's actions were trying to fulfill the first element of the Kartapolov Framework by trying to spread discontent in the American population. A review of the U.S. Census Bureau's analysis of the 2018 elections voter turnout revealed a mixed outcome to what the IRA would have desired. The overall voter turnout was the highest in 40 years, with 53.4 percent of eligible voters going to the polls in 2018. This turnout contrasts to the 41.9 percent who came out to the polls in 2014, which was the lowest midterm election turnout in 40 years.[233] Table 4 summarizes the increase in both Black and White voter turnout for the midterm elections. While the IRA promoted right-wing voter turnout, which are typically White voters, its efforts to suppress Black voter turnout failed.

Table 4. Voter Turnout by Demographic in Midterm Elections.[234]

Election Year	Black Voter Turnout	White Voter Turnout
2014	40.6%	45.8%
2018	51.4%	57.5%
Change	**+10.8%**	**+11.7%**

The Internet Research Agency's ongoing activities must have exerted some political pressure on the private sector and the U.S. government because of the assortment and frequency of public actions taken by both entities in the run-up 2018 U.S. elections. Thus, the IRA fulfilled the second element of the framework by applying political pressure to the American social media companies and government, but the actions taken by both entities may have blunted the effectiveness of its influence campaigns. However, it does

232 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 19.

233 Jordan Misra, "Voter Turnout Rates among All Voting Age and Major Racial and Ethnic Groups Were Higher Than in 2014," Behind the 2018 U.S. Midterm Election Turnout, April 23, 2019, https://www.census.gov/library/stories/2019/04/behind-2018-united-states-midterm-election-turnout.html.

234 Adapted from Misra.

not appear that the IRA's campaigns confused the political leadership in the United States because the different governmental countermeasures listed in the previous section seemed frequent, deliberate, and proportional.

Application of the Kartapolov Framework appeared to be more favorable to the social media companies' countermeasures during the 2018 election cycle. The framework's first element, spreading discontent in the population, was countered by the social media companies' account takedown operations. As mentioned before, Facebook and Twitter identified and shut down accounts in 2018 at about the same levels as were identified in 2016. The difference from 2016 was that the social media companies were able to disrupt the IRA's activities before the 2018 elections. The framework's second element, exerting political pressure, seemed to make the social media companies act more vigorously in policing their platforms and forthcoming in announcing any actions they took. The third element, confusing the political leadership, will be discussed in the next section when reviewing the efficacy of U.S. government countermeasures. Broadly speaking, the social media companies appeared to be better equipped and decisive in thwarting the IRA's information operations during this election cycle.

Overlaying the Kartapolov Framework's elements on the U.S. government's actions revealed a different outcome than in 2016. For the first element, spreading discontent in the population, the U.S. government showed very public attempts to educate the American public and hold Russian wrongdoing accountable. Through the Justice Department and the Treasury Department, the executive branch made public announcements of indictments and economic sanctions against Russians for their roles in election interference, respectively. In addition, the legislative branch held a series of public hearings to learn about the progress the social media companies were making to counter malign foreign influence and inform the American public.

For the second element, exerting political pressure, the U.S. government was obliged to prevent a repeat of the 2016 interference by Russia. Although difficult to determine whether the U.S. government felt political pressure from the IRA's influence campaign, it displayed a broad spectrum of countermeasures, which were listed in the prior section. Finally, for the third element, confusing the political leadership, both the executive

and legislative branches of the U.S. government appeared to be informed about the threat from Russian influence operations and took appropriate countermeasures to neutralize them.

C. CONCLUSIONS FROM THE 2016 AND 2018 ELECTIONS

In summary, a review of the recent history of Russia's actions to interfere in the U.S. election and America's actions to counter these actions revealed three conclusions. First, the Internet Research Agency was virtually unfettered in its social media campaign to sow division and confusion in the 2016 U.S. elections. Second, the U.S. government and social media companies' countermeasures against the IRA ahead of the 2018 U.S. midterm elections appeared to be generally effective. Third, the Internet Research Agency appeared to be undeterred by the American efforts and made only slight modifications in its tactics from 2016 to 2018.

Researchers have determined that Russian influence campaigns, especially those conducted ahead of the 2016 U.S. elections, can be effective for eliciting partisan responses.[235] Governmental reports, research papers, and the social media companies themselves have acknowledged that the social media companies were unaware of the Russian disinformation campaigns taking place on their platforms and therefore took no active role in countering them. Congressional report findings criticized the executive branch of the government for a tepid and ineffective response to the Russian interference activities. Analysis of voter turnout revealed a relatively high overall high voter turnout but low Black voter turnout in the 2016 elections. This combination of factors may have led to Vladimir Putin achieving his desired goals of eroding American faith in its democratic process and the election of Donald Trump.[236] Ambassador Michael McFaul noted that even if the impact of the Russian influence campaign was minimal, the margin

---

[235] Todd C. Helmus et al., *Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions* (Santa Monica, CA: RAND Corporation, 2020), 51, https://www.rand.org/pubs/research_reports/RRA704-3.html.

[236] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions*, 7.

of victory for Trump was about 78,000 votes across three states that tipped the electoral college.[237]

For the 2018 U.S. midterm elections, the combined countermeasures of the private sector and the U.S. government appeared to mitigate the effectiveness of the IRA's influence operations. On December 18, 2018, Dan Coates, Director of National Intelligence, released a press statement in which he said the "Intelligence Community does not have intelligence reporting that indicates any compromise of our nation's election infrastructure that would have prevented voting, changed vote counts or disrupted the ability to tally votes."[238] The ultimate proof was the record turnout of voters across all demographic groups, including Black voters.[239]

Director Coates stated that Russia continued to conduct influence operations after the 2016 elections ahead of the 2018 elections.[240] During this period, the IRA's only shift in tactics appeared to be jettisoning its use of online political advertisements, which was probably the result of the social media companies changing their advertising policies to make it more difficult for foreign entities to purchase advertisements.[241] However, the regular cadence of account shutdown announcements from the social media companies, reports by research firms, and U.S. government reports and statements indicated the Russians would continue to be active ahead of the 2020 U.S. elections. The uncertainty was whether the social media companies and the U.S. government would be up to the task of countering the Russian information operations.

---

237 McFaul, *Securing American Elections*, 14.

238 Office of the Director of National Intelligence, "DNI Coats Statement on the IC's Response to EO 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a U.S. Election," Office of the Director of National Intelligence, December 21, 2018, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2018/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election.

239 Misra, "Voter Turnout Rates among All Voting Age and Major Racial and Ethnic Groups Were Higher Than in 2014."

240 Office of the Director of National Intelligence, "DNI Coats Statement on the IC's Response to EO 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a U.S. Election."

241 Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security"; Twitter, "Elections Integrity."

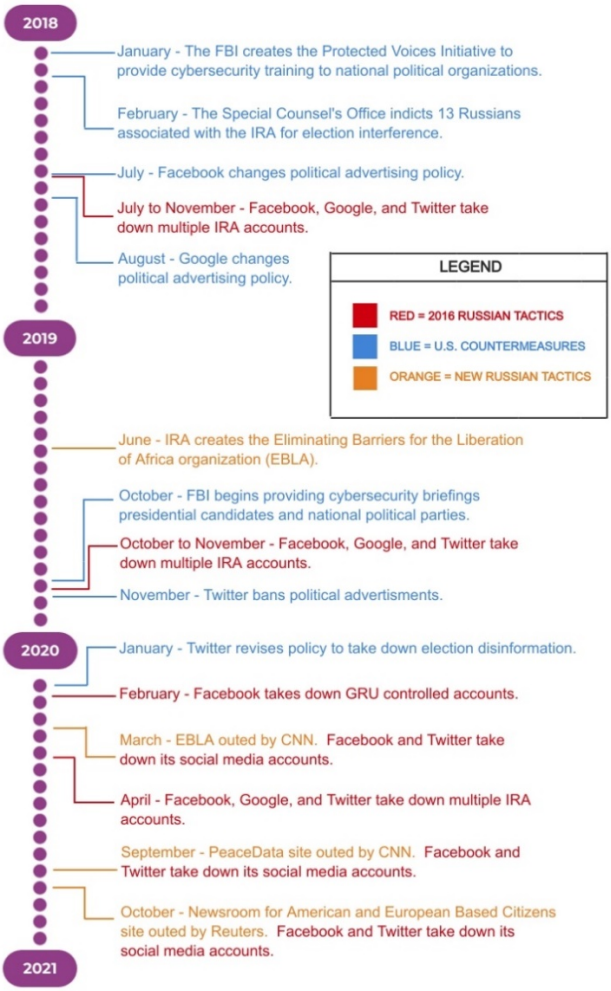
III. THE 2020 ELECTIONS – RUSSIAN GAMBIT AND AMERICAN COUNTERPLAY

> Foreign nations continue to use influence measures in social and traditional media to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord, and undermine confidence in our democratic process.
>
> — William Evanina, July 24, 2020

The elections of 2016 and 2018 put the major social media companies and the U.S. government on high alert about Russian interference. As a result, both entities were more aggressive in their efforts to thwart the Russians ahead of the 2020 elections. The social media companies partnered with the news media and research organizations to detect and disrupt these Russian disinformation operations. The U.S. government's endeavors included law enforcement actions, threat briefings, and information sharing to the private sector. The cumulative effect of American countermeasures compelled the Russians to evolve their tactics and methods to evade detection continually. Ultimately, the American actions appeared effective in mitigating the Russian online tactics because voters were undeterred and turned out in record numbers for the election.

This chapter reviews the Russian disinformation campaign targeting the 2020 U.S. elections, the countermeasures taken by the social media companies and the U.S. government. It then uses the Kartapolov Framework to evaluate the efficacy of those countermeasures, informing recommendations for counteracting future Russian disinformation campaigns in the next chapter. Finally, figure 5 provides some key highlights of the Russian and American actions after the 2018 midterms to the 2020 elections.

Figure 5. Highlights of Russian and American Actions from 2018 to 2020.[242]



[242]Adapted from Federal Bureau of Investigation, "Protected Voices"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive," *Twitter Information Operations* (blog), October 8, 2020, https://blog.twitter.com/en_us/topics/company/2020/disclosing-removed-networks-to-our-archive-of-state-linked-information.html; Facebook, "Facebook - Preventing Election Interference"; Facebook, "October 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), October 27, 2020, https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-mexico-iran-myanmar/; Federal Bureau of Investigation, "Combating Foreign Influence," What We Investigate, accessed October 18, 2020, https://www.fbi.gov/investigate/counterintelligence/foreign-influence; Lauren Feiner and Megan Graham, "Twitter Unveils Final Details for Political Ad Ban, but It's Still Looking Murky," CNBC, November 15, 2019, https://www.cnbc.com/2019/11/15/twitter-unveils-new-political-ad-policy.html; Google Threat Analysis Group, "TAG Bulletin: Q4 2020," Google: Updates from Threat Analysis Group, November 17, 2020, https://blog.google/threat-analysis-group/tag-bulletin-q4-2020/; Google Threat Analysis Group, "Google Safety & Security"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

A. THE IRA AND OTHER PROXIES' SOCIAL MEDIA ACTIVITIES

From 2019 through 2020, the major social media companies reported most of the IRA's activities with a couple of exceptions. On at least a quarterly basis, Facebook, Google, and Twitter made announcements regarding the detection and takedown of fake Russian accounts on their platforms via blogposts. In addition, many of the IRA-related activities involved account takedowns in various geographical locations, not just Russia-based accounts. The exceptions to the major social media companies reporting Russian account takedowns came when other organizations were able to identify and expose the activities of the Internet Research Agency. In one instance, CNN broke a story about the IRA's activities in March 2020.[243] In a second instance, Graphika, a New York-based social media analysis company, issued reports on IRA activities and identified another cluster of Russia-controlled campaigns it dubbed "Secondary Infektion."[244] These account takedowns appeared to be coordinated across different organizations as Facebook and Twitter made their own announcements after the reporting by CNN and Graphika.

Different Russian proxy organizations focused on specific voting groups to affect their attitudes. For example, the Internet Research Agency established a front organization called Eliminating Barriers for the Liberation of Africa (EBLA) with offices in Western Africa.[245] On March 12, 2020, CNN exposed EBLA when it televised a news story with an associated news article about EBLA being a Russian troll farm.[246] Through its investigation, CNN determined the head of EBLA was a Russian-speaking Ghanaian named Seth Wiredu, who called himself "Mr. Amara" and registered the organization in June 2019.[247] CNN assessed he was being funded through Yevgeniy Prigozhin's Project Lakhta. Wiredu managed offices outside Accra, Ghana, and Lagos, Nigeria, with

---

[243] Clarissa Ward et al., "Russian Election Meddling Is Back — Via Ghana and Nigeria — and in Your Feeds," CNN, April 11, 2020, https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html.

[244] Ben Nimmo et al., *Secondary Infektion* (New York: Graphika, 2020), https://secondaryinfektion.org/report/secondary-infektion-at-a-glance/.

[245] Ward et al., "Russian Election Meddling Is Back."

[246] Ward et al.

[247] Ward et al.

employees who portrayed themselves as African Americans and engaged in social media activities.[248] The EBLA employees focused primarily on racial issues such as police brutality, displays of anger towards white people, and black empowerment.[249] Figure 6 provides an example of the types of postings put out by EBLA. In a similar fashion to the IRA's operations in St. Petersburg, the EBLA employees received assignments on different themes, coordinated their postings, and worked on cross-platform campaigns.[250] Before it was outed, the EBLA organization appeared to be laying the groundwork for influencing the behavior of Black voters ahead of the 2020 U.S. elections.

Figure 6. An Image from a Facebook Account Controlled by EBLA.[251]

Although the Russians tried to evolve their tactics to evade detection by the social media companies, the effort failed because the social media companies partnered with other

248 Ward et al.

249 Ward et al.

250 Ward et al.

251 Source: Ward et al.

organizations to detect and expose the Russians. One example highlighted this collaboration. On September 1, 2020, Facebook and Twitter announced that they had identified and taken down social media accounts associated with an English and Arabic language website called "PeaceData," which portrayed itself as a progressive-leaning independent news site.[252] Figure 7 shows two postings from the PeaceData site.

In coordination with Facebook, Graphika issued a report on PeaceData, which provided detailed information about the site itself, an analysis of images on the site, and the site's writers.[253] This development was notable for four reasons. First, the site was an example of the IRA shifting content off the social media platforms to a website which it controlled. Second, Graphika analyzed the profile photos of several PeaceData staff members and determined they were created through generative adversarial networks (GANS), which is a type of artificial intelligence.[254] These photos were the first known instance of the IRA using artificial intelligence to generate phony images of people. Examples of these GANS-generated profile photos appear in Figure 8. Third, Reuters broke a story about the IRA posing as PeaceData staff to hire unwitting freelance journalists, including Americans, to write articles for the site.[255] The Carnegie Endowment for International Peace determined that at least 20 freelance journalists had been duped into writing articles for the PeaceData outlet.[256] This instance is the first identified example of the IRA hiring unwitting individuals to generate content on its behalf. Fourth, Facebook shared information about the PeaceData site and associated social media networks with

252 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive," Social Media, *Twitter Information Operations* (blog), September 1, 2020, https://twitter.com/TwitterSafety/status/1300848632120242181; Facebook, "September 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), September 2020, https://about.fb.com/wp-content/uploads/2020/10/September-2020-CIB-Report.pdf.

253 Nimmo et al., "IRA Again: Unlucky Thirteen."

254 Nimmo et al., 6.

255 Jack Stubbs, "Duped by Russia, Freelancers Ensnared in Disinformation Campaign by Promise of Easy Money," Reuters, September 3, 2020, https://www.reuters.com/article/us-usa-election-facebook-russia-idUSKBN25T35E.

256 Alicia Wanless and Laura Walters, "How Journalists Become an Unwitting Cog in the Influence Machine," Carnegie Endowment for International Peace, October 13, 2020, https://carnegieendowment.org/2020/10/13/how-journalists-become-unwitting-cog-in-influence-machine-pub-82923.

Graphika.[257] This collaboration revealed Facebook joining forces with a non-social media company third party to analyze its findings.

Figure 7. Postings from the PeaceData Site.[258]

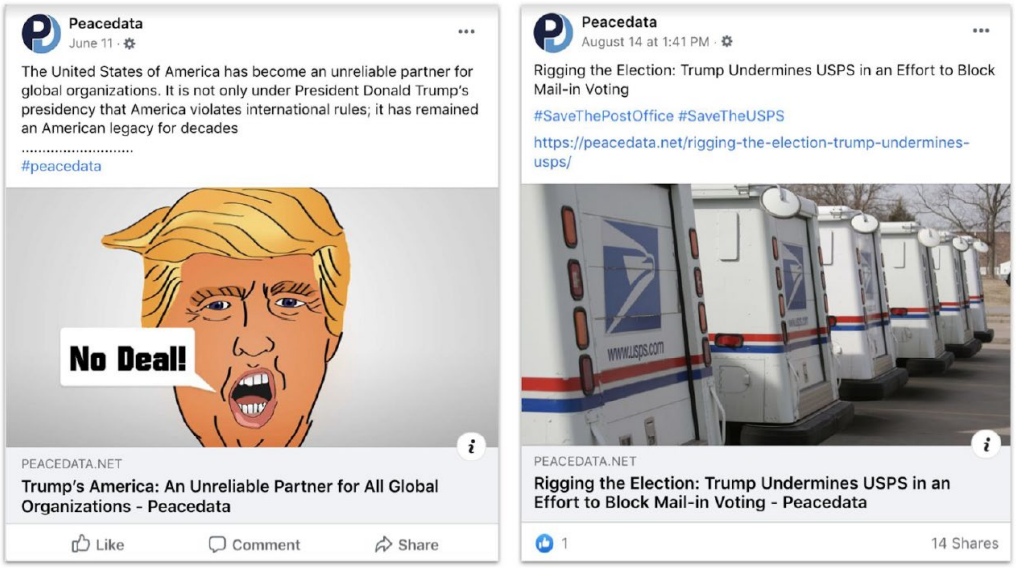
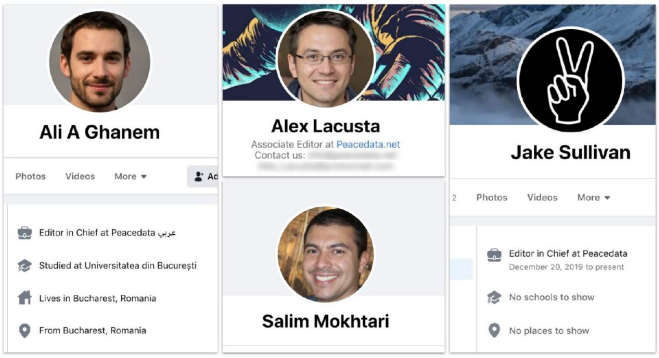


Figure 8. Photos of PeaceData Staff Created by Artificial Intelligence.[259]



257 Nimmo et al., "IRA Again: Unlucky Thirteen," 1.

258 Source: Nimmo et al., 20.

259 Source: Nimmo et al., 5.

The Russians continued to demonstrate different tactics such as using alternative communication platforms, artificial intelligence to generate false personas, and unwitting co-optees to avoid detection by the social media companies and the U.S. government. Not only did the Russians use the PeaceData site to appeal to progressives, but they also created another site called the Newsroom for American and European Based Citizens (NAEBC) to appeal to conservatives.[260] On October 1, 2020, Reuters published an article that exposed NAEBC as another news outlet run by the IRA, which appeared to be the ideological counterpart of the PeaceData outlet.[261] Figure 9 shows an example of a posting on NAEBC. Figure 10 shows an example of cross-posting of NAEBC content on Gab.

The NAEBC site was noteworthy for three reasons. First, in addition to the mainstream social media platforms of Facebook, Twitter, and LinkedIn, the IRA used two right-wing social media platforms, Gab and Parler, to disseminate content from NAEBC.[262] Second, Figure 11 shows that the IRA continued using GANS-generated staff profile photos on NAEBC to convey a sense of authenticity.[263] Lastly, Graphika determined that the IRA used various social media accounts to engage with real users and convince them to post on the NAEBC site, which met with some success.[264] However, Graphika assessed that both the PeaceData and NAEBC outlets had limited influence because they were created around June 2020 and taken down by September 2020 before either could generate much viewership.[265] Furthermore, Graphika opined that the purpose for both the websites was two-fold. First, the sites wanted to influence voter turnout through the type of content on each site. For example, on the PeaceData site, Graphika believed articles denigrating Joe Biden compared to other Democratic candidates would

---

[260] Stubbs, "Exclusive."

[261] Graphika Team, *Step Into My Parler; Suspected Russian Operation Targeted Far-Right American Users on Platforms Including Gab and Parler, Resembled Recent IRA-Linked Operation That Targeted Progressives* (New York: Graphika, 2020), 1, https://graphika.com/reports/step-into-my-parler/.

[262] Graphika Team, 16.

[263] Graphika Team, 20.

[264] Graphika Team, 23–26.

[265] Graphika Team, 26.

suppress Democratic voter turnout.[266] Second, the content on both PeaceData and NAEBC was meant to inflame existing discord within their viewership.[267]

Figure 9. Posting from the NAEBC Site.[268]

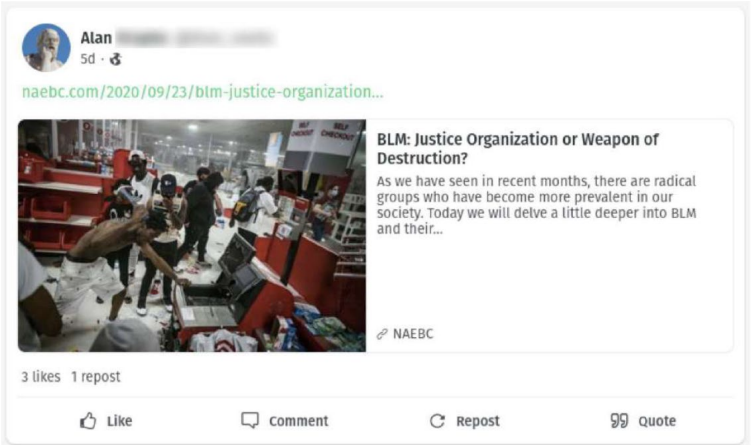
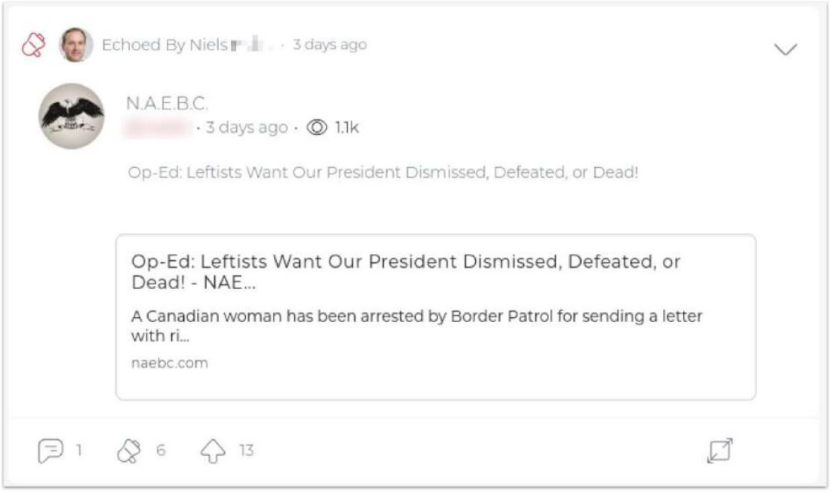


Figure 10. NAEBC Cross-platform Posting on Parler.[269]



266 Graphika Team, 34.

267 Graphika Team, 34.

268 Source: Graphika Team, 8.

269 Source: Graphika Team, 9.

Figure 11. GANS-generated Profile Photos for NAEBC Staff.[270]

The Russians targeted the far-right channels as well as the mainstream ones to reach different target audiences. In addition to its work analyzing the aforementioned IRA activities, Graphika conducted an independent investigation into another Russian information operation dubbed "Secondary Infektion."[271] Graphika determined this group has been active from 2014 to at least the beginning of 2020 and characterized the online campaigns as focusing on misinformation about foreign policy and diplomacy-related matters.[272] Although the content appeared in multiple languages, Graphika deduced the campaigns focused on targeting viewers in Europe and North America.[273] Its analysis of the top themes in the content revealed that the articles primarily concentrated on denigrating Ukraine, the United States, NATO, and sowing discord in the rest of Europe.[274] Figure 12 shows the breakdown of articles by quantity and topic. Thus, the Russians had expanded far beyond using the Internet Research Agency as a proxy for its disinformation campaigns.

[270] Source: Graphika Team, 20.

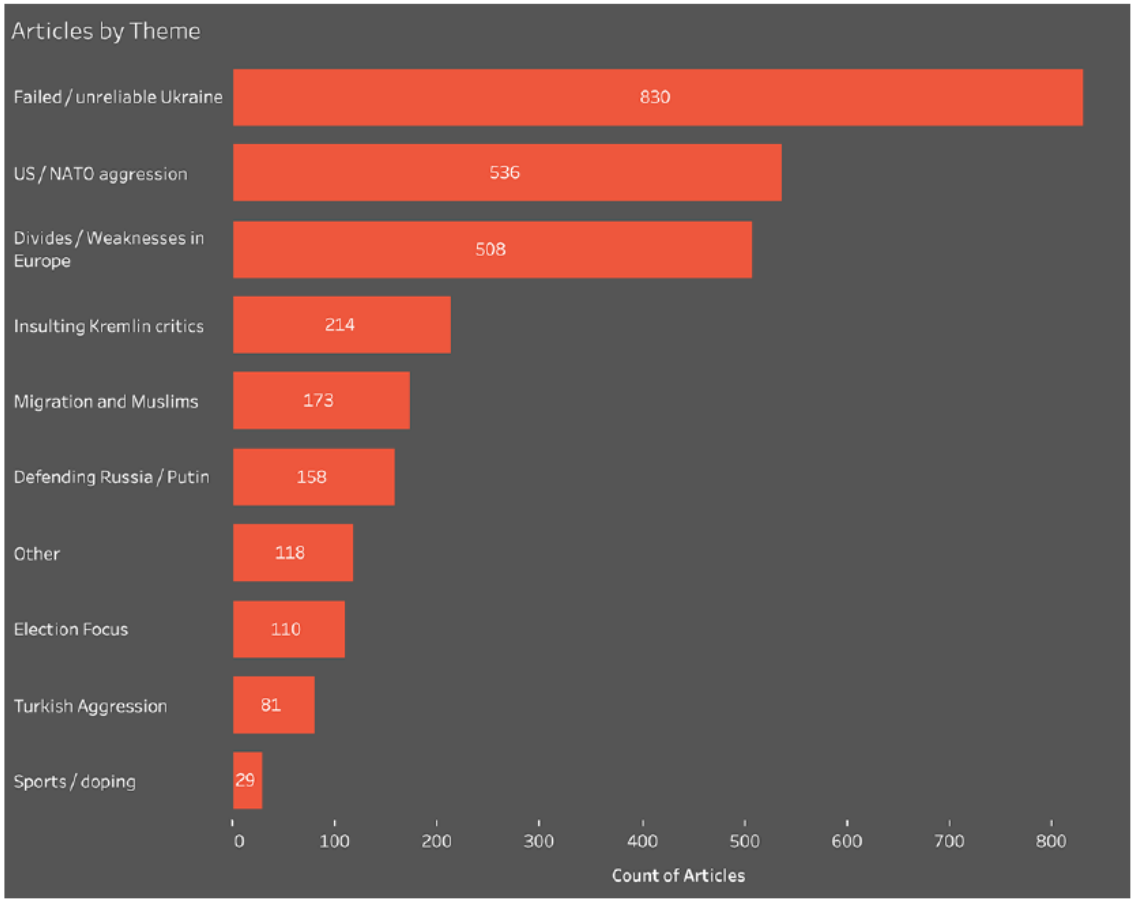
[271] Nimmo et al., *Secondary Infektion*.

[272] Nimmo et al., 4.

[273] Nimmo et al., 11.

[274] Nimmo et al., 14.

Figure 12. Breakdown of Secondary Infektion Articles by Topic.[275]



Secondary Infektion had two features that distinguished it from the other IRA-controlled campaigns. First, the actors behind Secondary Infektion made extensive use of forged postings and documents in an attempt to proliferate disinformation and propagate conflict.[276] Second, Graphika observed that Secondary Infektion used a wide-ranging set of online platforms, especially micro-blogging sites, to disseminate content, not only the mainstream social media platforms.[277] Examples of a forged post and forged document

[275] Source: Nimmo et al., 14.

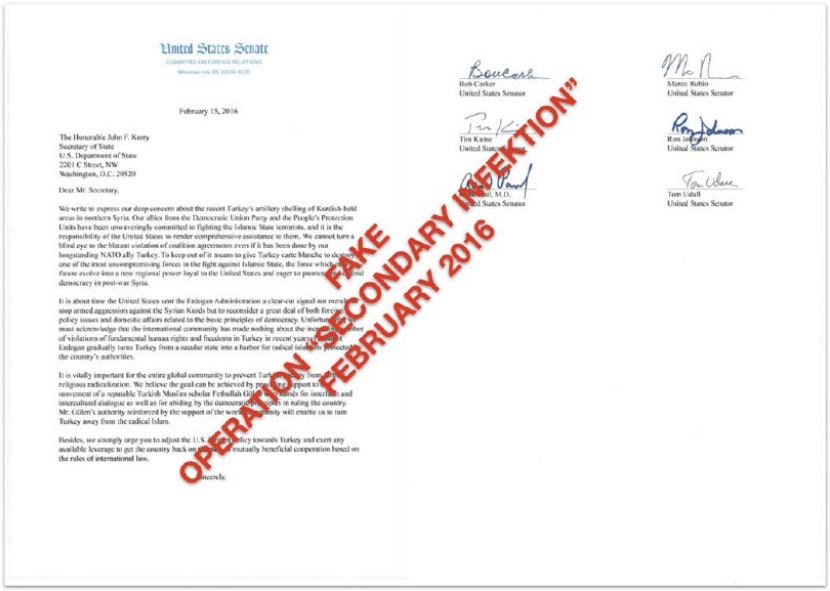
[276] Nimmo et al., 4.

[277] Nimmo et al., 8.

are shown in Figures 13 and 14, respectively. The Russians extended their reach across multiple channels and platforms by agilely adapting their tactics.

Figure 13. Secondary Infektion-made Forged Posting from Marco Rubio.[278]

Figure 14. Secondary Infektion-made Forged Letter to John Kerry.[279]



278 Source: Nimmo et al., 5.

279 Source: Nimmo et al., 6.

By being everywhere simultaneously, the Russians effectively reduced the likelihood of being shut down, given the reach of their operations. In discussion with some social media companies, Graphika believed the extensive variety of sites used by Secondary Infektion could be related to operational security.[280] Specifically, this type of behavior would reduce the impact of takedowns by any one company and make coordinated takedowns more difficult across multiple companies.[281] The social media companies told Graphika that the actors behind the Secondary Infektion activities used good security practices because they were consistent and disciplined about using "burner" accounts, which were registered, used to create a series of posts, and then abandoned within the day.[282] Graphika and the social media companies determined that Russian operators conducted Secondary Infektion. Still, they could not determine whether the campaign was associated with the IRA, GRU, or other Russia-based groups.[283] The Secondary Infektion campaigns were another example of the Russians trying to adjust their tactics to avoid detection by the social media companies.

B. PRIVATE SECTOR COUNTERMEASURES

Ahead of the 2020 U.S. elections, the major social media companies, consisting of Facebook, Google, and Twitter, continued their transparency efforts by regularly providing public notifications of foreign influence-related account takedowns. These notifications typically provided summaries of the activities the companies identified, the number of accounts taken down, and how these accounts violated their terms of service. In addition, all three companies published security measures regarding technology improvements and policy changes on their platforms ahead of the elections.[284]

---

[280] Nimmo et al., 8.

[281] Nimmo et al., 8.

[282] Nimmo et al., 8.

[283] Nimmo et al., 11.

[284] Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security"; Twitter, "Elections Integrity."

In 2019, Facebook announced two sets of takedowns. First, on October 21, 2019, it removed 50 Instagram and one Facebook account, which originated from Russia and focused on American users. Then, on October 30, 2019, Facebook removed five Instagram accounts, 35 Facebook accounts, 53 Pages, and seven Groups, which originated from Russia and focused on users in African countries (Cameroon, Côte d'Ivoire, the Democratic Republic of the Congo, Mozambique, Central African Republic, and Madagascar).[285] These actions showed that the IRA's activities persisted and expanded into targeting different countries and that Facebook was actively monitoring its platform and taking efforts to disrupt the IRA.

Social media companies uncovered even deeper links to Russia. In 2020, Facebook announced six sets of takedowns. All of them are summarized in Table 5. In contrast to 2016, when 470 IRA accounts were identified, Facebook identified and shut down 825 accounts in 2020. In one noteworthy takedown, Facebook discovered Facebook accounts, pages, and groups controlled by the GRU, targeting Ukraine and other Eastern European countries, and announced their removal on February 12, 2020.[286] The use of the GRU for disinformation campaigns appeared to be a new tactic by the Russians. As mentioned before, the GRU was responsible for the hack and dump attack of the Democratic National Committee in 2016 but had not previously engaged in social media influence campaigns. After the Internet Research Agency and Secondary Infektion, the GRU would be the third different Russian-controlled entity discovered to be conducting influence campaigns ahead of the 2020 elections. These takedowns confirmed the ongoing social media-focused portion of the Russian influence strategy.

[285] Facebook, "Facebook - Preventing Election Interference."

[286] Facebook.

Table 5. Summary of Facebook Takedowns for 2020.[287]

Type	Month					
	February	March	April	August	September	October
Facebook Account	78	49	91	13	229	0
Facebook Page	11	69	46	2	36	2
Facebook Group	29	0	2	0	19	0
Instagram Account	4	85	1	0	37	22
Total	122	203	140	15	321	24
Grand Total	825					

On March 12, 2020, Facebook announced another noteworthy takedown, in which it shut down 85 Instagram accounts, 69 Pages, and 49 Facebook accounts.[288] Its takedown coincided with the CNN story regarding the Eliminating Barriers for the Liberation of Africa organization discussed above. Facebook assessed that individuals from Russia had recruited locals in Ghana and Nigeria to build an online social network and develop an audience; EBLA controlled at least one Instagram account with over 260,000 followers and one Facebook account with over 13,000 followers.[289] The IRA's expansion into West Africa mirrored Yevgeniy Prigozhin's business interests on the continent and suggested the IRA thought its troll-farm model could be successfully exported into other countries.[290] These takedowns demonstrated that Facebook successfully identified Russian disinformation operations despite a shift in their tactics.

---

[287] Adapted from Facebook, "February 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), March 2020, https://about.fb.com/wp-content/uploads/2020/03/February-2020-CIB-Report.pdf; Facebook, "March 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), April 2, 2020, https://about.fb.com/news/2020/04/march-cib-report/; Facebook, "April 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), May 5, 2020, https://about.fb.com/news/2020/05/april-cib-report/; Facebook, "September 2020 Coordinated Inauthentic Behavior Report"; Facebook, "August 2020 Coordinated Inauthentic Behavior Report," *Facebook News* (blog), September 1, 2020, https://about.fb.com/wp-content/uploads/2020/09/August-2020-CIB-Report.pdf; Facebook, "October 2020 Coordinated Inauthentic Behavior Report."

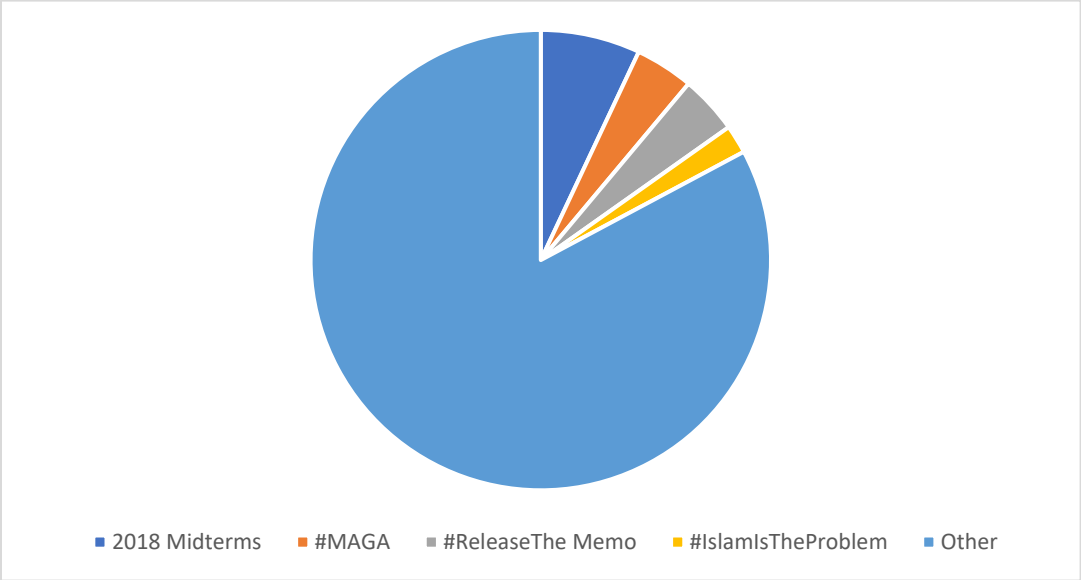
[288] Facebook, "Facebook - Preventing Election Interference."

[289] Facebook.

[290] Grossman, Bush, and DiResta, "Evidence of Russia-Linked Influence Operations in Africa," 2.

In 2019, Twitter announced two takedowns totaling 422 IRA-controlled accounts, which made about 929,000 tweets.[291] Figure 15 demonstrates a categorization of tweets by topic. A review of these tweets revealed a continued focus on the 2018 midterm U.S. elections, with seven percent of all tweets, where Democrats had taken over control of the House of Representatives. The other prominent topics focused on promoting Trump, a right-wing meme that accused the FBI of misusing the Steele dossier to obtain a surveillance order on Trump associate, Carter Page, and Islamophobic rhetoric. The themes promoted by the IRA on Twitter showed its continued acuity in determining the hot-button issues that would agitate right-wing voters.

Figure 15. Breakdown of Twitter Tweets by Topic for 2019.[292]



On November 11, 2019, Twitter announced a ban on virtually all political advertisements.[293] It made a few minor exceptions for issue-based ads and news

[291] Twitter, "Elections Integrity."

[292] Adapted from Twitter.

[293] Feiner and Graham, "Twitter Unveils Final Details for Political Ad Ban, but It's Still Looking Murky."

organizations already exempted from its policy. Twitter "defines political advertising as referencing a candidate, political party, elected or appointed government official, election, referendum, ballot measure, legislation, regulation, directive or judicial outcome."[294] Although Twitter was the first of the major social media companies to ban political advertisements, critics in news media perceived it as an expedient move meant to earn goodwill with the public while only costing less than one percent of its quarterly revenue.[295]

Expanding beyond earlier takedowns, the major social media companies coordinated their publicity for more significant impact and established more direct links to Russia. In 2020, Twitter announced four sets of takedowns, as summarized in Table 6. For 2020, a total of 1,233 accounts were taken down, versus the 3,814 accounts identified as being controlled by the IRA in 2016. One noteworthy takedown occurred on March 12, 2020, when Twitter announced the shutdown of 71 accounts operated by the Eliminating Barriers for the Liberation of Africa organization in Ghana and Nigeria.[296] Twitter attributed them to Russian-sponsored activities, which CNN characterized as an attempt "to sow discord by engaging in conversations about social issues, like race and civil rights."[297] The synchronization of announcements by Facebook and Twitter with the CNN breaking story suggests some level of coordination between the three companies.

Another significant Twitter takedown occurred in June 2020, with the shutdown of 1152 accounts, which Twitter and the Stanford Internet Observatory attributed a campaign dubbed the "Current Policy" to the IRA because of the anti-Western and pro-Putin content it disseminated.[298] Stanford's analysis determined the Current Policy accounts posted more than 3.4 million tweets since 2013, with some focused on portraying actual Russian

---

294 Feiner and Graham.

295 Michael Nuñez, "The Surprising Truth about Twitter's Political Ad Ban," *Forbes*, November 1, 2019, https://www.forbes.com/sites/mnunez/2019/11/01/the-surprising-truth-about-twitters-political-ad-ban/.

296 Ward et al., "Russian Election Meddling Is Back."

297 Ward et al.

298 Stanford Internet Observatory, "Analysis of June 2020 Twitter Takedowns Linked to China, Russia, and Turkey."

government agencies and others working to boost specific Russian politicians or federal initiatives.[299] These actions revealed coordination among the social media companies, news media, and a research organization to thwart Russian disinformation operations.

Table 6. Summary of Twitter Takedowns for 2020.[300]

Type	Month			
	March	June	September	October
Account	71	1152	5	5
Grand Total	1,233			

At the beginning of 2020, Twitter announced an enhancement of its safety policies, developing better tools for detecting abusive behavior, and aggressively taking actions against violations of the terms of service.[301] Twitter also highlighted its collaboration with political parties, researchers, and election officials. In addition, a Twitter spokesperson stressed the importance of staying in contact with state election officials and law enforcement.[302]

On November 26, 2019, Google announced it had shut down 15 YouTube channels and associated Google accounts. These IRA-controlled accounts used English, French, and Arabic language content to target users in South Africa, Madagascar, Sudan, and the Central African Republic. Google said these accounts were associated with the account

299 Stanford Internet Observatory.

300 Adapted from Ward et al., "Russian Election Meddling Is Back"; @TwitterSafety, "June 2020: Disclosing Networks of State-Linked Information Operations We've Removed," *Twitter Information Operations* (blog), June 12, 2020, https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.html; @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

301 Twitter, "Elections Integrity."

302 Twitter.

takedowns Facebook had announced on October 30, 2019.[303] This statement confirmed joint action facilitated by information sharing between the two companies.

On March 3, 2020, Google announced it had developed policies prohibiting deceptive practices such as voter suppression and misrepresentation in all its products, including Google Ads, YouTube, and the Google Play Store.[304] The company also mentioned working closely with other technology companies and the FBI regarding referrals and leads.[305] This announcement by Google showed an effort to be more transparent, coordinate with other social media companies, and acknowledge some engagement with the FBI.

In April 2020, Google's Threat Analyst Group began to blog about account takedowns every quarter. Table 7 provides a summary of the number and types of accounts taken down by Google. For 2020, Google took down a total of 129 accounts, which is lower in number than in 2016, when it identified and submitted 228 YouTube videos and 655 AdWord advertisements to the Senate Intelligence Committee for review.[306]

Table 7. Summary of Google Takedowns for 2020.[307]

Type	Month				
	April	May	June	October	November
YouTube Channel	22	47	17	28	10
Blog	3	0	0	1	0
AdSense Account	0	1	0	0	0
Total	25	48	17	29	10
Grand Total	129				

303 Google Threat Analysis Group, "Google Safety & Security."

304 Google Threat Analysis Group.

305 Google Threat Analysis Group.

306 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 7.

307 Adapted from Google Threat Analysis Group, "TAG Bulletin: Q2 2020," *Google: Updates from Threat Analysis Group* (blog), August 5, 2020, https://blog.google/threat-analysis-group/tag-bulletin-q2-2020/; Google Threat Analysis Group, "TAG Bulletin," November 17, 2020.

C. U.S. GOVERNMENT COUNTERMEASURES

Ahead of the 2020 U.S. elections, the U.S. government appeared publicly focused on transparency efforts, such as public statements and a hearing, and modifying the policies regarding interactions with political campaigns. The U.S. government also took security steps, such as information sharing with relevant stakeholders, including social media companies and political campaigns. The major social media companies mentioned working with the U.S. government to some extent. Some news reporting corroborated this engagement between the private sector companies and the U.S. government.

Only one public Congressional hearing took place before the U.S. elections on November 3, 2020. On September 18, 2019, the Senate Commerce Committee held a hearing with senior executives from Facebook, Google, and Twitter to discuss their companies' efforts to remove extremist content and disinformation from their platforms.[308] This hearing was the only opportunity in 2019 for the American public through Congressional testimony and for Congress to publicly hold the companies accountable for the actions they previously pledged to protect the elections.

On May 15, 2020, to address foreign interference threats more directly, William Evanina, Director of the National Counterintelligence and Security Center (NCSC), was tasked with leading all the U.S. government threat intelligence briefings to the relevant national political committees and presidential campaign committees.[309] The ODNI likely changed the briefers from a rotating cadre of analysts from the FBI and DHS to streamline the process for the recipients and let the political campaigns and all Americans know the entire U.S. Intelligence Community backs these threat briefings.[310]

Before the 2020 U.S. elections, the FBI took some public actions related to election security. On October 23, 2019, FBI Director Wray announced an expansion of the

---

[308] U.S. Congress. Senate, September 18, 2019.

[309] Office of the Director of National Intelligence, "Director of National Intelligence Announces Changes to Election Security Briefings," Office of the Director of National Intelligence, May 15, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2118-director-of-national-intelligence-announces-changes-to-election-security-briefings.

[310] Office of the Director of National Intelligence.

Protected Voices Initiative.[311] New cybersecurity training videos and reference materials were added to the website. Furthermore, the FBI indicated it would provide cybersecurity training to all of the presidential campaigns ahead of the primary election season.[312] This training supplemented the FBI's ongoing engagement with the national-level political committees. This security-related action continued the FBI's efforts to help the various political campaigns safeguard their computer networks and electronic devices.

On January 16, 2020, the FBI stated it was modifying its notification policy regarding computer intrusions to election infrastructure. Previously, the FBI would notify local election officials whose organizations typically owned and maintained the election systems and equipment. The local officials would be responsible for informing the state-level officials. With this policy change, the FBI would simultaneously notify the designated chief state-level election official as well as the local officials impacted by a cyber-attack. According to the FBI press release, "this new policy will result in increased collaboration between all levels of government for the integrity and security of U.S. elections."[313] Thus, the FBI appeared to publicly state affirmative actions it was taking to safeguard the elections. Previously, the FBI had been typically reluctant to disclose election-related actions to the public.

Despite not making public announcements about its involvement with the private sector, the U.S. government appeared to be more engaged with social media companies ahead of the 2020 U.S. elections than in 2016. On September 4, 2019, Facebook hosted an election security meeting with the FBI, DHS, and ODNI.[314] The other companies

311 "Protecting Every Voice: FBI Expands Suite of Resources on Election Security," *Homeland Security Today* (blog), October 23, 2019, https://www.hstoday.us/subject-matter-areas/infrastructure-security/protecting-every-voice-fbi-expands-suite-of-resources-on-election-security/.

312 "Protecting Every Voice."

313 Federal Bureau of Investigation, "FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure," FBI Press Releases, January 16, 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-policy-for-notifying-state-and-local-election-officials-of-cyber-intrusions-affecting-election-infrastructure.

314 Kurt Wagner, "Facebook Meets With FBI to Discuss 2020 Election Security," Bloomberg, September 4, 2019, https://www.bloomberg.com/news/articles/2019-09-04/facebook-meets-with-fbi-to-discuss-2020-election-security.

attending the meeting included Google, Microsoft, and Twitter.[315] The group discussed plans for better coordination and information sharing.[316] This meeting was the first indication of private sector companies meeting with the U.S. government to safeguard the 2020 U.S. elections. In August 2020, the New York Times broke a story revealing that the private sector companies working with the U.S. government had expanded to include the Wikimedia Foundation, Verizon Media, Reddit, Pinterest, and LinkedIn.[317] A spokesperson for the private sector companies stated that they regularly met with the U.S. government agencies responsible for election security to discuss threat trends and worked closely with each represented company to protect their platforms.[318]

Public statements from some social media companies revealed that the U.S. government, particularly the FBI, had provided them with tipper information to detect Russian influence operations on their platforms. In August 2020, Facebook announced that it had taken down two pages and 13 Facebook accounts, which the IRA was controlling, and mentioned finding the cluster due to off-platform activities identified by the FBI.[319] In September 2020, Facebook and Twitter announced the takedown of PeaceData-associated accounts being controlled by the IRA.[320] Facebook stated that it had been able to identify the accounts based on off-platform information provided by the FBI.[321] Twitter went further in its statement when it expressly thanked the FBI's Foreign Influence Task Force for its "close collaboration and continued support of our work to protect the public conversation at this critical time."[322] In October 2020, Facebook identified and shut down

315 Wagner.

316 Wagner.

317 Mike Isaac and Kate Conger, "Google, Facebook and Others Broaden Group to Secure U.S. Election," *New York Times*, August 12, 2020, https://www.nytimes.com/2020/08/12/technology/google-facebook-coalition-us-election.html.

318 Isaac and Conger.

319 Facebook, "August 2020 Coordinated Inauthentic Behavior Report."

320 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; Facebook, "September 2020 Coordinated Inauthentic Behavior Report."

321 Facebook, "September 2020 Coordinated Inauthentic Behavior Report."

322 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

a network of IRA-controlled Facebook and Instagram operated out of Mexico and Venezuela.[323] Once again, Facebook mentioned its ability to identify these accounts based on information provided by the FBI.[324] Also, in October 2020, Google noted it had shut down one blog and 26 YouTube channels being operated by the IRA.[325] In addition, Google's Threat Analysis Group mentioned it had received leads provided by the FBI to support its internal investigation.[326] In total, the FBI appears to have shared information with Facebook, Google, and Twitter on at least four occasions, which led to the detection and takedown of multiple IRA-controlled accounts on their respective platforms. This sharing contrasted with 2016 when it seemed that the U.S. government had not shared any threat information with the social media companies ahead of the 2016 U.S. elections.

Besides the FBI and DHS, other U.S. government agencies were also publicly involved in election security. For example, in August 2020, the NSA, jointly with the FBI, issued a cybersecurity advisory exposing complex malware dubbed "Drovorub," created by Russian Military Intelligence.[327] This advisory was the first of its kind and would allow private and public sector organizations to safeguard themselves ahead of the election. Also, in August 2020, the State Department's Global Engagement Center issued an extensive report revealing the disinformation tactics employed by the Russian government and associated organizations, such as the IRA.[328] The State Department believed this report would help news media, private and public sector organizations, and other governments detect and analyze Russian influence operations to build up a collective resilience.[329]

---

[323] Facebook, "October 2020 Coordinated Inauthentic Behavior Report."

[324] Facebook.

[325] Google Threat Analysis Group, "TAG Bulletin," November 17, 2020.

[326] Google Threat Analysis Group.

[327] National Security Agency and Federal Bureau of Investigation, *Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*, Rev 1.0 (Washington, DC: National Security Agency & Federal Bureau of Investigation, 2020), https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF.

[328] Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem*.

[329] Global Engagement Center, 2.

During the elections, the U.S. government had little to do with the actual administration of political campaigns or elections. Instead, the U.S. government was responsible for providing funding to states for equipment upgrades, conducting enforcement actions to ensure fair elections, and keeping the American public apprised of any significant developments.[330] On November 4, 2020, after the election polls had closed across the United States, Christopher Krebs, Director of the Cybersecurity and Infrastructure Security Agency, issued a statement that the U.S. government had seen no evidence of Russian or other foreign adversaries changing ballots or preventing Americans from voting. In December 2020, Krebs reaffirmed his belief about the integrity of the 2020 U.S. Elections during a hearing before the Senate Committee on Homeland Security and Governmental Affairs in December 2020.[331] Senior election executives representing America's election infrastructure sector made a statement that echoed Krebs' claim of a safe and fair election.[332]

In March 2021, the Office of the Director of National Intelligence issued the Intelligence Community's report assessing foreign threats to the 2020 U.S. elections.[333] Similar to what NCSC Director Evanina said in his August 2020 statement, the ODNI assessment emphasized the ongoing and concerted Russian disinformation campaign, which was designed to promote the reelection of President Trump, denigrate Joe Biden and the Democratic Party, erode trust in the election process, and inflame political and social tensions within the United States.[334] The ODNI discussed the efforts of the Internet

---

330 R. Sam Garrett, *Federal Role in U.S. Campaigns and Elections: An Overview*, CRS Report No. R45302 (Washington, DC: Congressional Research Service, 2018), 27, https://fas.org/sgp/crs/misc/R45302.pdf.

331 *Examining Irregularities in the 2020 Election: Hearing before the Committee on Homeland Security and Governmental Affairs*, Senate, 116th Cong., 2nd Session, December 16, 2020, 2, https://www.hsgac.senate.gov/imo/media/doc/Testimony-Krebs-2020-12-16.pdf.

332 Elections Infrastructure Government Coordinating Council and Election Infrastructure Sector Coordinating Executive Committee, "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees," November 12, 2020, https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

333 Office of the Director of National Intelligence, "Intelligence Community Assessment on Foreign Threats to the 2020 U.S. Federal Elections."

334 Office of the Director of National Intelligence.

Research Agency and highlighted the "short-lived troll farms" based in Mexico and Western Africa, which were initiated to avoid the ongoing account takedown efforts by the social media companies with help from the U.S. government.[335] The ODNI concluded that greater awareness by the news media and the American public, coupled with the actions taken by the social media companies and the U.S. government, likely countered the Russian efforts to some degree.[336]

D. USING THE KARTAPOLOV FRAMEWORK TO EVALUATE RUSSIAN AND AMERICAN MEASURES IN 2020

As previously used for appraising IRA information operations during the elections in 2016 and 2018, the relevant components of the Kartapolov Framework were used to evaluate the Russian and American efforts to determine their effectiveness for the 2020 U.S. Elections. To reiterate, these components are: (1) spreading discontent in the population, (2) exerting political pressure, and (3) confusing the political leadership.[337] The impact of the Russian campaigns on American political leadership will be gauged in the section evaluating the countermeasures taken by the U.S. government.

1. The IRA and Other Proxies – Impact and Evolution

The Internet Research Agency evolved its tactics ahead of the 2020 U.S. elections but was unsuccessful in achieving its ultimate desired outcome of a Trump reelection. The IRA's tactical developments were two-fold: (1) moving troll farm operations to locations outside of Russia, namely West Africa and Mexico, and (2) moving content from the social media platforms to websites the IRA controlled. For the first component of the Kartapolov Framework, a review of all four of the IRA's campaigns for 2020 showed they were focused on inflaming dissension in the populace. CNN evaluated the social media content disseminated by Eliminating Barriers for the Liberation of Africa and noted it was primarily focused on racial issues such as Black empowerment and used language meant

335 Office of the Director of National Intelligence, 3.

336 Office of the Director of National Intelligence, 6.

337 Wilhelm, "A Russian Military Framework," 35.

to inflame divisions between American racial groups.[338] For the PeaceData outlet, Graphika's analysis determined the actors behind it were targeting progressive groups in the United States, especially those who identified with democratic socialism.[339] The Newsroom for American and European Based Citizens site appeared to be the counterweight to PeaceData. It targeted viewers with a far-right ideology because it covered topics such as racist tropes about black people and criticism of the Black Lives Matter movement.[340] Lastly, the Secondary Infektion campaign's focus on diplomacy and foreign policy appeared to be tailored to denigrate the United States and its European allies while also trying to foment conflict between the allied countries.[341] Although the Russian actions likely inflamed already existing dissension in the United States, it did not appear to deter voter turnout at all. The effectiveness of the Russian messaging was probably blunted by the account takedowns by the major social media companies and being outed by the news media before it could develop traction with the targeted audiences.

For the second component of the Kartapolov Framework, exerting political pressure, the Russian campaigns appeared to have mixed results. On the one hand, from interviews conducted with the social media companies, CNN determined that the IRA-controlled organization, Eliminating Barriers for the Liberation of Africa, had successfully gathered many followers for its social media accounts since its inception in June 2019.[342] Facebook reported to CNN that the EBLA-controlled accounts had about 267,000 users following EBLA-controlled Facebook or Instagram accounts.[343] Twitter reported that EBLA-controlled accounts had about 68,000 followers before being shut down.[344] Although the number of followers does not directly correlate to the amount of political

338 Ward et al., "Russian Election Meddling Is Back."

339 Nimmo et al., "IRA Again: Unlucky Thirteen," 24–25.

340 Graphika Team, *Step Into My Parler*, 8.

341 Nimmo et al., *Secondary Infektion*, 13.

342 Ward et al., "Russian Election Meddling Is Back."

343 Ward et al.

344 Ward et al.

pressure, it indicates that EBLA's content resonated enough with social media users to convince them to follow the EBLA-controlled accounts.

On the other hand, the other Russian campaigns appeared to be less effective in creating political pressure. Since its inception in February 2020, the PeaceData site averaged about ten posts per day on the English-language page and 20 posts per day on the Arabic-language page.[345] Twitter noted that the PeaceData-associated Twitter accounts were "low quality and spammy," and assessed they did not garner much attention from other Twitter users.[346] Facebook also took down a few PeaceData-associated Facebook and Instagram accounts but did not characterize how other users engaged with these accounts.[347] The Newsroom for American and European Based Citizens outlet started in June 2020 but did not appear to attract much of a social media following. Graphika discovered that only about 14,000 users on Parler and 3,000 users on Gab followed the NAEBC site.[348] The Secondary Infektion campaign appeared to be prolific during its existence. Still, Graphika noted that the vast majority of the content produced did not garner much, if any, engagement with other users.[349] Graphika opined that the operators behind Secondary Infektion were motivated more by hitting production metrics than content engagement or virality.[350] The ability of the Russian influence campaigns to generate political pressure may have been dampened by the social media company account takedowns and exposure by media outlets and Graphika, which will be discussed in more detail in the next section.

For the third component of the Kartapolov Framework, namely confusing the political leadership, the impact of the Internet Research Agency and other Russian proxies'

345 Nimmo et al., "IRA Again: Unlucky Thirteen," 5.

346 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

347 Facebook, "September 2020 Coordinated Inauthentic Behavior Report."

348 Graphika Team, *Step Into My Parler*, 2.

349 Nimmo et al., *Secondary Infektion*, 8.

350 Nimmo et al., 8.

actions will be discussed in the section evaluating the impact of the U.S. government's actions.

2. The Private Sector Companies' Impact and Adaptations

The effectiveness of the private sector countermeasures used against the Russian influence operations targeting the 2020 U.S. election was evaluated using the Kartapolov Framework. To combat the first component, spreading discontent in the American public, the private sector responded to take security-focused actions. Specifically, the companies enhanced their detection systems to identify and disrupt Russian influence activities before gaining much traction with their users. As a result, each of the prominent social media companies had somewhat different results from 2016 to 2020, shown in table 8.

Table 8. Social Media Account Takedowns between 2016 and 2020.[351]

Company	Number of Accounts Taken Down		
	2016	2020	Difference
Facebook	470	825	+355
Google	883	129	-754
Twitter	1,233	3,814	+2,581

While Facebook and Twitter saw an increase in IRA-controlled accounts on their platforms, Google saw a decrease in accounts taken down. A partial explanation for this phenomenon could be that Instagram, a wholly-owned Facebook subsidiary, was the most

[351] Adapted from @TwitterSafety, "June 2020: Disclosing Networks of State-Linked Information Operations We've Removed"; @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; Facebook, "February 2020 Coordinated Inauthentic Behavior Report"; Facebook, "March 2020 Coordinated Inauthentic Behavior Report"; Facebook, "April 2020 Coordinated Inauthentic Behavior Report"; Facebook, "September 2020 Coordinated Inauthentic Behavior Report"; Facebook, "August 2020 Coordinated Inauthentic Behavior Report"; Facebook, "October 2020 Coordinated Inauthentic Behavior Report"; Google Threat Analysis Group, "TAG Bulletin," August 5, 2020; Google Threat Analysis Group, "TAG Bulletin," November 17, 2020; Ward et al., "Russian Election Meddling Is Back."

conducive social media platform for propagating memes, which has become prevalent in popular culture and was also favored by the IRA.[352] Another explanation was that the IRA might have needed to shift resources away from YouTube activities to develop the PeaceData and Newsroom for American and European Based Citizens outlets.

Another method for stopping the spread of discontent in the population was for the private sector companies to share data from foreign influence-related account takedowns with third-party organizations, such as researchers and research institutions. After the 2016 U.S. Elections, each of the companies shared data with the Senate Committee on Intelligence, who in turn shared it with researchers to analyze it.[353] Since that time, each company has shared data to varying degrees with researchers and other organizations. For example, in June 2020, Twitter shared information with Stanford University regarding the detection and takedown of Chinese, Russian, and Turkish influence campaigns on their platform.[354] Twitter shared the data with Stanford as an objective third party to analyze and publish the results in service of increased transparency.[355] In September 2020, Graphika revealed Facebook had given it data regarding the PeaceData outlet.[356] In October 2020, Graphika received information from Facebook and Twitter regarding the Newsroom for American and European Based Citizens outlet.[357] These examples illustrated the social media sharing information with third parties to presumably publicize objective analysis regarding IRA disinformation and tactics to the public.

All of the major social media companies took visible measures to counter political pressure, the second component of the Kartapolov Framework, which the IRA exerted through its online influence activities on the different social media platforms. These transparency-focused actions included the increased cadence of each company's public

352 Leighton, "For Instagram's 10th Birthday, Experts Predict The Future Of Meme Culture"; Alina Polyakova, "The Kremlin's Plot against Democracy," *Foreign Affairs*, October 2020.

353 *Russian Active Measures Campaigns: Volume 1*.

354 Stanford Internet Observatory, "Analysis of June 2020 Twitter Takedowns Linked to China, Russia, and Turkey."

355 Stanford Internet Observatory.

356 Nimmo et al., "IRA Again: Unlucky Thirteen."

357 Graphika Team, *Step Into My Parler*.

notifications to the general public regarding account takedowns. A secondary transparency-focused action was each company's effort to enact and improve its advertising purchasing policies. For Facebook and Google, these improvements appeared to make it more difficult for foreign actors to purchase political advertisements.[358] Twitter went the furthest of the three social media companies by banning political ads entirely in its November 2019 announcement.[359] The third type of transparency-focused action was the attempt by companies to improve the labeling of content. Again, Twitter appeared to be the most aggressive of the three social media companies. In May 2020, Twitter announced that labeling would be applied to all content disputed, misleading, or synthetically generated.[360] In June 2020, Facebook made a similar announcement and modified its policies to improve transparency for political content and advertisements.[361] Thus, the private sector companies' collective security and transparency-related actions seemed to diminish the impact of the Russian influence operations by preventing them from gaining much traction on the social media platforms.

3. The U.S. Government's Impact – Transparency and Private Sector Partnerships

Examining the U.S. government's actions to protect the 2020 U.S. Elections through the Kartapolov Framework revealed a more robust response than in 2016. For the first element of the framework, spreading discontent across the populace, the U.S. government took a range of security and transparency-related actions to impede Russian influence operations. Likely the most significant action was the FBI's reported information sharing with the social media companies on at least four occasions, which led to the

358 Facebook, "Facebook - Preventing Election Interference"; Google Threat Analysis Group, "Google Safety & Security."

359 Twitter, "Elections Integrity."

360 Yoel Roth and Nick Pickles, "Updating Our Approach to Misleading Information," *Only on Twitter* (blog), May 11, 2020, https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.html.

361 Facebook, "Facebook - Preventing Election Interference."

companies identifying and taking down multiple clusters of IRA-controlled accounts.[362] In addition, the U.S. government meeting with the private sector companies on at least two separate occasions to share information on threat trends may have added context and atmospherics to enhance the companies' detection methods.[363] Finally, the report issued by the State Department's Global Engagement Center in August 2020 may be regarded as a U.S. government transparency effort to expose Russian disinformation tactics to the American public and blunt the impact of these tactics.[364] In general, the U.S. government appeared more actively engaged with the social media companies ahead of the 2020 elections.

For the second element of the Kartapolov Framework, exerting political pressure, the U.S. government took a series of measures, which may have diffused the pressure that Russia was trying to apply through its information operations. The FBI's Protected Voice Initiative, which provided cybersecurity training to the national level political parties and presidential campaigns, was coupled with the classified threat briefings to the same organizations provided by National Counterintelligence and Security Center's Director William Evanina.[365] Furthermore, the FBI modified its victim notification process by including designated state-level election officials when notifying local or county-level election officials of cybersecurity issues.[366] Finally, the highly detailed joint NSA/FBI cybersecurity advisory regarding the Drovorub malware exposed one of the Russian

362 @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; @TwitterSafety, "October 2020: Disclosing Networks to Our State-Linked Information Operations Archive"; Facebook, "September 2020 Coordinated Inauthentic Behavior Report"; Facebook, "October 2020 Coordinated Inauthentic Behavior Report"; Google Threat Analysis Group, "TAG Bulletin," November 17, 2020; Graphika Team, *Step Into My Parler*.

363 Isaac and Conger, "Google, Facebook and Others Broaden Group to Secure U.S. Election"; Wagner, "Facebook Meets With FBI to Discuss 2020 Election Security."

364 Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem*, 3.

365 Federal Bureau of Investigation, "Combating Foreign Influence"; Office of the Director of National Intelligence, "Director of National Intelligence Announces Changes to Election Security Briefings."

366 Federal Bureau of Investigation, "FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure — FBI," FBI Press Releases, January 16, 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-policy-for-notifying-state-and-local-election-officials-of-cyber-intrusions-affecting-election-infrastructure.

military's most potent cyber weapons, providing organizations with time to protect themselves ahead of the elections.[367] This combination of actions by the U.S. government probably ensured no significant data breaches at any national-level political parties or campaigns during the 2020 U.S Elections.

For the third element of the Kartapolov Framework, confusing the political leadership, the U.S. government, both the executive and legislative branches, appeared to be focused and decisive in its endeavors to safeguard the 2020 U.S. Elections. In September 2019, the Republican-chaired Senate Commerce Committee called a hearing with senior executives from Facebook, Google, and Twitter to learn about their progress in removing disinformation and violent content from their platforms.[368] The following year, public statements made by NCSC Director William Evanina in July 2020 and August 2020 gave a clear indication that the U.S. Intelligence Community was aware of Russian activities targeting the elections and decided to inform the American public.[369] In a similar vein, on the day after the elections closed, Christopher Krebs, Director of the Cybersecurity and Infrastructure Security Agency, stated that the U.S. government had "no evidence any foreign adversary was capable of preventing Americans from voting or changing vote tallies."[370] In October 2020, the Department of Justice indicted six officers in the Russian Military Intelligence Unit 74455, responsible for hacking attacks in Georgia and Ukraine,

---

[367] Dan Goodin, "NSA and FBI Warn That New Linux Malware Threatens National Security," *Ars Technica*, August 13, 2020, https://arstechnica.com/information-technology/2020/08/nsa-and-fbi-warn-that-new-linux-malware-threatens-national-security/.

[368] September 18, 2019.

[369] William Evanina, "Statement by NCSC Director William Evanina: 100 Days Until Election 2020," Office of the Director of National Intelligence, July 24, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020; William Evanina, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," Office of the Director of National Intelligence, August 7, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

[370] Christopher Krebs, "Statement from CISA Director Krebs Following Final Day of Voting," Cybersecurity and Infrastructure Security Agency, November 4, 2020, https://www.cisa.gov/news/2020/11/04/statement-cisa-director-krebs-following-final-day-voting.

and the Winter Olympics in South Korea.[371] Some of these GRU officers had been previously indicted for hacking the Democratic National Committee in 2016.[372] Interestingly, the Department of Justice highlighted the assistance of the threat intelligence teams from Google and Cisco for this indictment.[373] Additionally, the report on Russian disinformation tactics issued by the State Department and the joint cybersecurity advisory issued by the NSA and FBI rounded out the U.S. government's multi-agency approach to exposing malign Russian activities through different avenues.

E. VOTER TURNOUT IN THE 2020 ELECTIONS

The two most important indicators of a secure and successful election were high voter turnout and no evidence of systemic voter fraud. The Pew Research Center determined that 2020 had the highest voter turnout since 1960, with approximately 158 million Americans casting ballots.[374] Table 9 shows a comparison in voter turnout between 2016 and 2020, both of which were presidential election years. In addition, multiple news organizations and think tanks on both sides of the aisle reported that the 2020 U.S. elections were free of any systemic voter fraud, impacting the results.[375]

---

371 Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," Department of Justice, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

372 Department of Justice.

373 Department of Justice.

374 Drew DeSilver, "Turnout Soared in 2020 as Nearly Two-Thirds of Eligible U.S. Voters Cast Ballots for President," *Pew Research Center Fact Tank* (blog), January 28, 2021, https://www.pewresearch.org/fact-tank/2021/01/28/turnout-soared-in-2020-as-nearly-two-thirds-of-eligible-u-s-voters-cast-ballots-for-president/.

375 Brennan Center for Justice, "It's Official: The Election Was Secure | Brennan Center for Justice," *Brennan Center for Justice* (blog), December 11, 2020, https://www.brennancenter.org/our-work/research-reports/its-official-election-was-secure; Nick Corasaniti, Reid J. Epstein, and Jim Rutenberg, "The Times Called Officials in Every State: No Evidence of Voter Fraud," *New York Times*, November 11, 2020, https://www.nytimes.com/2020/11/10/us/politics/voting-fraud.html; Justin Grimmer, Haritz Garro, and Andrew Eggers, "No Evidence For Voter Fraud: A Guide To Statistical Claims About The 2020 Election," Text (Palo Alto, CA: Hoover Institution, February 3, 2021), https://www.hoover.org/research/no-evidence-voter-fraud-guide-statistical-claims-about-2020-election; Reality Check Team, "US Election 2020: Fact-Checking Trump Team's Main Fraud Claims," BBC News, November 23, 2020, https://www.bbc.com/news/election-us-2020-55016029.

Table 9. Comparison of Overall Voter Turnout for Presidential Elections.[376]

Election Year	Number of Voters Turning Out	Percentage of Voter Turnout
2016	137,500,000	61.4%
2020	158,000,000	66.2%
Change	**+20,500,000**	**+4.8%**

It is still unclear whether the IRA's operations contributed to the record number of Americans to vote or suppress turnout among Black voters in 2016. The U.S. Census Bureau will not have an analysis of voter demographics for the 2020 elections until late in 2021. Despite the lack of demographic data for 2020, the Russian attempts to depress voter turnout were unsuccessful as Americans turned out in record numbers.

F. CONCLUSIONS FROM THE 2020 U.S. ELECTIONS

Reflecting on the 2020 elections, three main themes emerged. First, the Russians continued their efforts to target the U.S. elections while shifting tactics to avoid detection. Second, the social media companies, along with news media and research organizations, were able to identify and disrupt the evolving Russian disinformation campaigns. Third, the U.S. government was a more active player in securing the elections, primarily through its information sharing with the social media companies, political organizations, and the American public.

Despite the best efforts of the Russians, social media companies, news media, and research organizations were able to detect, expose, and disrupt the activities of the Internet Research Agency and their other online groups, namely Secondary Infektion and the GRU. Although America's private sector may have been caught unaware during the 2016 elections, it was on heightened alert ahead of 2020, with the noteworthy efforts of CNN,

[376] Adapted from DeSilver, "Turnout Soared in 2020 as Nearly Two-Thirds of Eligible U.S. Voters Cast Ballots for President"; Krogstad and Lopez, "Black Voter Turnout Fell in 2016."

Reuters, and Graphika exposing Russian disinformation activities and paving the way for the social media companies to shut down their social media accounts.

The U.S. government's response to the Russian influence campaign appeared more robust before the 2020 elections than in the 2016 or 2018 elections. These efforts comprised a series of transparency and security-related measures. The most important actions taken by the U.S. government may have been the information sharing with the social media companies to expose Russia's different operations and shut down its accounts. In addition, the U.S. government's information-sharing may have helped the social media companies secure their platforms by identifying malign Russian influence activities. At first glance, the U.S. government's other responses, such as economic sanctions and indictments, may not seem impactful because the United States does not have an extradition treaty with Russia. As a result, the sanctioned or indicted individuals may never be brought to justice in the U.S. court system. However, a critical role of sanctions and indictments is to provide transparency, i.e., factual narratives of the crimes perpetrated by Russia that informs the American public.

It took the collaborative efforts of the private sector, in the form of social media companies, researcher organizations, and news media, and the public sector, in the form of the executive and legislative branches of the U.S. government, to turn back the Putin-sanctioned disinformation operations which were targeting the 2020 U.S. elections. These collective actions were viewed through the lens of the Kartapolov Framework to determine their effectiveness in countering Russian influence operations. The next chapter will identify and examine the most effective countermeasures and provide recommendations for safeguarding future elections.

IV. CONCLUSIONS AND RECOMMENDATIONS TO COUNTER RUSSIA IN THE FUTURE

> The problem of foreign actors trying to influence the American electorate is not going away and, given the current partisan divides in this country, may find fertile ground in which to grow in the future.
>
> — Mark Warner, March 16, 2021

Senator Warner, Chair of the Senate Intelligence Committee, made the above statement after the Office of the Director of National Intelligence released its report appraising foreign threats to the 2020 U.S. elections. This report, backed by the entire U.S. Intelligence Community, assessed that Russia was actively trying to influence the elections through information operations.[377] Furthermore, the report forecasts Russia will continue to interfere in future U.S. elections to degrade the United States' global credibility and weaken its influence overseas.[378] In anticipation of the continued Russian influence threat, this chapter provides a final summation of the American efforts to protect the 2020 elections and concludes which efforts were the most effective. Based on these conclusions, recommendations have been proposed to protect future U.S. elections. These recommendations are derived, in part, from proposals by subject matter experts in a variety of fields.

A. CONCLUSIONS – THERE IS NO END GAME

The major social media companies and the U.S. government's efforts to protect the 2020 U.S. elections against Russian malign influence campaigns appeared to be generally successful. Using the Kartapolov Framework in this thesis provided a systematic method to analyze the effectiveness of the American countermeasures qualitatively. As a reminder, the framework is a mental model devised by Thomas Wilhelm, a U.S. Army researcher, to understand better the Russian military's perspective in conducting information operations

[377] Office of the Director of National Intelligence, "Intelligence Community Assessment on Foreign Threats to the 2020 U.S. Federal Elections," 2.

[378] Office of the Director of National Intelligence, 5.

to further its objectives.[379] The most effective measure taken by the major social media companies was the rapid detection and takedown of fake accounts and content generated by the Internet Research Agency and other Russian proxies. The social media companies' other efficacious efforts included publicizing these account takedowns, which promoted transparency to the American public, and partnering with other organizations, such as news media and researchers, to expose Russian influence activities which were not on the social media platforms. The most effective measure taken by the U.S. government was likely its information-sharing efforts with the social media companies to help them identify previously unknown Russian influence activities on their platforms. The U.S. government's other effective efforts included its initiative to inculcate good cybersecurity practices among the national-level political parties and campaigns and regular public messaging about malign influence activities to the American populace.

The Internet Research Agency resembled a professional marketing firm that employed both technology and psychology to maximum effect.[380] It took advantage of easy-to-use social media platforms to reach millions of U.S. citizens.[381] The IRA recognized the existing dissension among different sectors of the American population and exploited it to drive people further into tribalism.[382] Over the past several years, the IRA honed its skills and precisely identified specific in-groups it wanted to influence. On the right side of the political spectrum, the IRA focused on issues such as illegal immigration, gun rights, religious freedom, anti-abortion, and the general fear of change.[383] Although challenging, if not impossible to quantify, the IRA's influence activities may have reinforced these people's in-group beliefs, which could have potentially activated them to vote for Trump. On the left side of the political spectrum, the IRA appeared to play on the fears and frustrations of the more racially and ideologically diverse group to suppress voter

379 Wilhelm, "A Russian Military Framework," 33.

380 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 6.

381 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 39.

382 *Report on Russian Active Measures*, 4.

383 DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, 99.

turnout.[384] The IRA's main shift in tactics from 2016 to 2020 was its creation of fake news outlets appealing to far-right conservatives, in the form of the Newsroom for American and European Based Citizens, and ultraliberals, in the form of the PeaceData site.[385] Ostensibly, the IRA's rationale for this shift was to control its own content and avoid the aggressive disruption tactics of the major social media companies. The IRA's other significant shift was to use indigenous workers in other countries to mask its true identity, explicitly creating the front organization known as Eliminating Barriers for the Liberation of Africa.[386]

The Internet Research Agency's role in influencing the 2016 and 2020 U.S. Presidential Elections may have been marginal but still impactful. That being said, the IRA's influence in 2020 was significantly diminished compared to its efforts in 2016. The primary reason was that the IRA's activities were unnoticed and unconstrained in 2016 but were quickly detected and disrupted in 2020 by the major social media companies and the U.S. government. One of the IRA's primary goals was to suppress Black voter turnout.[387] An illustrative statistic was the decline of Black voter turnout in 2016 by seven percent compared to the 2012 elections.[388] In 2020, Black voter turnout rebounded by four percent over the 2016 levels.[389] In addition, other minority groups had significant increases in voter turnout for 2020. Hispanic voter turnout increased by six percent, and Asian voter turnout increased by ten percent.[390] These 2020 turnout results showed the ineffectiveness of the IRA's efforts.

---

384 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 3.

385 Graphika Team, *Step Into My Parler*, 2; Nimmo et al., "IRA Again: Unlucky Thirteen," 1.

386 Ward et al., "Russian Election Meddling Is Back."

387 Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 18.

388 Krogstad and Lopez, "Black Voter Turnout Fell in 2016."

389 William H. Frey, *Turnout in 2020 Election Spiked among Both Democratic and Republican Voting Groups, New Census Data Shows* (Washington, DC: Brookings, 2021), https://www.brookings.edu/research/turnout-in-2020-spiked-among-both-democratic-and-republican-voting-groups-new-census-data-shows/.

390 Frey.

Many factors are at play when trying to measure the effects of Russia's influence operations. First-order effects include real users interacting with inauthentic content, Russian-bot amplification of divisive organic content, and IRA-controlled accounts communicating directly with real users. Second-order effects include changes to the social network itself by the actions mentioned above and contemporaneous sociopolitical events influencing discussions. Due to how the U.S. Electoral College process awards presidential electoral votes, the U.S. Presidency was decided by about 78,000 votes combined across Michigan, Pennsylvania, and Wisconsin for 2016.[391] In 2020, Biden won the presidency by about 45,000 votes combined across Arizona, Georgia, and Wisconsin.[392] In both presidential elections, voter turnout was near historical highs.[393] In order to protect future elections in the United States, a whole-of-society approach will be needed to counter malign influence from Russia and other adversarial nation-states.

B. RECOMMENDATIONS FOR PROTECTING FUTURE ELECTIONS FROM RUSSIAN INTERFERENCE

Like the Cold War's nuclear arms race, the United States may be in a new information operations race with Russia. Based on the evaluation of the Russian actions and the effectiveness of the American responses, this section makes recommendations for protecting future elections that have been drawn from experts in the U.S. government, non-governmental organizations, and academic institutions. The three types of possible actions are broadly categorized as security, transparency, and resiliency measures.[394] Social media companies and the U.S. government have mainly focused on the first two types of measures: security and transparency. Although these measures proved to be successful for the 2020 elections and are essential to safeguarding our democracy and the public

391 Dante Chinni, "Did Biden Win by a Little or a Lot? The Answer Is ... Yes.," NBC News, December 20, 2020, https://www.nbcnews.com/politics/meet-the-press/did-biden-win-little-or-lot-answer-yes-n1251845.

392 Chinni.

393 Frey, *Turnout in 2020 Election Spiked*; Krogstad and Lopez, "Black Voter Turnout Fell in 2016."

394 Cederberg et al., *National Counter-Information Operations Strategy*; DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*; King and Gallagher, *Cybersecurity Lessons from the Pandemic*; *Report on Russian Active Measures*; *Russian Active Measures Campaigns: Volume 1*.

perception of fair elections, they may not be sufficient for future elections because of the current political rancor in the United States. To that end, resiliency measures will be the third critical component to promote a flourishing American democracy.

1. Security Measures

Security measures serve three purposes: (1) prevention of disinformation or data breaches, (2) deterrence of damaging actions or operations, and (3) punishment of criminal or other harmful actions.[395] These recommendations came from an evaluation of U.S. government and private sector actions taken to counter the efforts of the Internet Research Agency and other Russian actors. The most impactful measures against the evolving threat from Russian information operations were distilled from various U.S. government, non-governmental organizations, and academic literature. The proposed security measures, summarized in Table 10, include enhanced cybersecurity, enhanced disinformation detection, economic sanctions, information sharing, and the establishment of a fusion center. Items highlighted in yellow are existing measures. Items highlighted in green are new proposed measures.

[395] Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; U.S. Congress. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns: Volume 1*, 54.

Table 10. Security Measures for Countering Russian Information Operations.

Measure	Description	Responsibility
Enhanced Cybersecurity	Build up cyber expertise and defenses to prevent breaches of election infrastructure and other government infrastructure.[396]	• Government • Private Sector
Enhanced Detection	Use advanced technologies, such as artificial intelligence, to quickly detect and take down disinformation. These technologies can augment other types of content moderation.[397]	• Private Sector
Economic Sanctions	Deter malicious activities and impose costs for actors who seek to interfere in U.S. elections and the democratic process.[398]	• Government
Information Sharing among Government, Social Media Companies, and External Researchers	Share threat intelligence among key stakeholders to detect, identify, and disrupt disinformation campaigns.[399]	• Government • Private Sector • Researchers
National Counter Information Operations Center	Create an interagency fusion center under the Office of the Director of National Intelligence to coordinate strategy, intelligence, and operations regarding disinformation campaigns.[400]	• Government

The first recommendation is for the U.S. government to continue providing cybersecurity training and briefings to relevant stakeholders. The Russians did not cause any significant data breaches of any national-level political organizations or campaigns for

396 Adapted from O'Connor et al., *Cyber-Enabled Foreign Interference*, 6; *Russian Active Measures Campaigns: Volume 1*, 55; *Report on Russian Active Measures*, 121–22.

397 Adapted from Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; Cartwright, Weir, and Frank, "Fighting Disinformation Warfare with Artificial Intelligence," 73.

398 Adapted from Cederberg et al., *National Counter-Information Operations Strategy*, 11; Polyakova, "The Kremlin's Plot against Democracy."

399 Adapted from Cederberg et al., *National Counter-Information Operations Strategy*, 12; Hanlon, *A Long Way to Go*, 10; O'Connor et al., *Cyber-Enabled Foreign Interference*, 6.

400 Adapted from Cederberg et al., *National Counter-Information Operations Strategy*, 12; Terry L. Thompson, "No Silver Bullet: Fighting Russian Disinformation Requires Multiple Actions," *Georgetown Journal of International Affairs* 21 (2020): 182–94, https://doi.org/10.1353/gia.2020.0033.

the 2020 U.S. Elections. Some of this success can be attributed to the cybersecurity training and briefings provided to the political organizations and campaigns by the FBI and DHS.[401] The prevention of data breaches in the future will mean less fodder for the Russians or other adversarial governments to incorporate into disinformation campaigns. These cybersecurity enhancement actions should continue to be used moving forward as technological changes happen rapidly.[402]

The second recommendation calls for advanced technologies, including artificial intelligence, to be developed and deployed on social media and news platforms to enhance the detection, monitoring, and neutralization of covert malign foreign influence activities.[403] These malign activities may take the form of disinformation content, botnet amplifications, or incitement of divisive issues. The neutralization can take the form of traditional account takedowns or marking the accounts and content with labels identifying their origins and providing access to sources of factual information. Advanced technology tools should be developed so platform companies or users may detect disinformation or influence activities and crowdsource the appropriate neutralization methods.[404] The removal of foreign disinformation content can help promote the integrity of American free speech and halt the erosion of trust in the electoral process.[405] Due to the First Amendment (free speech) and Fourth Amendment (privacy) constraints on the U.S. government, advanced detection and removal technologies are best employed by private sector companies.[406]

---

401 Federal Bureau of Investigation, "Combating Foreign Influence"; Federal Bureau of Investigation, "Protected Voices"; Office of the Director of National Intelligence, "Director of National Intelligence Announces Changes to Election Security Briefings."

402 U.S. Congress. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns: Volume 1*, 55–56.

403 Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; Hanlon, *A Long Way to Go*, 2; Marcellino et al., *Foreign Interference in the 2020 Election*.

404 Cartwright, Weir, and Frank, "Fighting Disinformation Warfare with Artificial Intelligence," 73.

405 Suzanne E. Spaulding and Eric Goldstein, *Countering Adversary Threats to Democratic Institutions: An Expert Report* (Washington, DC: Center for Strategic and International Studies, 2018), 4, https://www.csis.org/analysis/countering-adversary-threats-democratic-institutions.

406 Facebook, "The State of Influence Operations 2017–2020," *About Facebook* (blog), May 26, 2021, 5, https://about.fb.com/news/2021/05/influence-operations-threat-report/.

The third recommendation is the continued use of economic sanctions by the U.S. government. Continued sanctions by the Department of Treasury against Russian individuals and entities appeared to have had a significant impact on Russia as a security measure. As anecdotal evidence, one of the primary discussion topics at the infamous Trump Tower meeting was supposed to be the previously mentioned Magnitsky Act.[407] This act imposed severe financial sanctions on the close allies of Putin and continues to be a thorn in his side.[408] The sanctions imposed in 2018 may have an add-on effect to the Magnitsky Act.[409] Economic sanctions should continue to be part of a broad range of tools utilized concurrently by the U.S. government for deterrent and punitive effects.[410]

The fourth recommendation is the establishment of formal information-sharing mechanisms. Information sharing among different organizations is occurring, but on an ad hoc basis, as was seen ahead of the 2020 elections when the FBI shared information with the social media companies to help them detect the disinformation campaigns on their platforms.[411] Information sharing among relevant stakeholders in the malign foreign influence space should be formalized and standardized. Appropriate sharing should occur between social media companies, those companies and the U.S. government, and researchers with the U.S. government and social media companies. The Information Sharing and Analysis Center (ISAC) model has proven successful in different sectors for information sharing. One example of this is the Financial Sector ISAC (FS-ISAC).[412] Currently, no Social Media Sector ISAC exists. This gap is likely because of the competitive nature of social media companies. Still, the FS-ISAC has shown that financial

---

[407] Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 185.

[408] Ioffe, "Why Does the Kremlin Care So Much about the Magnitsky Act?"

[409] Rennack, *U.S. Sanctions on Russia*.

[410] Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; Cederberg et al., *National Counter-Information Operations Strategy*, 12.

[411] Facebook, "September 2020 Coordinated Inauthentic Behavior Report"; Facebook, "October 2020 Coordinated Inauthentic Behavior Report"; Google Threat Analysis Group, "TAG Bulletin," November 17, 2020; @TwitterSafety, "September 2020: Disclosing Networks to Our State-Linked Information Operations Archive."

[412] ISAO Standards Organization, "Financial Services ISAC," ISAO Standards Organization, accessed April 21, 2021, https://www.isao.org/information-sharing-group/sector/financial-services-isac/.

institutions can set aside rivalries for the common good. The benefit of having an information-sharing organization would be to establish norms and best practices for the private sector, in addition to sharing threat indicators for mutual benefit.

The last recommendation is for the U.S. government to establish a National Counter Information Operations Center as an interagency fusion center and focal point for countering disinformation campaigns.[413] The bipartisan U.S. Cyberspace Solarium Commission pointed out that the 2020 National Defense Authorization Act (NDAA) provided a provision wherein the Office of the Director of National Intelligence could form a "Social Media Data and Threat Analysis Center."[414] This center could be modeled after the National Counterterrorism Center, which also operates under the Office of the Director of National Intelligence. The commission envisioned a center that would allow the relevant U.S. government elements to work alongside social media companies to combat disinformation.[415] In April 2021, the Office of the Director of National Intelligence responded to the new legislation by announcing it was establishing "the Foreign Malign Influence Center "in light of evolving threats and in support of growing policy and congressional requirements."[416] As of the writing of this thesis, no further details have been provided by ODNI, but the announcement appears to be in line with the functionality of the center proposed in the 2020 NDAA.

2. Transparency Measures

Transparency measures are designed to build trust and confidence in organizations by sharing relevant information with the general public.[417] The transparency measures proposed include a public communications strategy, content labeling standards, updated

---

413 Cederberg et al., *National Counter-Information Operations Strategy*, 12; Thompson, "No Silver Bullet."

414 King and Gallagher, *Cybersecurity Lessons from the Pandemic*, 12.

415 King and Gallagher, 12.

416 Martin Matishak, "Intelligence Community Creating Hub to Gird against Foreign Influence," *Politico*, April 26, 2021, https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604.

417 Cederberg et al., *National Counter-Information Operations Strategy*, 12.

political advertising and campaign finance laws, and transparency reporting. Table 11 summarizes the proposed transparency measures to combat Russian disinformation campaigns. As with the last table, yellow highlighted items are existing measures, and green highlighted items are new proposed measures.

Table 11. Transparency Measures for Countering Malign Russian Influence.

Measure	Description	Responsibility
Public Communication Strategy	Devise and execute a strategy to counter disinformation in the public sphere, both domestically and overseas, through multiple avenues.[418]	• Government • Private Sector
Content Labeling	Establish and use a standardized method for labeling disinformation and misinformation on websites and social media platforms.[419]	• Private Sector
Transparency Reporting	Provide the public with reports that summarize the quantity and type of disinformation on a company's platform. These reports should include raw data for third parties, such as researchers, to conduct detailed analyses.[420]	• Private Sector • Researchers
Update Political Advertising and Campaign Finance Laws	Strengthen current statutes to improve transparency and prevent foreign entities from purchasing advertisements or donating to political campaigns.[421]	• Government

[418] Adapted from Cederberg et al., 11–12; Marcellino et al., *Foreign Interference in the 2020 Election*; Polyakova, "The Kremlin's Plot against Democracy."

[419] Adapted from Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 2; Hanlon, *A Long Way to Go*, 6; Thompson, "No Silver Bullet."

[420] Adapted from DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1; Hanlon, *A Long Way to Go*, 1; Thompson, "No Silver Bullet."

[421] Adapted from Cederberg et al., *National Counter-Information Operations Strategy*, 12; *Report on Russian Active Measures*, 127.

First, a public communications strategy would be a whole-of-government plan to effectively counter disinformation and propaganda campaigns being waged against the American populace.[422] An effective strategy would involve providing counter-narratives using factual information across various mediums to ensure the public received it, such as through news media and social media outlets.[423] It would also involve exposing false or misleading content and the origins of this information so Americans could understand how they were being targeted.[424]

Second, the private sector companies should also standardize and expand their use of labeling for disinformation, misleading content, and the origins of content.[425] This change would allow users to decide for themselves how to think about and handle the content. As an example, Twitter and Facebook have started labeling misleading tweets and posts by government officials.[426] The Foreign Agent Registration Act (FARA) is the U.S. government's version of what Twitter is doing regarding labeling.[427] FARA mandates that all agents of foreign governments register with the Department of Justice and ensure all of their content in advertising or other messaging is prominently labeled.[428] However, this statute was enacted in 1938 and could use an update to consider current malign influence efforts by Russia and other countries.[429] Congress should provide legislative fixes to enhance the transparency of foreign involvement with U.S. officials or political

---

422 Cederberg et al., *National Counter-Information Operations Strategy*, 11.

423 Cederberg et al., 11.

424 Marcellino et al., *Foreign Interference in the 2020 Election*; Polyakova, "The Kremlin's Plot against Democracy."

425 Hanlon, *A Long Way to Go*, 6.

426 Facebook, "Facebook - Preventing Election Interference"; Twitter, "Elections Integrity."

427 Jessica Brandt and Josh Rudolph, *Spies and Money: Legal Defenses Against Foreign Interference in Political Campaigns* (Washington, DC: Alliance for Security Democracy, German Marshall Fund, 2021), https://securingdemocracy.gmfus.org/spies-and-money-legal-defenses-against-foreign-interference-in-political-campaigns/.

428 Brandt and Rudolph.

429 Carolyn Kenney, Max Bergmann, and James Lamond, *Understanding and Combating Russian and Chinese Influence Operations* (Washington, DC: Center for American Progress, 2019), 8, https://www.hsdl.org/?view&did=822729.

candidates.[430] This addendum includes foreign businesses and consultants who support political campaigns, as well as the disclosure of any financial interests a political candidate may have overseas.

Third, transparency reports are the key mechanism for private sector organizations to share information with the American public.[431] These reports should be expanded to include more nuanced details about foreign influence activities detected and thwarted on social media platforms. All social media companies should also make public their entire archives of malign covert influence content that was taken down.[432] These archives will enable general users, as well as researchers and non-governmental organizations, to analyze the data and provide reports to the American populace. The relationship between the companies and the researchers can help the companies build capacity to analyze malign foreign influence efforts and earn public trust from engaging with independent researchers.

Last, both political advertising and campaign finance laws should be strengthened by closing loopholes to identify the buyers and donors more quickly while also considering the exponential growth of online platforms for advertising and fundraising.[433] Current technology advancements have allowed foreign entities to anonymize or obscure their identities and origins. The House Intelligence Committee noted loopholes in current campaign finance laws that allow foreign entities to provide services to political campaigns.[434] Improved political advertising and campaign finance laws will allow the American public to make informed decisions during the elections.

---

430 McFaul, *Securing American Elections*, 55.

431 DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1; Facebook, "Threat Report," 5; Hanlon, *A Long Way to Go*, 1.

432 DiResta and Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, 1; Hanlon, *A Long Way to Go*, 10; Howard et al., *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*, 40.

433 Cederberg et al., *National Counter-Information Operations Strategy*, 12; "Page 1 - Introduction," n.d., 127.

434 U.S. Congress. House Permanent Select Committee on Intelligence, *Report on Russian Active Measures*, 127.

3. Resiliency Measures

The last but perhaps most crucial measure for consideration is resiliency. The 2021 Intelligence Community's annual threat assessment named Russia as one of "the most serious intelligence threats to the United States" and warned that the Russian government would continue its efforts to propagate dissension in the American populace.[435] In combating future Russian influence campaigns, the two relevant facets of resiliency are improved media literacy and critical thinking for the American public.[436]

Improved media literacy requires both educational and technological components. One study showed that media literacy education for adolescents had "more to do with promoting an understanding of media content and production, rather than simply forming habits of consumption."[437] The government, news media, and social media companies all need to play a role in helping both children and adults understand media content origination and generation.[438] The solutions include public service announcements that are informed by media literacy experts, education programs for school-aged children, and career development or continuing education programs for adults.[439]

Technological enhancements are also needed to improve media literacy. In our current digital age, Americans are awash with overwhelming amounts of information, much of which is false or misleading. A recent study showed that exposure to inaccurate or misleading information on Facebook might slow down or stop users' knowledge

435 Office of the Director of National Intelligence, *2021 Annual Threat Assessment of the U.S. Intelligence Community*, 11.

436 McFaul, *Securing American Elections*, 8.

437 Sebastián Valenzuela, Ingrid Bachmann, and Marcela Aguilar, "Socialized for News Media Use: How Family Communication, Information-Processing Needs, and Gratifications Determine Adolescents' Exposure to News," *Communication Research* 46, no. 8 (2016): 1111, https://doi.org/10.1177/0093650215623833.

438 Spaulding and Goldstein, *Countering Adversary Threats to Democratic Institutions*, 11.

439 Cederberg et al., *National Counter-Information Operations Strategy*, 11; Jon Roozenbeek and Sander van der Linden, "Breaking Harmony Square: A Game That 'Inoculates' against Political Misinformation," *Harvard Kennedy School Misinformation Review* 1, no. 8 (2020): 1–26, https://doi.org/10.37016/mr-2020-47; Spaulding and Goldstein, *Countering Adversary Threats to Democratic Institutions*, 4.

acquisition.[440] All of this content, if made by Americans, is considered free speech. A thornier issue is the artificial amplification of American free speech by Russia or other foreign actors through social media botnets.[441] Artificial intelligence and other advanced technologies will be needed to detect and take down the Russian-controlled bots generating or amplifying malicious content while distinguishing it from First Amendment protected American speech.[442]

One of the essential skills needed for each American is critical thinking, i.e., the ability to discern fact from fiction to make informed conclusions and decisions.[443] Although the focus of this thesis was Russian disinformation campaigns, domestic disinformation operations also featured prominently ahead of the 2020 elections.[444] Critical thinking is an important measure that can be used to examine information despite its origin and is already being taught to some degree as a part of different school subjects such as language arts, mathematics, and social studies. A vital part of a good school curriculum should teach students how to be critical and discerning in their digital media consumption as references and sources for their other coursework.[445]

Furthermore, Americans can learn from other democracies targeted by Russian propaganda. Even with the unrelenting assault of Russian information operations, the democracies in former Soviet Bloc countries appear to have relatively informed and resilient electorates because media literacy and critical thinking are indoctrinated into their

---

[440] Sangwon Lee and Michael Xenos, "Social Distraction? Social Media Use and Political Knowledge in Two U.S. Presidential Elections," *Computers in Human Behavior* 90 (January 2019): 22, https://doi.org/10.1016/j.chb.2018.08.006.

[441] Linvill and Warren, "Engaging with Others," 3.

[442] Bodine-Baron et al., *Countering Russian Social Media Influence*, 12; Cartwright, Weir, and Frank, "Fighting Disinformation Warfare with Artificial Intelligence," 1.

[443] Spaulding and Goldstein, *Countering Adversary Threats to Democratic Institutions*, 11.

[444] Scott Jaspar, "Why Foreign Election Interference Fizzled in 2020," *Atlantic Council* (blog), November 23, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/why-foreign-election-interference-fizzled-in-2020/.

[445] Belinha S. de Abreu, *Teaching Media Literacy*, 2nd ed. (Chicago: American Library Association, 2019), 10.

entire education and news media ecosystem.[446] European media platforms do not feature standardized labeling of disinformation or state-sponsored content. Though these Eastern European countries do not have the economic or technological advantages of the United States, they seem to be inoculated from the effects of Russian disinformation operations.[447] Improved media literacy and critical thinking will help Americans discern what they are reading to make better-informed decisions regarding elections and other vital issues.[448]

During his farewell speech after serving a second term in office, George Washington stated, "Against the insidious wiles of foreign influence...the jealousy of a free people ought to be constantly awake, since history and experience prove that foreign influence is one of the most baneful foes of republic government."[449] Those words seem prescient today, well over two hundred years later. Except for an interlude from the end of the Cold War in 1991 to 2014, Russia has waged a campaign of information warfare to tear the fabric of Western democracy through wide-ranging operations on social media platforms targeting Americans.[450] Both the U.S. government and major social media companies were caught flatfooted in 2016 but took a series of security and transparency actions since then to counter the ongoing Russian efforts targeting U.S. elections specifically and American democracy more broadly. Hopefully, incorporating the existing and proposed measures will help repair and strengthen the framework of American democracy for the 21st century.

---

446 John R. Raines, *Countering Russian Disinformation: Europe Dusts Off the Mighty Wurlitzer*, E-Notes (Philadelphia, PA: Foreign Policy Research Institute, 2015), 6, http://www.fpri.org/docs/haines_-_wurlitzer.pdf.

447 Raines, 6.

448 Spaulding and Goldstein, *Countering Adversary Threats to Democratic Institutions*, 12.

449 George Washington, "Washington's Farewell Address," Digital History, 1796, http://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=3&psid=160.

450 Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2019, 4; National Museum of American History, "The End of the Cold War," Cold War Timeline, 2000, https://americanhistory.si.edu/subs/history/timeline/end/.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abrams, Steve. "Beyond Propaganda: Soviet Active Measures in Putin's Russia." *Connections: The Quarterly Journal* 15, no. 1 (2016): 5–31. https://doi.org/10.11610/Connections.15.1.01.

Abreu, Belinha S. de. *Teaching Media Literacy*. 2nd ed. Chicago: American Library Association, 2019.

Alperovitch, Dmitri. "Our Work with the DNC: Setting the Record Straight." *Crowdstrike Blog* (blog), June 5, 2020. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Barbu, Viorel. "The Hybrid War in the East-West Paradigm." In *Strategic Changes in Security and International Relations*, edited by Dorin Corneliu Pleșcan, Ion Puricel, Daniel Ghiba, Lucian Dragoș Popescu, Ioana Enache, and Tudorel Lehaci, XVI, Part 2:101–12. Bucharest, Romania: "Carol I" National Defence University, 2020. https://www.strategii21.ro/A/2020-04.%20STRATEGIC%20CHANGES%20IN%20SECURITY%20AND%20INTERNATIONAL%20RELATIONS/FSA_2020_VOLUMUL%202.pdf#page=102.

Birch, Sarah. "Perceptions of Electoral Fairness and Voter Turnout." *Comparative Political Studies* 43, no. 12 (December 1, 2010): 1601–22. https://doi.org/10.1177/0010414010374021.

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger. *Countering Russian Social Media Influence*. Santa Monica, CA: RAND Corporation, 2018. https://doi.org/10.7249/RR2740.

Brandt, Jessica, and Josh Rudolph. *Spies and Money: Legal Defenses Against Foreign Interference in Political Campaigns*. Washington, DC: Alliance for Security Democracy, German Marshall Fund, 2021. https://securingdemocracy.gmfus.org/spies-and-money-legal-defenses-against-foreign-interference-in-political-campaigns/.

Brennan Center for Justice. "It's Official: The Election Was Secure | Brennan Center for Justice." *Brennan Center for Justice* (blog), December 11, 2020. https://www.brennancenter.org/our-work/research-reports/its-official-election-was-secure.

Buzzetto-More, Nicole A. "Social Media and Prosumerism." *Issues in Informing Science and Information Technology* 10 (July 2013): 67–80.

Cartwright, Barry, George Weir, and Richard Frank. “Fighting Disinformation Warfare with Artificial Intelligence: Identifying and Combatting Disinformation Attacks in Cloud-Based Social Media Platforms.” In *CLOUD COMPUTING 2019 Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization*, edited by Bob Duncan, Yong Woo Lee, Magnus Westerlund, and Andreas Aßmuth, 73–77. Venice, Italy: IARIA, 2019. https://www.researchgate.net/publication/333024381_CLOUD_COMPUTING_2019_Proceedings_of_the_Tenth_International_Conference_on_Cloud_Computing_GRIDs_and_Virtualization.

Cederberg, Gabriel, Jordan D’Amato, Corinna Fehst, Simon Jones, Kunal Kothari, Aleksandra Milcheva, and Irene Solaiman. *National Counter-Information Operations Strategy*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019. https://www.belfercenter.org/publication/national-counter-information-operations-strategy.

Chekinov, S.G., and S.A. Bogdanov. “The Nature and Content of New Generation War.” *Military Thought*, no. 4 (February 2013): 12–23.

Chinni, Dante. “Did Biden Win by a Little or a Lot? The Answer Is ... Yes.” NBC News, December 20, 2020. https://www.nbcnews.com/politics/meet-the-press/did-biden-win-little-or-lot-answer-yes-n1251845.

Chowdhury, Farhan Asif, Dheeman Saha, Md Rashidul Hasan, Koustuv Saha, and Abdullah Mueen. “Examining Factors Associated with Twitter Account Suspension Following the 2020 U.S. Presidential Election.” *ArXiv* 2101, no. 09575 (January 23, 2021). https://arxiv.org/pdf/2101.09575.pdf.

Clement, J. “Social Media Usage in the United States.” Statista, May 19, 2020. https://www.statista.com/topics/3196/social-media-usage-in-the-united-states/.

Colton, Timothy J., and Michael McFaul. “Russian Democracy under Putin.” *Problems of Post-Communism* 50, no. 4 (July 2003): 12–21. https://doi.org/10.1080/10758216.2003.11656043.

Corasaniti, Nick, Reid J. Epstein, and Jim Rutenberg. “The Times Called Officials in Every State: No Evidence of Voter Fraud.” *New York Times*, November 11, 2020. https://www.nytimes.com/2020/11/10/us/politics/voting-fraud.html.

Cybersecurity and Infrastructure Security Agency. “Election Infrastructure Security.” Cybersecurity and Infrastructure Security Agency. Accessed June 3, 2020. https://www.cisa.gov/election-security.

Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, Public Law 20 (2018). https://www.hsdl.org/?view&did=829787.

Department of Homeland Security and Federal Bureau of Investigation. *GRIZZLY STEPPE – Russian Malicious Cyber Activity*. Washington, DC: Department of Homeland Security and Federal Bureau of Investigation, 2016. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

Department of Homeland Security and Office of the Director of National Intelligence. *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*. Washington, DC: Department of Homeland Security and Office of the Director of National Intelligence, 2016. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

Department of Justice. "Russian National Charged with Interfering in U.S. Political System." United States Attorney's Office Eastern District of Virginia, October 19, 2018. https://www.justice.gov/usao-edva/pr/russian-national-charged-interfering-us-political-system.

———. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." Department of Justice, October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

———. "Special Counsel's Office." Department of Justice Special Counsel's Office, October 16, 2017. https://www.justice.gov/sco.

Department of State. "Senior Administration Official on Russia." U.S. Department of State, August 31, 2017. https://2017-2021.state.gov/senior-administration-official-on-russia/.

DeSilver, Drew. "Turnout Soared in 2020 as Nearly Two-Thirds of Eligible U.S. Voters Cast Ballots for President." *Pew Research Center Fact Tank* (blog), January 28, 2021. https://www.pewresearch.org/fact-tank/2021/01/28/turnout-soared-in-2020-as-nearly-two-thirds-of-eligible-u-s-voters-cast-ballots-for-president/.

DiResta, Renée, and Shelby Grossman. *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*. Palo Alto, CA: Stanford University, 2019. https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks.

DiResta, Renee, Kris Shaffer, Becky Ruppel, Robert Matney, Ryan Fox, Jonathan Albright, Ben Johnson, and Canfield Research. *The Tactics & Tropes of the Internet Research Agency*. New York: New Knowledge, 2018.

Elections Infrastructure Government Coordinating Council, and Election Infrastructure Sector Coordinating Executive Committee. "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees," November 12, 2020. https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

Evanina, William. "Statement by NCSC Director William Evanina: 100 Days Until Election 2020." Office of the Director of National Intelligence, July 24, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020.

———. "Statement by NCSC Director William Evanina: Election Threat Update for the American Public." Office of the Director of National Intelligence, August 7, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

Ewing, Philip. "Fact Check: Why Didn't Obama Stop Russia's Election Interference In 2016?" National Public Radio, February 21, 2018. https://www.npr.org/2018/02/21/587614043/fact-check-why-didnt-obama-stop-russia-s-election-interference-in-2016.

Fabian, Sandor. "The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy." *Defense & Security Analysis* 35, no. 3 (2019): 308–25. https://doi.org/10.1080/14751798.2019.1640424.

Facebook. "April 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), May 5, 2020. https://about.fb.com/news/2020/05/april-cib-report/.

———. "August 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), September 1, 2020. https://about.fb.com/wp-content/uploads/2020/09/August-2020-CIB-Report.pdf.

———. "Facebook - Preventing Election Interference." About Facebook, 2020. https://about.fb.com/actions/preventing-election-interference/.

———. "February 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), March 2020. https://about.fb.com/wp-content/uploads/2020/03/February-2020-CIB-Report.pdf.

———. "March 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), April 2, 2020. https://about.fb.com/news/2020/04/march-cib-report/.

———. "October 2020 Coordinated Inauthentic Behavior Report." *Facebook News* (blog), October 27, 2020. https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-mexico-iran-myanmar/.

———. “September 2020 Coordinated Inauthentic Behavior Report.” *Facebook News* (blog), September 2020. https://about.fb.com/wp-content/uploads/2020/10/September-2020-CIB-Report.pdf.

———. “The State of Influence Operations 2017-2020.” *About Facebook* (blog), May 26, 2021. https://about.fb.com/news/2021/05/influence-operations-threat-report/.

Federal Bureau of Investigation. “Combating Foreign Influence.” What We Investigate. Accessed October 18, 2020. https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

———. “FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure.” FBI Press Releases, January 16, 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-policy-for-notifying-state-and-local-election-officials-of-cyber-intrusions-affecting-election-infrastructure.

———. “FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure — FBI.” FBI Press Releases, January 16, 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-policy-for-notifying-state-and-local-election-officials-of-cyber-intrusions-affecting-election-infrastructure.

———. “Protected Voices.” Federal Bureau of Investigation. Accessed August 5, 2020. https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices.

Feiner, Lauren, and Megan Graham. “Twitter Unveils Final Details for Political Ad Ban, but It’s Still Looking Murky.” CNBC, November 15, 2019. https://www.cnbc.com/2019/11/15/twitter-unveils-new-political-ad-policy.html.

Frankovic, Kathy. “Republicans Still Not Convinced of Russian Election Meddling.” YouGov, August 10, 2018. https://today.yougov.com/topics/politics/articles-reports/2018/08/10/republicans-still-not-convinced-russian-election-m.

Freelon, Deen, and Tetyana Lokot. “Russian Disinformation Campaigns on Twitter Target Political Communities across the Spectrum. Collaboration between Opposed Political Groups Might Be the Most Effective Way to Counter It.” *Harvard Kennedy School Misinformation Review* 1, no. 1 (2020): 1–9. https://doi.org/10.37016/mr-2020-003.

Frey, William H. *Turnout in 2020 Election Spiked among Both Democratic and Republican Voting Groups, New Census Data Shows*. Washington, DC: Brookings, 2021. https://www.brookings.edu/research/turnout-in-2020-spiked-among-both-democratic-and-republican-voting-groups-new-census-data-shows/.

Fridman, Ofer. “On the ‘Gerasimov Doctrine’: Why the West Fails to Beat Russia to the Punch.” *PRISM* 8, no. 2 (2019): 100–113.

Galeotti, Mark. “The Mythical ‘Gerasimov Doctrine’ and the Language of Threat.” *Critical Studies on Security* 7, no. 2 (2019): 157–61. https://doi.org/10.1080/21624887.2018.1441623.

Garrett, R. Sam. *Federal Role in U.S. Campaigns and Elections: An Overview*. CRS Report No. R45302. Washington, DC: Congressional Research Service, 2018. https://fas.org/sgp/crs/misc/R45302.pdf.

Gerasimov, Valery. “The Value of Science in Prediction.” *Military-Industrial Kurier*, February 27, 2013. https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf.

Global Engagement Center. *Pillars of Russia’s Disinformation and Propaganda Ecosystem*. Washington, DC: Department of State, 2020. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

Goodin, Dan. “NSA and FBI Warn That New Linux Malware Threatens National Security.” *Ars Technica*, August 13, 2020. https://arstechnica.com/information-technology/2020/08/nsa-and-fbi-warn-that-new-linux-malware-threatens-national-security/.

Google Threat Analysis Group. “Google Safety & Security.” *Google* (blog). Accessed May 27, 2020. https://blog.google/technology/safety-security/.

———. “TAG Bulletin: Q2 2020.” *Google: Updates from Threat Analysis Group* (blog), August 5, 2020. https://blog.google/threat-analysis-group/tag-bulletin-q2-2020/.

———. “TAG Bulletin: Q4 2020.” Google: Updates from Threat Analysis Group, November 17, 2020. https://blog.google/threat-analysis-group/tag-bulletin-q4-2020/.

Gould-Davies, Nigel. “Russia, the West and Sanctions.” *Survival* 62, no. 1 (January 2, 2020): 7–28. https://doi.org/10.1080/00396338.2020.1715060.

Graphika Team. *Step Into My Parler; Suspected Russian Operation Targeted Far-Right American Users on Platforms Including Gab and Parler, Resembled Recent IRA-Linked Operation That Targeted Progressives*. New York: Graphika, 2020. https://graphika.com/reports/step-into-my-parler/.

Grimmer, Justin, Haritz Garro, and Andrew Eggers. “No Evidence For Voter Fraud: A Guide To Statistical Claims About The 2020 Election.” Text. Palo Alto, CA: Hoover Institution, February 3, 2021. https://www.hoover.org/research/no-evidence-voter-fraud-guide-statistical-claims-about-2020-election.

Grossman, Shelby, Daniel Bush, and Renée DiResta. "Evidence of Russia-Linked Influence Operations in Africa." *Stanford Internet Observatory* (blog), October 30, 2019. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf.

Hanlon, Bradley. *A Long Way to Go - Analyzing Facebook, Twitter, and Google's Efforts to Combat Foreign Interference*. Policy Brief No. 41. Washington, DC: German Marshall Fund of the United States, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/12/A-Long-Way-to-Go-Analyzing-Facebook-Twitter-and-Googles-Efforts-to-Combat-Foreign-Interference.pdf.

Hardwick, Joshua. "Top 100 Most Visited Websites by Search Traffic (as of 2020)." *Ahrefs* (blog), May 12, 2020. https://ahrefs.com/blog/most-visited-websites/.

Hartmann, Margaret. "How Conservatives View Russia's Alleged Meddling in the U.S. Election." *New York Magazine*, December 16, 2016. https://nymag.com/intelligencer/2016/12/how-the-right-is-talking-about-russias-election-meddling.html.

Helmus, Todd C., James V. Marrone, Marek N. Posard, and Danielle Schlang. *Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA704-3.html.

Higgins, Tucker. "Obama Response to 2016 Russian Election Meddling Had 'many Flaws,' Senate Report Finds." CNBC, February 6, 2020. https://www.cnbc.com/2020/02/06/obama-response-to-2016-russian-meddling-had-many-flaws-senate-report.html.

Hochschild, Jennifer. "If Democracies Need Informed Voters, How Can They Thrive While Expanding Enfranchisement?" *Election Law Journal: Rules, Politics, and Policy* 9, no. 2 (2010): 111–23.

Howard, Philip N., Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. *The IRA, Social Media, and Political Polarization in the United States, 2012–2018*. Oxford, UK: University of Oxford, Computational Propaganda Research Project, 2019. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs.

Ioffe, Julia. "Why Does the Kremlin Care So Much about the Magnitsky Act?" *The Atlantic*, July 27, 2017. https://www.theatlantic.com/international/archive/2017/07/magnitsky-act-kremlin/535044/.

Isaac, Mike, and Kate Conger. “Google, Facebook and Others Broaden Group to Secure U.S. Election.” *New York Times*, August 12, 2020. https://www.nytimes.com/2020/08/12/technology/google-facebook-coalition-us-election.html.

ISAO Standards Organization. “Financial Services ISAC.” ISAO Standards Organization. Accessed April 21, 2021. https://www.isao.org/information-sharing-group/sector/financial-services-isac/.

Jaspar, Scott. “Why Foreign Election Interference Fizzled in 2020.” *Atlantic Council* (blog), November 23, 2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/why-foreign-election-interference-fizzled-in-2020/.

Jojart, Krisztian. “Russia Military Thinking and the Hybrid War.” *Scientific Periodical of the Hungarian Military National Security Service*, no. 1 (2019): 82.

Kang, Cecilia, Nicholas Fandos, and Mike Isaac. “Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill.” *New York Times*, October 31, 2017. https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html.

Kartapolov, A. V. “Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods.” *Journal of the Academy of Military Science* 51, no. 2 (2015): 26–36.

Kenney, Carolyn, Max Bergmann, and James Lamond. *Understanding and Combating Russian and Chinese Influence Operations*. Washington, DC: Center for American Progress, 2019. https://www.hsdl.org/?view&did=822729.

King, Angus, and Mike Gallagher. *Cybersecurity Lessons from the Pandemic*. CSC White Paper #1. Washington, DC: U.S. Cyberspace Solarium Commission, 2020. https://www.solarium.gov/public-communications/pandemic-white-paper.

Kollars, Nina A., and Michael B. Petersen. “Feed the Bears, Starve the Trolls: Demystifying Russia’s Cybered Information Confrontation Strategy.” *The Cyber Defense Review* Special edition (2019): 145–60.

Krebs, Christopher. “Statement from CISA Director Krebs Following Final Day of Voting.” Cybersecurity and Infrastructure Security Agency, November 4, 2020. https://www.cisa.gov/news/2020/11/04/statement-cisa-director-krebs-following-final-day-voting.

Krogstad, Jens Manuel, and Mark Hugo Lopez. “Black Voter Turnout Fell in 2016, Even as a Record Number of Americans Cast Ballots.” FactTank: News in the Numbers, May 12, 2017. https://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/.

Laird, Chryl. “Why Black Voter Turnout Fell in 2016.” Vox, January 15, 2020. https://www.vox.com/mischiefs-of-faction/2018/1/15/16891020/black-voter-turnout.

Laurence, Peter. “Powerful ‘Putin’s Chef’ Cooks up Murky Deals.” *BBC News*. November 4, 2019, Online edition, sec. Europe. https://www.bbc.com/news/world-europe-50264747.

Lee, Sangwon, and Michael Xenos. “Social Distraction? Social Media Use and Political Knowledge in Two U.S. Presidential Elections.” *Computers in Human Behavior* 90 (January 2019): 18–25. https://doi.org/10.1016/j.chb.2018.08.006.

Leighton, Heather. “For Instagram’s 10th Birthday, Experts Predict The Future Of Meme Culture.” *Forbes*, October 7, 2020. https://www.forbes.com/sites/heatherleighton/2020/10/07/for-instagrams-10th-birthday-experts-predict-the-future-of-meme-culture/.

Linvill, Darren L., and Patrick L. Warren. “Engaging with Others: How the IRA Coordinated Information Operation Made Friends.” *Harvard Kennedy School Misinformation Review* 1, no. 2 (April 2020): 1–14. https://doi.org/10.37016/mr-2020-011.

Lukito, Josephine. “Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017.” *Political Communication* 37, no. 2 (2020): 238–55. https://doi.org/10.1080/10584609.2019.1661889.

Marcellino, William, Christian Johnson, Marek N. Posard, and Todd C. Helmus. *Foreign Interference in the 2020 Election: Tools for Detecting Online Election Interference*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA704-2.html.

Matishak, Martin. “Intelligence Community Creating Hub to Gird against Foreign Influence.” *Politico*, April 26, 2021. https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604.

McFaul, Michael, ed. *Securing American Elections*. Palo Alto, CA: Stanford University, Cyber Policy Center, 2019. https://www.hsdl.org/?view&did=827251.

Miller, Gregory A., Edward Perez, E. John Sebes, and Sergio Valente. *Critical Democracy Infrastructure: Protecting American Elections in the Digital Age Threats, Vulnerabilities, and Countermeasures as a National Security Agenda*. 2nd ed. Palo Alto, CA: OSET Institute, 2020. https://trustthevote.org/wp-content/uploads/2020/05/01May20_CDI-2nd.pdf.

Misra, Jordan. “Voter Turnout Rates among All Voting Age and Major Racial and Ethnic Groups Were Higher Than in 2014.” Behind the 2018 U.S. Midterm Election Turnout, April 23, 2019. https://www.census.gov/library/stories/2019/04/behind-2018-united-states-midterm-election-turnout.html.

Monje Jr., Carlos. “2018 U.S. Midterm Elections Review.” *Twitter Company* (blog), January 31, 2019. https://blog.twitter.com/en_us/topics/company/2019/18_midterm_review.html.

Mueller, Robert. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: Department of Justice, 2019.

———. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: Department of Justice, 2019. https://www.hsdl.org/?view&did=824221.

Murthy, Dhiraj, Alison B. Powell, Ramine Tinati, Nick Anstead, Leslie Carr, Susan J. Halford, and Mark Weal. “Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital.” *International Journal of Communication* 10 (2016): 4952–71.

Nakashima, Ellen. “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms.” *Washington Post*, February 27, 2019. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

National Museum of American History. “The End of the Cold War.” Cold War Timeline, 2000. https://americanhistory.si.edu/subs/history/timeline/end/.

National Security Agency, and Federal Bureau of Investigation. *Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*. Rev 1.0. Washington, DC: National Security Agency & Federal Bureau of Investigation, 2020. https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_drovorub_russian_gru_malware_aug_2020.PDF.

Nimmo, Ben, Camille François, C Shawn Eib, and Léa Ronzaud. “IRA Again: Unlucky Thirteen.” New York, NY: Graphika, September 2020. https://public-assets.graphika.com/reports/graphika_report_ira_again_unlucky_thirteen.pdf.

Nimmo, Ben, Camille François, C. Shawn Eib, Lea Ronzaud, Rodrigo Ferreira, Chris Hernon, and Tim Kostelancik. *Secondary Infektion*. New York: Graphika, 2020. https://secondaryinfektion.org/report/secondary-infektion-at-a-glance/.

Nuñez, Michael. “The Surprising Truth about Twitter’s Political Ad Ban.” *Forbes*, November 1, 2019. https://www.forbes.com/sites/mnunez/2019/11/01/the-surprising-truth-about-twitters-political-ad-ban/.

O'Connor, Sarah, Fergus Hanson, Emilia Currey, and Tracy Beattie. *Cyber-Enabled Foreign Interference in Elections and Referendums*. Policy Brief Report No. 41. Canberra, Australia: Australian Strategic Policy Institute, 2020. https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums.

Office of the Director of National Intelligence. *2021 Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, 2021. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2204-2021-annual-threat-assessment-of-the-u-s-intelligence-community.

———. *Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution*. Washington, DC: Office of the Director of National Intelligence, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

———. "Director of National Intelligence Announces Changes to Election Security Briefings." Office of the Director of National Intelligence, May 15, 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2118-director-of-national-intelligence-announces-changes-to-election-security-briefings.

———. "DNI Coats Statement on the IC's Response to EO 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a U.S. Election." Office of the Director of National Intelligence, December 21, 2018. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2018/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election.

———. "Intelligence Community Assessment on Foreign Threats to the 2020 U.S. Federal Elections." Intelligence Community Assessment. Washington, DC, March 16, 2021. https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2192-intelligence-community-assessment-on-foreign-threats-to-the-2020-u-s-federal-elections.

———. "Members of the IC." Office of the Director of National Intelligence. Accessed April 27, 2021. https://www.dni.gov/index.php/what-we-do/members-of-the-ic. "Page 1 - Introduction," n.d.

Parks, Miles, and Philip Ewing. "Foreign Interference Persists And Techniques Are Evolving, Big Tech Tells Hill." National Public Radio, June 18, 2020. https://www.npr.org/2020/06/18/880349422/foreign-interference-persists-and-techniques-are-evolving-big-tech-tells-hill.

Polyakova, Alina. "The Kremlin's Plot against Democracy." *Foreign Affairs*, October 2020.

Homeland Security Today. “Protecting Every Voice: FBI Expands Suite of Resources on Election Security,” October 23, 2019. https://www.hstoday.us/subject-matter-areas/infrastructure-security/protecting-every-voice-fbi-expands-suite-of-resources-on-election-security/.

Rad, Armin A., Mohammad S. Jalali, and Hazhir Rahmandad. “How Exposure to Different Opinions Impacts the Life Cycle of Social Media.” *Annals of Operations Research* 268, no. 1 (2018): 63–91. https://doi.org/10.1007/s10479-017-2554-8.

Raines, John R. *Countering Russian Disinformation: Europe Dusts Off the Mighty Wurlitzer*. E-Notes. Philadelphia, PA: Foreign Policy Research Institute, 2015. http://www.fpri.org/docs/haines_-_wurlitzer.pdf.

Reality Check Team. “US Election 2020: Fact-Checking Trump Team’s Main Fraud Claims.” BBC News, November 23, 2020. https://www.bbc.com/news/election-us-2020-55016029.

Rennack, Dianne E. *U.S. Sanctions on Russia: An Overview*. CRS Report No. IF10779. Washington, DC: Congressional Research Service, 2018. https://www.hsdl.org/?view&did=813693.

Robinson, Ryan. “7 Top Social Media Sites in 2020.” Adobe Spark. Accessed July 21, 2021. https://www.adobe.com/express/learn/blog/top-social-media-sites.

Romm, Tony. “5 Things We Learned When Facebook, Google, and Twitter Testified to Congress About Russia’s Election Meddling.” Recode Daily, October 31, 2017. https://www.vox.com/2017/10/31/16588032/facebook-google-twitter-congress-russia-election-2016-tech-hearings-franken-cruz-graham.

Roozenbeek, Jon, and Sander van der Linden. “Breaking Harmony Square: A Game That ‘Inoculates’ against Political Misinformation.” *Harvard Kennedy School Misinformation Review* 1, no. 8 (2020): 1–26. https://doi.org/10.37016/mr-2020-47.

Roth, Yoel, and Nick Pickles. “Updating Our Approach to Misleading Information.” *Only on Twitter* (blog), May 11, 2020. https://blog.twitter.com/en_us /topics/product/2020/updating-our-approach-to-misleading-information.html.

Sattelberger, F. “Optimising Media Marketing Strategies in a Multi-Platform World: An Inter-Relational Approach to Pre-Release Social Media Communication and Online Searching.” *Journal of Media Business Studies* 12, no. 1 (2015): 66–88. https://doi.org/10.1080/16522354.2015.1027117.

Savage, Patrick. *Russian Social Media Information Operations: How Russia Has Used Social Media to Influence U.S. Politics*. Washington, DC: American Security Project, 2017. https://www.hsdl.org/?view&did=808713.

Shahani, Aarti. “Zuckerberg Denies Fake News on Facebook Had Impact On the Election.” *All Things Considered*. Washington, DC: National Public Radio, 11/112016. https://www.npr.org/sections/alltechconsidered/2016/11/11/501743684/zuckerberg-denies-fake-news-on-facebook-had-impact-on-the-election.

Snider, Mike. “What’s at Stake for Facebook’s Mark Zuckerberg as He Testifies for Day 2.” *USA Today*, April 10, 2018. https://www.usatoday.com/story/tech/news/2018/04/10/whats-stake-facebooks-mark-zuckerberg-he-testifies-before-congress/503017002/.

Spaulding, Suzanne E., and Eric Goldstein. *Countering Adversary Threats to Democratic Institutions: An Expert Report*. Washington, DC: Center for Strategic and International Studies, 2018. https://www.csis.org/analysis/countering-adversary-threats-democratic-institutions.

Stanford Internet Observatory. “Analysis of June 2020 Twitter Takedowns Linked to China, Russia, and Turkey.” *Stanford Internet Observatory* (blog), June 11, 2020. https://cyber.fsi.stanford.edu/io/news/june-2020-twitter-takedown.

Starbird, Kate, Ahmer Arif, and Tom Wilson. “Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations.” *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 2019): 1–26. https://doi.org/10.1145/3359229.

Steinmetz, Katy. “Lawmakers Hint at Regulating Social Media During Hearing with Facebook and Twitter Execs.” *Time*, September 5, 2018. https://time.com/5387560/senate-intelligence-hearing-facebook-twitter/.

Strohm, Chris. “Russian Hacking Began as ‘Grizzly Steppe.’” *Chicago Tribune*, December 30, 2016, sec. Nation & World. https://www.chicagotribune.com/nation-world/ct-russian-hack-grizzly-steppe-20161230-story.html.

Stubbs, Jack. “Duped by Russia, Freelancers Ensnared in Disinformation Campaign by Promise of Easy Money.” Reuters, September 3, 2020. https://www.reuters.com/article/us-usa-election-facebook-russia-idUSKBN25T35E.

———. “Exclusive: Russian Operation Masqueraded as Right-Wing News Site to Target U.S. Voters - Sources.” Reuters, October 1, 2020. https://www.reuters.com/article/usa-election-russia-disinformation-idUSKBN26M5OP.

Thomas, Timothy. “The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking.” *Journal of Slavic Military Studies* 29, no. 4 (2016): 554–75. https://doi.org/10.1080/13518046.2016.1232541.

———. “The Evolving Nature of Russia’s Way of War.” *Military Review* 97, no. 4 (August 2017): 34–42.

Thompson, Terry L. “No Silver Bullet: Fighting Russian Disinformation Requires Multiple Actions.” *Georgetown Journal of International Affairs* 21 (2020): 182–94. https://doi.org/10.1353/gia.2020.0033.

Thornton, Rod. “The Russian Military’s New ‘Main Emphasis.’” *RUSI Journal* 162, no. 4 (2017): 18–28. https://doi.org/10.1080/03071847.2017.1381401.

THR Staff. “Donald Trump Caught on Hot Mic in 2005 Talking About Women: ‘When You’re a Star, They Let You Do It.’” News. Hollywood Reporter, October 7, 2016. https://www.hollywoodreporter.com/news/donald-trump-caught-hot-mic-936343.

Twitter. “Elections Integrity: We’re Focused on Serving the Public Conversation.” About Twitter, 2020. https://about.twitter.com/en_us/advocacy/elections-integrity.html.

———. “Retrospective Review Twitter, Inc. and the 2018 Midterm Elections in the United States.” Twitter, February 4, 2019. https://blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf.

@TwitterSafety. “June 2020: Disclosing Networks of State-Linked Information Operations We’ve Removed.” *Twitter Information Operations* (blog), June 12, 2020. https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020.html.

———. “October 2020: Disclosing Networks to Our State-Linked Information Operations Archive.” *Twitter Information Operations* (blog), October 8, 2020. https://blog.twitter.com/en_us/topics/company/2020/disclosing-removed-networks-to-our-archive-of-state-linked-information.html.

———. “September 2020: Disclosing Networks to Our State-Linked Information Operations Archive.” Social Media. *Twitter Information Operations* (blog), September 1, 2020. https://twitter.com/TwitterSafety/status/1300848632120242181.

Uhlmann, Allon J., and Stephen McCombie. “The Russian Gambit and the U.S. Intelligence Community: Russia’s Use of Kompromat and Implausible Deniability to Optimize Its 2016 Information Campaign against the U.S. Presidential Election.” *Library Trends* 68, no. 4 (2020): 679–96. https://doi.org/10.1353/lib.2020.0017.

U.S. Congress. House Permanent Select Committee on Intelligence. *Report of the House Permanent Select Committee on Intelligence on Russian Active Measures Together with Minority Views*. H.Rept 115-1110. Washington, DC: Government Publishing Office, 2019. https://www.congress.gov/115/crpt/hrpt1110/CRPT-115hrpt1110.pdf.

U.S. Congress. Senate Select Committee on Intelligence. *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts against Election Infrastructure with Additional Views*. Senate, 116th Cong., 1st Sess. Washington, DC: U.S. Congress. Senate, 2017. https://www.intelligence.senate.gov /sites/default/files/documents/Report_Volume1.pdf.

———. *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures, Campaigns, and Interference In the 2016 U.S. Election, Volume 2: Russia's Use Of Social Media With Additional Views*. Senate, 116th Cong., 1st Sess. Washington, DC: U.S. Congress. Senate, 2019. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume 2.pdf.

U.S. Congress. House of Representatives. "HPSCI Minority Open Hearing Exhibits." Permanent Select Committee on Intelligence. Accessed March 20, 2021. https://intelligence.house.gov/hpsci-11-1/hpsci-minority-open-hearing-exhibits.htm.

U.S. Congress. House of Representatives. *Facebook, Google, and Twitter: Examining the Content Filtering Practices of Social Media Giants, House of Representatives*, House of Representatives, 115th Cong., 1st sess., July 17, 2018. https://www.hsdl.org/?view&did=821944.

U.S. Congress. House Permanent Select Committee on Intelligence. *Report on Russian Active Measures*. Washington, DC: U.S. Congress. House, 2018. https://republicans-intelligence.house.gov/uploadedfiles/ final_russia_investigation_report.pdf.

U.S. Congress. Senate. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel I: Hearing before the Select Committee on Intelligence*, Senate, 115th Cong., 1st sess., March 20, 2017, 55.

———. *Mass Violence, Extremism, and Digital Responsibility: Hearing before the Committee on Commerce, Science, and Transportation*, Senate, 116th Cong., 1st sess., September 18, 2019. https://www.commerce.senate.gov/2019/9/mass-violence-extremism-and-digital-responsibility.

———. *Examining Irregularities in the 2020 Election: Hearing before the Committee on Homeland Security and Governmental Affairs*, Senate, 116th Cong., 2nd Session, December 16, 2020. https://www.hsgac.senate.gov/imo/media/doc/Testimony-Krebs-2020-12-16.pdf.

U.S. Congress. Senate. Committee on Foreign Relations. *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*. S.Rpt. 115-21. Washington, DC: Government Publishing Office, 2018. https://www.hsdl.org/?view&did=806949.

U.S. vs. Internet Research Agency LLC, No. 18-cr-00032-DLF (U.S. District Court for the District of Columbia February 16, 2018).

Valenzuela, Sebastián. "Unpacking the Use of Social Media for Protest Behavior: The Roles of Information, Opinion Expression, and Activism." *American Behavioral Scientist* 57, no. 7 (July 2013): 920–42. https://doi.org/10.1177/0002764213479375.

Valenzuela, Sebastián, Ingrid Bachmann, and Marcela Aguilar. "Socialized for News Media Use: How Family Communication, Information-Processing Needs, and Gratifications Determine Adolescents' Exposure to News." *Communication Research* 46, no. 8 (2016): 1095–1118. https://doi.org/10.1177/0093650215623833.

Wagner, Kurt. "Facebook Meets With FBI to Discuss 2020 Election Security." Bloomberg, September 4, 2019. https://www.bloomberg.com/news/articles/2019-09-04/facebook-meets-with-fbi-to-discuss-2020-election-security.

Walker, Robert E. "Combating Strategic Weapons of Influence on Social Media." Master's thesis, Naval Postgraduate School, 2019. http://hdl.handle.net/10945/62826.

Wanless, Alicia, and Laura Walters. "How Journalists Become an Unwitting Cog in the Influence Machine." Carnegie Endowment for International Peace, October 13, 2020. https://carnegieendowment.org/2020/10/13/how-journalists-become-unwitting-cog-in-influence-machine-pub-82923.

Ward, Clarissa, Katie Polglase, Sebastian Shukla, Gianluca Mezzofiore, and Tim Lister. "Russian Election Meddling Is Back — Via Ghana and Nigeria — and in Your Feeds." CNN, April 11, 2020. https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html.

Washington, George. "Washington's Farewell Address." Digital History, 1796. http://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=3&psid=160.

Weed, Matthew. *Global Engagement Center: Background and Issues*. CRS Report No. IN10744. Washington, DC: Congressional Research Service, 2017. https://fas.org/sgp/crs/row/IN10744.pdf.

Weir, Kellie J. "Safeguarding Democracy: Increasing Election Integrity through Enhanced Voter Verification." Master's thesis, Naval Postgraduate School, 2018. https://www.hsdl.org/?view&did=811383.

Wiener, Jon. *How We Forgot the Cold War: A Historical Journey Across America*. Berkeley: University of California Press, 2012. https://books.google.com/books?hl=en&lr=&id=w_Sa-F8DXhgC&oi=fnd&pg=PA1&dq=american+memory+of+the+cold+war&ots=kvRphYu1TG&sig=sVpOOZBAdl0fqcHCskio5uy7tiE#v=onepage&q=american%20memory%20of%20the%20cold%20war&f=false.

Wilhelm, Thomas. "A Russian Military Framework for Understanding Influence in the Competition Period." *Military Review* 100, no. 4 (August 2020): 32–41.

Woolley, Samuel C., and Philip N. Howard. "Political Communication, Computational Propaganda, and Autonomous Agents." *National Science Foundation Public Access Repository*, September 3, 2016, 6.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California