116TH CONGRESS *1st Session* | SENATE | REPORT 116-XX

(U) 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

[redacted]

CONTENTS

I. (U) INTRODUCTION 3
II. (U) FINDINGS 4
III. (U) THE REACH OF SOCIAL MEDIA 8
IV. (U) RUSSIAN USE OF DISINFORMATION 11
A. (U) Russian Active Measures 12
B. (U) Russia's Military and Information Warfare 13
C. (U) Russia's Weaponization of Social Media 14
D. (U) Russian Social Media Tactics 15
E. (U) Features of Russian Active Measures 20
V. (U) THE INTERNET RESEARCH AGENCY 22
A. (U) Yevgeniy Prigozhin and the Kremlin 23
B. (U) IRA Operations 24
C. (U) The Role of the IRA Troll 25
D. (U) Troll Narratives 28
VI. (U) IRA ACTIVITIES AGAINST THE UNITED STATES IN 2016 29
A. (U) Origins of IRA Activity in the United States 29
B. (U) IRA Operations Explicitly Targeting the 2016 U.S. Election 32
C. (U) Other IRA Operations Targeting U.S. Politicians and Society 37
D. (U) IRA Use of Paid Advertisements 40
E. (U) The IRA Information Warfare Campaign 41
F. (U) Ongoing IRA Activities 42
VII. (U) IRA USE OF SOCIAL MEDIA BY PLATFORM 43
VIII. (U) OTHER RUSSIAN SOCIAL MEDIA INFORMATION WARFARE EFFORTS 63
A. (U) Main Intelligence Directorate (GRU) 63
B. [redacted] 69
C. (U) Other Russian Government Activities 70
IX. (U) U.S. GOVERNMENT RESPONSE 71
X. (U) THE COMMITTEE'S REVIEW OF RUSSIA'S USE OF SOCIAL MEDIA 76
XI. (U) RECOMMENDATIONS 78
A. (U) Industry Measures 78
B. (U) Congressional Measures 80
C. (U) Executive Branch Measures 81
D. (U) Other Measures 81
XII. (U) Additional Views of Senator Wyden 83

[redacted]

I. (U) INTRODUCTION

[redacted] In 2016, Russian operatives associated with the St. Petersburg-based Internet Research Agency (IRA) used social media to conduct an information warfare campaign designed to spread disinformation and societal division in the United States.[1] [redacted] Masquerading as Americans, these operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users in the United States. This campaign sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election. [redacted]

(U) The Senate Select Committee on Intelligence undertook a study of these events, consistent with its congressional mandate to oversee and conduct oversight of the intelligence activities and programs of the United States Government, to include the effectiveness of the Intelligence Community's counterintelligence function. In addition to the work of the professional staff of the Committee, the Committee's findings drew from the input of cybersecurity professionals, social media companies, U.S. law enforcement and intelligence agencies, and researchers and experts in social network analysis, political content, disinformation, hate speech, algorithms, and automation, working under the auspices of the Committee's Technical Advisory Group (TAG).[3] The efforts of these TAG researchers led to the release of two public reports on the IRA's information warfare campaign, based on data provided to the Committee by the social media companies.[4] These reports provided the

---

[1] **(U)** For purposes of this Volume, "information warfare" refers to Russia's strategy for the use and management of information to pursue a competitive advantage. *See* Congressional Research Service, *Defense Primer: Information Operations*, December 18, 2018.

[2] [redacted]

[3] **(U)** The TAG is an external group of experts the Committee consults for substantive technical advice on topics of importance to Committee activities and oversight. In this case, the Committee requested the assistance of two independent working groups, each with the technical capabilities and expertise required to analyze the data. The two working groups were led by three TAG members, with John Kelly, the founder and CEO of the social media analytics firm Graphika, and Phil Howard, an expert academic researcher at the Oxford Internet Institute, leading one working group, and Renee DiResta, the Director of Research at New Knowledge, a cybersecurity company dedicated to protecting the public sphere from disinformation attacks, leading the other.

[4] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/; Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018,

Committee, social media companies, U.S. law enforcement, international partners, fellow researchers and academics, and the American public with an enhanced understanding of how Russia-based actors, at the direction of the Russian government, effectuated a sustained campaign of information warfare against the United States aimed at influencing how this nation's citizens think about themselves, their government, and their fellow Americans. The Committee supports the findings therein.

(U) The Committee also engaged directly with a number of social media companies in the course of this study. The willingness of these companies to meet with Members and staff, share the results of internal investigations, and provide evidence of foreign influence activity collected from their platforms was indispensable to this study. Specifically, the Committee's ability to identify Russian activity on social media platforms was limited. As such, the Committee was largely reliant on social media companies to identify Russian activity and share that information with the Committee or with the broader public. Thus, while the Committee findings describe a substantial amount of Russian activity on social media platforms, the full scope of this activity remains unknown to the Committee, the social media companies, and the broader U.S. Government.

II. (U) FINDINGS

1. **(U)** The Committee found that the IRA sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Kremlin.

   (U) The Committee found that the IRA's information warfare campaign was broad in scope and entailed objectives beyond the result of the 2016 presidential election. Further, the Committee's analysis of the IRA's activities on social media supports the key judgments of the January 6, 2017 Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent US Elections," that "Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency."[5] However, where the Intelligence Community assessed that the Russian government "aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him," the Committee found that IRA social media activity was overtly and almost invariably supportive of then-candidate Trump, and to the detriment of Secretary Clinton's campaign.[6]

---

https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[5] **(U)** Office of the Director of National Intelligence (ODNI), "Assessing Russian Activities and Intentions in Recent US Elections," *Intelligence Community Assessment (Unclassified Version),* January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[6] **(U)** *Ibid.*

(U) The Committee found that the Russian government tasked and supported the IRA's interference in the 2016 U.S. election. This finding is consistent with the Committee's understanding of the relationship between IRA owner Yevgeniy Prigozhin and the Kremlin, the aim and scope of the interference by the IRA, and the correlation between the IRA's actions and electoral interference by the Russian government in other contexts and by other means.[7] Despite Moscow's denials, the direction and financial involvement of Russian oligarch Yevgeniy Prigozhin, as well as his close ties to high-level Russian government officials including President Vladimir Putin, point to significant Kremlin support, authorization, and direction of the IRA's operations and goals.

[redacted]

2. **(U)** The Committee found that Russia's targeting of the 2016 U.S. presidential election was part of a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society. Moreover, the IRA conducted a vastly more complex and strategic assault on the United States than was initially understood. The IRA's actions in 2016 represent only the latest installment in an increasingly brazen interference by the Kremlin on the citizens and democratic institutions of the United States.

[redacted] Russia's history of using social media as a lever for online influence operations predates the 2016 U.S. presidential election and involves more than the IRA. The IRA's operational planning for the 2016 election goes back at least to 2014, when two IRA operatives were sent to the United States to gather intelligence in furtherance of the IRA's objectives.[9] [redacted]

[7] **(U)** Indictment, *United States v. Internet Research Agency*, et al., Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[8] [redacted]

[9] **(U)** Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election – Unraveling the Russia Story So Far," *The New York Times,* September 20, 2018.

[10] [redacted]

[11] [redacted]

[12] **(U)** *Ibid.*

[redacted]

(U) Analysis of the behavior of the IRA-associated social media accounts makes clear that while the Russian information warfare campaign exploited the context of the election and election-related issues in 2016, the preponderance of the operational focus, as reflected repeatedly in content, account names, and audiences targeted, was on socially divisive issues—such as race, immigration, and Second Amendment rights—in an attempt to pit Americans against one another and against their government. The Committee found that IRA influence operatives consistently used hot-button, societal divisions in the United States as fodder for the content they published through social media in order to stoke anger, provoke outrage and protest, push Americans further away from one another, and foment distrust in government institutions. The divisive 2016 U.S. presidential election was just an additional feature of a much more expansive, target-rich landscape of potential ideological and societal sensitivities.

3. **(U)** The Committee found that the IRA targeted not only Hillary Clinton, but also Republican candidates during the presidential primaries. For example, Senators Ted Cruz and Marco Rubio were targeted and denigrated, as was Jeb Bush.[14] As Clint Watts, a former FBI Agent and expert in social media weaponization, testified to the Committee, "Russia's overt media outlets and covert trolls sought to sideline opponents on both sides of the political spectrum with adversarial views towards the Kremlin." IRA operators sought to impact primaries for both major parties and "may have helped sink the hopes of candidates more hostile to Russian interests long before the field narrowed."[15]

4. **(U)** The Committee found that no single group of Americans was targeted by IRA information operatives more than African-Americans. By far, race and related issues were the preferred target of the information warfare campaign designed to divide the country in 2016. Evidence of the IRA's overwhelming operational emphasis on race is evident in the IRA's Facebook advertisement content (over 66 percent contained a term related to race) and targeting (locational targeting was principally aimed at African-Americans in key metropolitan areas with), its Facebook pages (one of the IRA's top-performing pages, "Blacktivist," generated 11.2 million engagements with Facebook users), its Instagram content (five of the top 10 Instagram accounts were focused on African-American issues and audiences), its Twitter content (heavily focused on hot-button issues with racial undertones, such as the NFL kneeling protests), and its YouTube

[13] [redacted]

[14] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018); Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018.

[15] **(U)** Clint Watts, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

activity (96 percent of the IRA's YouTube content was targeted at racial issues and police brutality).

5. **(U)** The Committee found that paid advertisements were not key to the IRA's activity, and moreover, are not alone an accurate measure of the IRA's operational scope, scale, or objectives, despite this aspect of social media being a focus of early press reporting and public awareness.[16] An emphasis on the relatively small number of advertisements, and the cost of those advertisements, has detracted focus from the more prevalent use of original, free content via multiple social media platforms. According to Facebook, the IRA spent a total of about $100,000 over two years on advertisements—a minor amount, given the operational costs of the IRA were approximately $1.25 million dollars a month.[17] The nearly 3,400 Facebook and Instagram advertisements the IRA purchased are comparably minor in relation to the over 61,500 Facebook posts, 116,000 Instagram posts, and 10.4 million tweets that were the original creations of IRA influence operatives, disseminated under the guise of authentic user activity.

6. **(U)** The Committee found that the IRA coopted unwitting Americans to engage in offline activities in furtherance of their objectives. The IRA's online influence operations were not constrained to the unilateral dissemination of content in the virtual realm, and its operatives were not just focused on inciting anger and provoking division on the internet. Instead, the IRA also persuaded Americans to deepen their engagement with IRA operatives. For example, the IRA targeted African-Americans over social media and attempted and succeeded in some cases to influence their targets to sign petitions, share personal information, and teach self-defense training courses.[18] In addition, posing as U.S. political activists, the IRA requested—and in some cases obtained—assistance from the Trump Campaign in procuring materials for rallies and in promoting and organizing the rallies.[19]

7. **(U)** The Committee found that the IRA was not Russia's only vector for attempting to influence the United States through social media in 2016. Publicly available information showing additional influence operations emanating from Russia unrelated to IRA activity make clear the Kremlin was not reliant exclusively on the IRA in 2016. Russia's intelligence services, including the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), also exploited U.S. social media platforms as a

[16] **(U)** Dan Keating, Kevin Schaul and Leslie Shapiro, "The Facebook ads Russians targeted at different groups," *Washington Post,* November 1, 2017.
[17] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[18] **(U)** Shelby Holliday and Rob Barry, "Russian Influence Campaign Extracted Americans' Personal Data," *Wall Street Journal,* March 7, 2018.
[19] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

vehicle for influence operations.[20] Information acquired by the Committee from intelligence oversight, social media companies, the Special Counsel's investigative findings, and research by commercial cybersecurity companies all reflect the Russian government's use of the GRU to carry out another core vector of attack on the 2016 election: the dissemination of hacked materials.

8. **(U)** The Committee found that IRA activity on social media did not cease, but rather increased after Election Day 2016. The data reveal increases in IRA activity across multiple social media platforms, post-Election Day 2016: Instagram activity increased 238 percent, Facebook increased 59 percent, Twitter increased 52 percent, and YouTube citations went up by 84 percent.[21] As John Kelly noted: "After election day, the Russian government stepped on the gas. Accounts operated by the IRA troll farm became more active after the election, confirming again that the assault on our democratic process is much bigger than the attack on a single election."[22]

   (U) Though all of the known IRA-related accounts from the Committee's data set were suspended or taken down in the fall of 2017, outside researchers continue to uncover additional IRA social media accounts dedicated to spreading malicious content. According to an October 2018 study of more than 6.6 million tweets linking to publishers of intentionally false news and conspiracy stories, in the months before the 2016 U.S. election, "more than 80% of the disinformation accounts in our election maps are still active . . . [and] continue to publish more than a million tweets in a typical day."[23]

III. (U) THE REACH OF SOCIAL MEDIA

(U) Social media and its widespread adoption have changed the nature and practice of human interaction for much of the world. During the 2016 election campaign season, approximately 128 million Facebook users in the United States alone generated nearly nine billion interactions related to the 2016 U.S. presidential election.[24] In just the last month of the campaign, more than 67 million Facebook users in the United States generated over 1.1 billion likes, posts, comments, and shares related to Donald Trump. Over 59 million Facebook users in the United States generated over 934 million likes, posts, comments and shares related to Hillary Clinton. On Election Day, 115.3 million Facebook users in the United States generated 716.3

[20] **(U)** Adam Entous, Elizabeth Dwoskin, and Craig Timberg, "Obama tried to give Zuckerberg a wake-up call over fake news on Facebook," *Washington Post,* September 24, 2017.
[21] **(U)** John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.
[22] **(U)** John Kelly, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[23] **(U)** Matthew Hindman and Vlad Barash, "Disinformation, 'Fake News' and Influence Campaigns on Twitter," Knight Foundation, October 4, 2018, https://knightfoundation.org/articles/seven-ways-misinformation-spread-during-the-2016-election.
[24] **(U)** Dana Feldman, "Election Day Dominated Facebook With Over 716M Election-Related Interactions," *Forbes,* November 9, 2016.

million interactions related to the election and viewed election-related videos over 640 million times.[25]

(U) The Twitter platform also featured prominently across the arc of the 2016 campaign season. Americans sent roughly one billion tweets and retweets about the election between the first primary debates in August 2015 and Election Day 2016.[26] The U.S. Election Day 2016 was the most-Tweeted Election Day ever, with worldwide users generating more than 75 million election-related tweets.[27]

(U) Political campaigns, in the ambition of harvesting this connectivity and speaking "directly" with as many voters as possible, have adapted and attempted to exploit this new media environment. Total digital advertisement spending related to the 2016 election cycle on social media reached $1.4 billion—a 789 percent increase over 2012.[28]

(U) Social media has created new virtual venues for American participation in the national political discourse, and offered a new channel for direct democratic engagement with elected officials, media representatives, and fellow citizens around the world. However, the same system of attributes that empowers these tools and their users to positively increase civic engagement and constructive dialogue lends itself to exploitation, which frequently materializes as the dissemination of intentionally false, misleading, and deliberately polarizing content.[29]

(U) According to one November 2016 analysis, in the final three months leading up to Election Day, calculated by total number of shares, reactions, and comments, the top-performing intentionally false stories on Facebook actually outperformed the top news stories from the nineteen major news outlets.[30] That analysis found that in terms of user engagement, the top two intentionally false election stories on Facebook included articles alleging Pope Francis' endorsement of Donald Trump for President (960,000 shares, reactions, and comments), and WikiLeaks' confirmation of Hillary Clinton's sale of weapons to ISIS (789,000 shares, reactions, and comments).[31]

---

[25] **(U)** Ivana Kottasova, "Trump's Win Smashes Social Media Records," *CNN*, November 9, 2016.
[26] **(U)** Bridget Coyne, "How #Election2016 was Tweeted so far," *Twitter Blog*, November 7, 2016.
[27] **(U)** Twitter, "6.8 Million Viewers Watch Twitter Live Stream of BuzzFeed News' Election Night Special," November 10, 2016, https://www.prnewswire.com/news-releases/68-million-viewers-watch-twitter-live-stream-of-buzzfeed-news-election-night-special-300360415.html.
[28] **(U)** Kate Kaye, "Data-Driven Targeting Creates Huge 2016 Political Ad Shift: Broadcast TV Down 20%, Cable and Digital Way Up," *AdAge,* January 3, 2017.
[29] **(U)** The term "fake news" is not a useful construct for understanding the complexity of influence operations on social media in today's online ecosystem. The term's definition has evolved since the 2016 election and today, has been, at times, misappropriated to fit certain political and social perspectives.
[30] **(U)** Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook," *Buzzfeed*, November 16, 2016, ("During these critical months of the campaign, 20 top-performing false election stories from hoax sites and hyper-partisan blogs generated 8,7111,000 shares, reactions and comments on Facebook. . . . Within the same time period, the 20 best performing election stories from 19 major news websites generated a total of 7,367,000 shares, reactions and comments on Facebook.")
[31] **(U)** *Ibid.*

(U) A September 2017 Oxford Internet Institute study of Twitter users found that, "users got more misinformation, polarizing, and conspiratorial content than professionally produced news."[32] According to the study, in the "swing state" of Michigan, professionally produced news was, by proportion, "consistently smaller than the amount of extremist, sensationalist, conspiratorial, masked commentary, fake news and other forms of junk news," and the ratio was most disproportionate the day before the 2016 U.S. election.[33,34] A National Bureau of Economic Research paper from January 2017 assessed that intentionally false content accounted for 38 million shares on Facebook in the last 3 months leading up to the election, which translates into 760 million clicks—or "about three stories read per American adult."[35]

(U) In conducting a broader analysis of false information dissemination, in what was described as "the largest ever study of fake news," researchers at MIT tracked over 125,000 news stories on Twitter, which were shared by three million people over the course of 11 years.[36,37] The research found that, "Falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information, and the effects were more pronounced for false political news than for false news about terrorism, natural disasters, science, urban legends, or financial information." The study also determined that false news stories were 70 percent more likely to be retweeted than accurate news, and that true stories take about six times as long to reach 1,500 people on Twitter as false stories do. According to the lead researcher in the study, Soroush Vosoughi, "It seems pretty clear that false information outperforms true information."[38]

(U) The spread of intentionally false information on social media is often exacerbated by automated, or "bot" accounts. The 2016 U.S. election put on full display the impact that more sophisticated automation and the proliferation of bots have had on American political discourse. Researchers at the University of Southern California who evaluated nearly 20 million election-related tweets assessed that about one-fifth of the political discourse around the 2016 election on Twitter may have been automated and the result of bot activity. This research, however, does not make clear what country the bot activity originated from, or whether the activity was

---

[32] **(U)** Phil Howard, et al., "Social Media, News and Political Information during the U.S. Election: Was Polarizing Content Concentrated in Swing States," Oxford Internet Institute, Project on Computational Propaganda, September 29, 2017, https://arxiv.org/ftp/arxiv/papers/1802/1802.03573.pdf.

[33] **(U)** A swing state is a U.S. state in which Republican and Democratic candidates have similar levels of support and which is likely to play a key role in the outcome of presidential elections.

[34] **(U)** Philip Howard, Gillian Bolsover, et al., "Junk News and Bots During the U.S. Election: What Were Michigan Voters Sharing Over Twitter?" Oxford Internet Institute, Project on Computational Propaganda, March 26, 2017, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/03/What-Were-Michigan-Voters-Sharing-Over-Twitter-v2.pdf.

[35] **(U)** Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 election," *Journal of Economic Perspectives,* Volume 31, Number 2, Spring 2017, 211-236, http://www.nber.org/papers/w23089.

[36] **(U)** Soroush Vosoughi, et al., "The spread of true and false news online," *Science*, Volume 359, Issue 6380, March 9, 2018, http://ide.mit.edu/sites/default/files/publications/2017%20IDE%20Research%20Brief%20False%20News.pdf.

[37] **(U)** Robinson Meyer, "The Grim Conclusions of the Largest Ever Study of Fake News," *The Atlantic*, March 8, 2018: https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/.

[38] **(U)** *Ibid.*

necessarily malicious in nature. These researchers also concluded that "bots [were] pervasively present and active in the online political discussion about the 2016 U.S. presidential election," adding that "the presence of social media bots can indeed negatively affect democratic political discussion rather than improving it."[39] Arriving at a similar conclusion, an Oxford Internet Institute study of 17 million tweets posted during the 2016 election found that bots "reached positions of measurable influence," and "did infiltrate the upper cores of influence and were thus in a position to significantly influence digital communications during the 2016 U.S. election."[40]

(U) In testimony to the Committee, social media researcher John Kelly suggested that automated accounts focused on fringe political positions are far more active than the voices of actual people holding politically centrist views: "In our estimate, today the automated accounts at the far left and far right extremes of the American political spectrum produce as many as 25 to 30 times the number of messages per day on average as genuine political accounts across the mainstream." In other words, "the extremes are screaming while the majority whispers."[41] Taken as a whole, the attributes of social media platforms render them vulnerable for foreign influence operations intent on sowing discord throughout American society.

IV. (U) RUSSIAN USE OF DISINFORMATION

(U) Russia's attack on the 2016 election was a calculated and brazen assault on the United States and its democratic institutions, but this was not the Kremlin's first foray into asymmetric warfare against America. Russian interference in 2016 represents the latest and most sophisticated example of Russia's effort to undermine the nation's democracy through targeted operations. As the January 6, 2017, Intelligence Community Assessment states, Moscow's provocations "demonstrated a significant escalation in directness, level of activity, and scope of effort." However, the activities only "represent the most recent expression of Moscow's longstanding desire to undermine the U.S.-led liberal democratic order."[42]

(U) Russia's intelligence services have been focused for decades on conducting foreign influence campaigns, or "active measures," and disinformation.[43,44] The Russian intelligence services "pioneered dezinformatsiya [disinformation] in the early twentieth century," and by the mid-1960's, had significantly invested in disinformation and active measures.[45] According to

---

[39] **(U)** Alessandro Bessi and Emilio Ferrara, "Social Bots Distort the 2016 US Presidential Election Online Discussion," *First Monday*, Volume 21, Number 11, 7 November 7, 2016, https://ssrn.com/abstract=2982233.
[40] **(U)** Samuel Woolley and Douglas Guilbeault, "Computational Propaganda in the United States of America: Manufacturing Consensus Online," Oxford Internet Institute Computational Propaganda Research Project, May 2017, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-USA.pdf.
[41] **(U)** John Kelly, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[42] **(U)** ODNI, "Background to 'Assessing Russian Activities and Intentions in Recent U.S. Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[43] **(U)** "Active measures" is a Soviet-era term now called "measures of support" by the Russian government.
[44] **(U)** Disinformation is the intentional spread of false information to deceive.
[45] **(U)** *"Dezinformatsiya"* is a Russian word, defined in the 1952 Great Soviet Encyclopedia as the "dissemination (in the press, on the radio, etc.) of false reports intended to mislead public opinion."

testimony Roy Godson and Thomas Rid provided to the Committee, over 10,000 individual disinformation operations were carried out during the Cold War involving approximately 15,000 personnel at its peak.[46,47]

A. (U) Russian Active Measures

(U) For decades, Soviet active measures pushed conspiratorial and disinformation narratives about the United States around the world. The KGB authored and published false stories and forged letters concerning the Kennedy assassination, including accounts suggesting CIA involvement in the killing. Martin Luther King, Jr. was the target of manufactured KGB narratives, as was Ronald Reagan. Russian intelligence officers planted anti-Reagan articles in Denmark, France, and India during his unsuccessful 1976 bid for the Republican presidential nomination. A declassified U.S. State Department document from 1981 outlines a series of realized Russian active measures operations, including the spread of falsehoods concerning U.S. complicity in the 1979 seizure of the Grand Mosque of Mecca and responsibility for the 1981 death of Panamanian General Omar Torrijos, as well as an elaborate deception involving multiple forgeries and false stories designed to undermine the Camp David peace process and to exacerbate tensions between the United States and Egypt.[48] Among the most widely known and successful active measures operations conducted during the Cold War centered on a conspiracy that the AIDS virus was manufactured by the United States at a military facility at Fort Detrick in Maryland. This fictional account of the virus' origin received considerable news coverage, both in the United States and in over forty non-Cold War aligned countries around the world.[49]

(U) In a 1998 CNN interview, retired KGB Major General Oleg Kalugin described active measures as "the heart and soul of Soviet intelligence":

> *Not intelligence collection, but subversion; active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO; to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs.*[50]

(U) While this history of discrediting the United States with spurious rumors and disinformation is well-chronicled, Russia has continued the practice today.

---

[46] **(U)** Thomas Rid, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[47] **(U)** Roy Godson, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[48] **(U)** Department of State, "Soviet Active Measures: Forgery, Disinformation, Political Operations," Special Report No. 88, October 1981, https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf.

[49] **(U)** Christopher M. Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive & the Secret History of the KGB*, Basic Books, 1985, p. 244.

[50] **(U)** Oleg Kalugin, "Inside the KGB: An interview with retired KGB Maj. Gen. Oleg Kalugin," *CNN*, January 1998.

(U) As Sergey Tretyakov, the former SVR (the foreign intelligence service of the Russian Federation, and a successor organization to the KGB) "rezident," or station chief for Russian intelligence in New York, wrote in 2008, "Nothing has changed. . . . Russia is doing everything it can today to embarrass the U.S."[51]

B. (U) Russia's Military and Information Warfare

(U) While active measures have long been a tool of the Russian intelligence services, a shift toward developing and honing the tools of information warfare represents a more recent development for the Russian conventional military and larger national security establishment.

(U) The embrace of asymmetric information operations resulted from a number of factors, but chiefly from the Russian national security establishment's belief that these operations are effective. Pavel Zolotarev, a retired major general in the Russian Army, explained, "We had come to the conclusion . . . that manipulation in the information sphere is a very effective tool."[52] That conclusion was reinforced by the perception that these operations are extremely difficult to defend against, particularly with multinational military alliances like NATO, which is built to deter and if necessary defeat a traditional, conventional military threat. Information warfare, in addition, is an extremely low-cost alternative to conventional military conflict.

(U) A lack of alternatives also motivates Russia's reliance on asymmetric tactics. Russia's national security establishment may have had no choice but to increase its asymmetric capabilities given its inability to compete with the West on a more traditional, military hard power basis. Former National Intelligence Officer for Russia and Eurasia Eugene Rumer stated in 2017 testimony to the Committee that Russia's information warfare toolkit "performs the function of the equalizer that in the eyes of the Kremlin is intended to make up for Russia's weakness vis-à-vis the West."[53]

[redacted]

[51] **(U)** *See* Evan Osnos, David Remnick, and Joshua Yaffa, "Trump, Putin, and the new Cold War," *New Yorker*, March 6, 2017.
[52] **(U)** *Ibid.*
[53] **(U)** Eugene Rumer, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.
[54] [redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

C. (U) Russia's Weaponization of Social Media

(U) Portending what was to come in 2016, General Philip Breedlove assessed in his September 2014 remarks to the NATO Wales Summit that, regarding Ukraine, "Russia is waging

[55] **(U)** *Ibid.*
[56] **(U)** *Ibid.*

the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[57] Social media platforms enabled Russia's Ukraine campaign, and aided materially in the realization of its military's adoption of information warfare doctrine.

(U) Compared to more traditional methods for information warfare used in the Cold War, Watts described social media as providing Russia a "cheap, efficient, and highly effective access to foreign audiences with plausible deniability of their influence."[58]

(U) Russia's aptitude for weaponizing internet-based social media platforms against the United States resulted from Moscow's experience conducting online disinformation campaigns against its own citizens for over a decade. Russia's online disinformation efforts are rooted in the early and mid-2000s, when the Kremlin sought to suppress opposition in the face of rapidly expanding internet-based communications.[59]

(U) Studying the technology used by its political opponents, the Kremlin hijacked the capabilities and weaponized their use against Russia's own people. Russia perfected the use of these tools and methods of information warfare over time, paving the way for its decision to similarly target the citizens of other countries. Russia has also continued its domestic deployment of these tools.

- [redacted]
- [redacted]

D. (U) Russian Social Media Tactics

(U) The Kremlin has honed and refined its social media disinformation tactics over the last decade. Lessons learned through information warfare campaigns directed both internally

---

[57] **(U)** *See* John Vandiver, "SACEUR: Allies must prepare for Russia 'hybrid war,'" *Stars and Stripes*, September 4, 2014.

[58] **(U)** Clint Watts, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[59] **(U)** Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," CNA Analysis and Solutions, Occasional Paper Series, March 2017.

[60] [redacted]

[61] **(U)** *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, Special Counsel Robert S. Mueller, III, March 2019.

and at the populations of regional neighbors provided Moscow valuable insights into how information and social media could be most effectively used against the West.

(U) Although the tactics employed by Russia vary from one campaign to the next, there are several consistent themes in the Russian disinformation playbook.

(U) High Volume and Multiple Channels. Russian disinformation efforts tend to be wide-ranging in nature, in that they utilize any available vector for messaging, and when they broadcast their messaging, they do so at an unremitting and constant tempo. Christopher Paul and Miriam Matthews from the RAND Corporation describe the Russian propaganda effort as a "firehose of falsehood," because of its "incredibly large volumes," its "high numbers of channels and messages," and a "rapid, continuous, and repetitive" pace of activity. Russia disseminates the disinformation calculated to achieve its objectives across a wide variety of online vehicles: "text, video, audio, and still imagery propagated via the internet, social media, satellite television and traditional radio and television broadcasting."[62] One expert, Laura Rosenberger of the German Marshall Fund, told the Committee that "[t]he Russian government and its proxies have infiltrated and utilized nearly every social media and online information platform—including Instagram, Reddit, YouTube, Tumblr, 4chan, 9GAG, and Pinterest."[63]

(U) The desired effect behind the high volume and repetition of messaging is a flooding of the information zone that leaves the target audience overwhelmed. Academic research suggests that an individual is more likely to recall and internalize the *initial* information they are exposed to on a divisive topic. As RAND researchers have stated, "First impressions are very resilient."[64] Because first impressions are so durable and resistant to replacement, being first to introduce narrative-shaping content into the information ecosystem is rewarded in the disinformation context.

(U) Merging Overt and Covert Operations. The modern Russian disinformation playbook calls for illicitly obtaining information that has been hacked or stolen, and then weaponizing it by disseminating it into the public sphere. The most successful Russian operations blend covert hacking and dissemination operations, social media operations, and fake personas with more overt influence platforms like state-funded online media, including RT and Sputnik.

(U) According to FBI:

[redacted]

[62] **(U)** Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood,' Propaganda Model," *RAND Corporation,* 2016, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.
[63] **(U)** Laura Rosenberger, Written Testimony, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[64] **(U)** Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood,' Propaganda Model," *RAND Corporation,* 2016, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

[redacted]

(U) Another notable example of Russia using social media platforms and news media to advance disinformation objectives occurred in Germany in 2016. At the center of the operation was a report that falsely accused Arab migrants of sexually assaulting a Russian-German girl. The incident originates with Lisa, a 13-year-old girl from Berlin, who was reported missing by her parents after failing to show up for school. Initially claiming to have been attacked by men of Middle Eastern or North African appearance, Lisa eventually admitted to having fabricated the entire story. Despite Lisa's admission to the police that her story was made up, her original account of kidnapping and rape catapulted across social media. While German law enforcement officials formally debunked the initial report, Russian state-controlled news media, including Channel One and later RT, promoted the social media-inspired and ardently anti-migrant fervor among the Russian-German populations, in particular on YouTube.

(U) Far-right political parties, some of whom are supported by the Kremlin, reacted to these false stories by protesting in Berlin, protests which were covered by RT cameras. Sputnik then claimed there was a potential police cover-up, citing reporting of its own claim as its only evidence. A few days later, as protests spread, Russian Foreign Minister Lavrov publicly disputed that Lisa's 30-hour disappearance was voluntary. Germany, he said, was "covering up reality in a politically correct manner for the sake of domestic politics."[66] The office of Chancellor Merkel was forced to respond, and the episode added to the confusion and fear surrounding the politically roiling migrant crisis in Germany.

(U) Speed. Speed is critical to Russia's use of disinformation. Online, themes and narratives can be adapted and trained toward a target audience very quickly. This allows Russia

[65] **(U)** FBI, Written response to SSCI inquiry of January 3, 2019, March 1, 2019.
[66] **(U)** Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *The New York Times Magazine,* September 13, 2017.

to formulate and execute information operations with a velocity that far outpaces the responsivity of a formal decision-making loop in NATO, the United States, or any other western democracy. For example, within hours of the downing of Malaysian Airlines Flight 17 over Ukraine, Russian media had introduced a menu of conspiracy theories and false narratives to account for the plane's destruction, including an alleged assassination attempt against President Putin, a CIA plot, an onboard explosive, and the presence of a Ukrainian fighter jet in the area.[67,68] Dutch investigators with the Joint Investigation Team determined later the plane was shot down by a surface-to-air missile fired from a Russia-provided weapon system used in separatist-held territory in Ukraine.

(U) Use of Automated Accounts and Bots. The use of automated accounts on social media has allowed social media users to artificially amplify and increase the spread, or "virulence," of online content. Russia-backed operatives exploited this automated accounts feature and worked to develop and refine their own bot capabilities for spreading disinformation faster and further across the social media landscape. In January 2018, Twitter disclosed its security personnel assess that over 50,000 automated accounts linked to Russia were tweeting election-related content during the U.S. presidential campaign.[69]

(U) Russian actors are prolific users of automated accounts and bots. Phil Howard, citing the findings of a study done by the Oxford Internet Institute, concluded that Russian Twitter networks "are almost completely bounded by highly automated accounts, with a high degree of overall automation." His study assessed that "some 45 percent of Twitter activity in Russia is managed by highly automated accounts," and that Ukraine remains "the frontline of experimentation in computational propaganda with active campaigns of engagement" between Russian and Ukrainian botnets.[70] Early automation was fairly primitive and easier to detect and disrupt, but malicious bot activity has continued to grow in sophistication.

(U) Use of Paid Internet "Trolls." The act of "trolling" online has been a feature of the internet eco-system since the development of online chat rooms, blogs, internet forums, and other early communications platforms. An internet "troll" is a real person sitting behind a keyboard who posts inflammatory, aggressive, harassing, or misleading messages online in an attempt to provoke a response from other users of social media.[71] Kremlin-backed entities have spent years professionalizing a cadre of paid trolls, investing in large-scale, industrialized "troll

---

[67] **(U)** Joel Gunter and Olga Robinson, "Sergei Skripal and the Russian disinformation game," *BBC News,* September 9, 2018.

[68] **(U)** Margaret Hartmann, "Russia's 'Conspiracy Theory': MH17 Shot Down by Ukrainian Fighter Jet or Missile," *New York Magazine,* July 22, 2014.

[69] **(U)** Twitter Public Policy Blog, "Update on Twitter's review of the 2016 US election," January 19, 2018.

[70] **(U)** Samuel Woolley and Phil Howard, "Computational Propaganda Worldwide: Executive Summary," Computational Propaganda Research Project, Oxford Internet Institute, University of Oxford, November 2017, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

[71] **(U)** The concept of a "troll" online is subjective and can encompass a range of differing motivations, tactics, and objectives. For the purposes of this paper, the Committee is focused on professional "trolls" who are paid to engage in dialogue online and provide commentary and content on various social media and news channels.

farms," in order to obscure Moscow's hand and advance the aims of Russia's information operations both domestically and abroad.

(U) While Russia's use of trolls has been more widely exposed in recent years, one of the first public exposures came through WikiLeaks in early 2012 and subsequent reporting by *The Guardian*. According to data and documents provided to WikiLeaks by a group operating under the moniker "Anonymous," the Kremlin-backed youth group Nashi was paying a network of bloggers and trolls to support President Putin and undermine his political opposition online. These Putin-supported commentators were paid to comment on articles, "dislike" anti-Putin YouTube videos, and support smear campaigns against opposition leaders.[72]

(U) In 2015, NATO's Strategic Communications Center of Excellence commissioned research on the use of trolling in hybrid warfare, publishing its conclusions in the spring of 2016. The study, which was largely focused on discussions surrounding the Ukraine-Russia conflict, outlined a variety of influence techniques employed by trolls online, including the aggressive use of offensive slurs and attacks; utilization of irony and sarcasm; peddling conspiracy theories; employing profile pictures of young, attractive men and women; diverting discourse to other problems; posting misleading information on information sources like *Wikipedia*; emphasizing social divisions; and presenting indigestible amounts of data without sources or verification.[73]

(U) In addition to the aggressive and persistent pushing of Kremlin-narrated themes and content, a principal objective of the Russian internet troll appears to be stifling the democratic debate entirely.

(U) As journalist Adrian Chen of *The New Yorker* reported, the objectives for Russia's troll army are primarily "to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."[74] Leonid Volkov, a Russian politician and supporter of opposition leader Alexei Navalny, told Chen, "The point [of Russian disinformation] is to create the atmosphere of hate, to make it so stinky that normal people won't want to touch it." He stressed, "Russia's information war might be thought of as the biggest trolling operation in history, and its target is nothing less than the utility of the Internet as a democratic space."[75] Exemplifying the assertion, a 2015 analysis by the Finnish public broadcasting company concluded that many Finns elect to simply disengage from online discussions due to trolling, as "they did not see the use of fighting with masses of aggressive comments or threatening messages."[76]

---

[72] **(U)** Miriam Elder, "Hacked emails allege Russian youth group Nashi paying bloggers," *The Guardian*, February 7, 2012.

[73] **(U)** Sanda Svetoka, et al., "Social Media as a Tool of Hybrid Warfare," NATO Strategic Communications Centre of Excellence, May 2016, https://www.stratcomcoe.org/social-media-tool-hybrid-warfare.

[74] **(U)** Adrian Chen, "The Real Paranoia-Inducing Purpose of Russian Hacks." *The New Yorker,* July 27, 2016.

[75] **(U)** *Ibid.*

[76] **(U)** Sanda Svetoka, et al., "Social Media as a Tool of Hybrid Warfare," NATO Strategic Communications Centre of Excellence, May 2016, https://www.stratcomcoe.org/social-media-tool-hybrid-warfare.

(U) Manipulating Real People and Events. Russian-backed trolls pushing disinformation have also sought to connect with and potentially coopt individuals to take action in the real world. From influencing unwitting Americans to retweet or spread propaganda, to convincing someone to host a real world protest, Russian disinformation agents employ online methods to attract and exploit a wide range of real people.

(U) In testifying to the Committee in 2017, Clint Watts outlined three different types of potential real-world targets for Russian influence operators.[77] A class of "useful idiots" refers to unwitting Americans who are exploited to further amplify Russian propaganda, unbeknownst to them; "fellow travelers" are individuals ideologically sympathetic to Russia's anti-western viewpoints who take action on their own accord; and "agent provocateurs" are individuals who are actively manipulated to commit illegal or clandestine acts on behalf of the Russian government. As Watts explains, "Some people are paid for. Some are coerced. Some are influenced. Some agree. Some don't know what they're doing. . . . Where they fall on that spectrum may not matter ultimately." What matters most, he argues, is the message they are carrying and whether its reach is growing.[78]

E. (U) Features of Russian Active Measures

(U) Although information warfare can target an opposing government, its officials, or its combat forces, Russian information warfare on social media is often aimed squarely at attacking a society and its relationship to its own democratic institutions.. Modern Russian active measures on social media exhibit several notable features.

(U) Attacking the Media. Information warfare, at its core, is a struggle over information and truth. A free and open press—a defining attribute of democratic society—is a principal strategic target for Russian disinformation. As Soviet-born author Peter Pomerantsev notes, "The Kremlin successfully erodes the integrity of investigative and political journalism, producing a lack of faith in traditional media." He concludes, "The aim of this new propaganda is not to convince or persuade, but to keep the viewer hooked and distracted, passive and paranoid, rather than agitated to action."[79]

(U) Jakub Kalensky, a former official with the European Union's rapid response team created to counter Russian disinformation, similarly argues, "It's not the purpose to persuade someone with one version of events. The goal for Russia is to achieve a state in which the

---

[77] **(U)** Clint Watts, Hearing before the Senate Armed Services Committee, April 27, 2017, available at https://www.fpri.org/wp-content/uploads/2017/04/Watts-Testimony-Senate-Armed-Services-email-distro-Final.pdf.
[78] **(U)** Denise Clifton, "A Murder Plot, a Twitter Mob and the Strange Unmasking of a Pro-Kremlin Troll," *Mother Jones,* June 5, 2018.
[79] **(U)** Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," *Institute of Modern Russia*, 2014, https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

average media consumer says, 'There are too many versions of events, and I'll never know the truth.'"[80]

(U) Fluid Ideology. Because the Kremlin's information warfare objectives are not necessarily focused on any particular, objective truth, Russian disinformation is unconstrained by support for any specific political viewpoint and continually shifts to serve its own self-interest. Provided the information space is rendered confused and clouded, Russia's information operatives are unencumbered and can support any and all perspectives.

(U) An August 2018 report on information manipulation commissioned by the French government notes that the Kremlin "can simultaneously support far right and far left movements, so long as they are in competition with one another." As examples, the report cites the downing of Malaysian Airlines Flight 17, the chemical attacks in the Syrian town of Douma, and the poisoning of Sergei and Yulia Skripal in Salisbury, England, as instances in which Kremlin-backed disinformation amplified far-fetched and mutually exclusive conspiracy theories on both sides of the political spectrum.[81] This key characteristic distinguishes modern day Russian operations from former Soviet Union-era active measures campaigns. Speaking to the resultant operational flexibility, Pomerantsev describes the transition: "Unlike in the Cold War, when Soviets largely supported leftist groups, a fluid approach to ideology now allows the Kremlin to simultaneously back far-left and far-right movements, greens, anti-globalists, and financial elites. The aim is to exacerbate divides and create an echo chamber of Kremlin support."[82]

(U) In sum, the modern-day Russian information warfare campaign combines the advantages of social media information delivery and the operational freedom of being ideologically agnostic.

(U) Exploiting Existing Fissures. Successful Russian active measures attempt to exploit societal divisions that already exist, rather than attempt to create new ruptures. Alexander Sharavin, the head of a military research institute and a member of the Academy of Military Sciences in Moscow, provides an illustrative example in relation to the Queen's popular appeal in the England: "If you go to Great Britain, for example, and tell them the Queen is bad, nothing will happen, there will be no revolution, because the necessary conditions are absent—there is no existing background for this operation." As Thomas Rid noted in his 2017 testimony to the Committee, "The tried and tested way of active measures is to use an adversary's existing weaknesses against himself, to drive wedges into pre-existing cracks: the more polarized a

[80] **(U)** *See* Joby Warrick and Anton Troianovski, "Agents of doubt," *Washington Post*, December 10, 2018.
[81] **(U)** Jean-Baptiste Jeangene Vilmer, et al., "Information Manipulation: A Challenge for our Democracies," Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.
[82] **(U)** Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," *Institute of Modern Russia*, 2014, https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

society, the more vulnerable it is."[83] Institutions and norms that define western liberal democracies—open and competitive elections, free flow of information, vibrant press freedoms, freedom of speech, and diverse societies—are conducive to exploitation by anti-Western propagandists.

(U) Indirect Objectives. As western governments grapple with addressing an internet operating environment that at present favors Russia, democratic institutions and constituencies must also weigh the potential indirect objectives of Russian active measures. As the August 2018 French disinformation report points out, the desired objectives of disinformation on a population can be two-fold. The direct objective, discussed earlier in this Volume, uses information manipulation to push the target audience in a preferred direction. The indirect objective entices overreach by the targeted country's government—in essence, baiting governments to respond in a heavy-handed or improper fashion that is irreconcilable with the nation's principles and civil liberties. The *indirect* objective, is, according to the French report, "not so much to convince a population of this or that story as to lead governments to take measures that are contrary to their democratic, liberal values, which, in turn, will provoke a reaction."[84]

(U) Similarly, even the fear of active measures being unleashed on a society risks societal damage, whether the foreign capability exists or not. Democratic governments and populations must balance the need for calling out and shining light on Russian activities with remaining realistic and sober about Moscow's actual capabilities and their effectiveness.

(U) The public needs to be made aware of the tactics being directed at them, but there also needs to be appreciation for the limitations of those tactics. As Massimo Calabresi reports in his 2017 *Time* article on Russia's social media war on America, "the fear of Russian influence operations can be more damaging than the operations themselves. Eager to appear more powerful than they are, the Russians would consider it a success if you questioned the truth of your news sources, knowing that Moscow might be lurking in your Facebook or Twitter feed."[85]

V. (U) THE INTERNET RESEARCH AGENCY

(U) The IRA is an entity headquartered in St. Petersburg, Russia, which since at least 2013 has undertaken a variety of Russian active measures campaigns at the behest of the Kremlin. The IRA has conducted virtual and physical influence operations in Russia, the United States, and dozens of other countries. The IRA conducted a multi-million dollar, coordinated

[83] **(U)** Thomas Rid, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[84] **(U)** Jean-Baptiste Jeangene Vilmer, et al., "Information Manipulation: A Challenge for our Democracies," Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

[85] **(U)** Massimo Calabresi, "Inside Russia's Social Media War on America," *Time*, May 18, 2017.

effort to influence the 2016 U.S. election as part of a broader information campaign to harm the United States and fracture its society.[86]

A. (U) Yevgeniy Prigozhin and the Kremlin

(U) The IRA is funded and directed by Yevgeniy Prigozhin, a Russia oligarch who works to conduct intelligence operations, military activities, and influence operations globally on behalf of the Kremlin. The IRA is one of several companies Prigozhin owns. He has also been linked to the financing and direction of the Wagner Group, a contract security organization that provides unofficial paramilitary support for Russian military operations.

[redacted]

(U) Prigozhin is a businessman and restauranteur who acquired the nickname "Putin's Chef," in part for the numerous catering contracts his company was awarded by the Russian government, including one for President Putin's 2012 inauguration. Prigozhin's companies have branched into areas including online propaganda, harassment of opposition leaders, and contracting a privatized military force to fight in Ukraine and Syria. *Fontanka*, a leading St. Petersburg news website, has also reported that Prigozhin's companies have secured oil revenues from Syrian oil fields in exchange for providing soldiers to protect those fields.[88]

[redacted]

[86] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[87] [redacted]

[88] **(U)** Neil MacFarquhar, "Meet Yevgeny Prigozhin, the Russian Oligarch Indicted in U.S. Election Interference," *New York Times*, February 16, 2018.

[89] [redacted]

(U) Prigozhin was publicly exposed as the main financial supporter of the IRA as early as 2014,[90] and his close relationship with Putin has been reported in numerous media sources, with the two appearing together in public photographs."[91]

(U) Prigozhin and companies he controlled, along with nine other employees, were indicted in the District of Columbia for a number of criminal violations, including acting as unregistered foreign agents inside the United States.[92] Further, Prigozhin and his companies have been targeted by the U.S. Department of Treasury with sanctions for "interfering with or undermining election processes and institutions," with specific respect to the 2016 U.S. presidential election.[93] Demonstrating that IRA operations were related to the broader scope of the Kremlin's objectives, these sanctions were announced alongside additional designations against the FSB and the Russian military intelligence organization, the GRU. Both entities were also designated for their online efforts to target the U.S. Government and undermine the election.

(U) Despite these public connections to the Russian government, President Putin denies any knowledge of Prigozhin's trolling operation. The Committee finds this denial to be false.

[redacted]

B. (U) IRA Operations

[redacted]

[90] **(U)** Max Seddon, "Documents Show How Russia's Troll Army Hit America," *BuzzFeed*, June 2, 2014.
[91] **(U)** Neil MacFarquhar, "Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is Known as Putin's Cook," New York Times, February 16, 2018.
[92] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[93] **(U)** Department of Treasury, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," March 15, 2018, https://home.treasury.gov/news/press-releases/sm0312.
[94] [redacted]
[95] **(U)** *Ibid.*
[96] **(U)** *Ibid.*

[redacted]

(U) According to the Special Counsel's Office, the IRA was funded as part of a larger interference operation called "Project Lakhta," which was part of a global set of operations undertaken both within Russia and abroad. The monthly budget for Project Lakhta "exceeded 73 million Russian rubles (over 1,250,000 U.S. dollars), including approximately one million rubles in bonus payments."[103]

C. (U) The Role of the IRA Troll

(U) A 2015 article by Adrian Chen in *The New York Times Magazine* provides a detailed open source account of the IRA's operations. According to that article, in 2015 the IRA had an estimated 400 employees who worked 12-hour shifts, divided between numerous departments, filling nearly 40 rooms. The trolls would create content on nearly every social media network—including LiveJournal, VKontakte (a Russia-based social media platform modeled after Facebook), Facebook, Twitter, and Instagram. Managers responsible for overseeing the trolls would monitor the workplace by CCTV and were "obsessed with statistics" like page views,

---

[97] [redacted]

[98] (U) *Ibid.*

[99] (U) *Ibid.*

[100] [redacted]

[101] (U) *Ibid.*

[102] (U) *Ibid.*

[103] (U) Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

posts, clicks, and traffic. One IRA employee, Ludmila Savchuk, described work shifts during which she was required to meet a quota of five political posts, 10 nonpolitical posts, and 150 to 200 comments on other trolls' postings.[104]

> **(U)** *The first thing employees did upon arriving at their desks was to switch on an Internet proxy service, which hid their I.P. addresses from the places they posted; those digital addresses can sometimes be used to reveal the real identity of the poster. Savchuk would be given a list of the opinions she was responsible for promulgating that day. Workers received a constant stream of 'technical tasks' —point-by-point exegeses of the themes they were to address, all pegged to the latest news.*[105]

(U) Savchuk's description largely matches similar depictions outlined in a series of leaked documents from an unidentified Russian hacker organization in June 2014. The leaked documents, purported to be attached to internal emails from within the IRA, describe the responsibilities of the IRA teams. As reported by *BuzzFeed* at the time:

> *On an average working day, the Russians are to post on news articles 50 times. Each blogger is to maintain six Facebook accounts publishing at least three posts a day and discussing the news in groups at least twice a day. By the end of the first month, they are expected to have won 500 subscribers and get at least five posts on each item a day. On Twitter, the bloggers are expected to manage 10 accounts with up to 2,000 followers and tweet 50 times a day.*[106]

(U) As a member of the Special Projects department of the IRA, Savchuk was responsible for creating and maintaining believable, fake personas online that would eventually seed pro-Kremlin narratives into their otherwise normal-looking online activities. One former employee said: "We had to write 'ordinary posts,' about making cakes or music tracks we liked, but then every now and then throw in a political post about how the Kiev government is fascist, or that sort of thing." Instructions for those political posts would come to the bloggers every morning as "technical tasks," which would have a "news line, some information about it, and a 'conclusion' that the commenters should reach."[107] As described by Chen, "The point was to weave propaganda seamlessly into what appeared to be the nonpolitical musings of an everyday person."[108]

(U) According to two former employees who spoke to *The Guardian*, trolls were paid based on their capabilities and the expertise required to maintain their particular fake personas. One employee who signed a non-disclosure agreement was paid around 45,000 rubles a month (roughly $700), while others could make up to 65,000 rubles (roughly $1,000) monthly if they

[104] **(U)** Adrian Chen, "The Agency," *The New York Times Magazine,* June 2, 2015.
[105] **(U)** *Ibid.*
[106] **(U)** Max Seddon, "Documents Show How Russia's Troll Army Hit America," *BuzzFeed*, June 2, 2014.
[107] **(U)** Shaun Walker, "Salutin' Putin: Inside a Russian troll House," *The Guardian*, April 2, 2015.
[108] **(U)** Adrian Chen, "The Agency," *The New York Times Magazine,* June 2, 2015.

were able to join the most prestigious wing of the IRA, the English-language trolls. Penalties were instituted for employees who failed to reach their quota or were caught copying previous posts as opposed to creating new content. The trolls worked "round the clock to flood Russian internet forums, social networks and the comments sections of western publications with remarks praising the President, Vladimir Putin, and raging at the depravity and injustice of the west."[109]

(U) One former employee's description of his work at the IRA is notable:

> *I arrived there, and I immediately felt like a character in the book '1984' by George Orwell—a place where you have to write that white is black and black is white. Your first feeling, when you ended up there, was that you were in some kind of factory that turned lying, telling untruths, into an industrial assembly line. The volumes were colossal—there were huge numbers of people, 300 to 400, and they were all writing absolute untruths. It was like being in Orwell's world.*[110]

(U) The Special Counsel's Office description of the IRA's activities is consistent with much of the reporting derived from interviews of former employees. As an example, the IRA indictment alleges in detail how IRA employees, referred to as "specialists," were tasked with creating fake social media accounts that purported to be U.S. citizens engaged on social media:

> *The specialists were divided into day-shift and night-shift hours and instructed to make posts in accordance with the appropriate U.S. time zone. The [IRA] also circulated lists of U.S. holidays so that specialists could develop and post appropriate account activity. Specialists were instructed to write about topics germane to the United States such as U.S. foreign policy and U.S. economic issues. Specialists were directed to create "political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements."*[111]

(U) The indictment indicates that IRA management made efforts to monitor and track the impact of its online efforts, through measurables such as comments, likes, reposts, changes in audience size, and other metrics.[112]

[redacted]

[109] **(U)** Shaun Walker, "Salutin' Putin: Inside a Russian troll House," *The Guardian*, April 2, 2015.
[110] **(U)** Anton Troianovski, "A former Russian troll speaks: 'It was like being in Orwell's world,'" *Washington Post,* February 17, 2018.
[111] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[112] **(U)** *Ibid.*

[redacted]

D. (U) Troll Narratives

(U) The IRA's trolls monitored societal divisions and were poised to pounce when new events provoked societal discord. For example, a former IRA troll interviewed by the *Guardian* in 2015 described his focus on race-related issues: "When there were black people rioting in the U.S. we had to write that U.S. policy on the black community had failed, Obama's administration couldn't cope with the problem, the situation is getting tenser. The negroes are rising up."[115]

[redacted]

(U) Leaked IRA documents from 2014 reveal a sophisticated approach to the various social media platforms aimed at ensuring trolls could evade online monitors. IRA employees were taught how to comment on each of the different websites so as to avoid being blocked or removed. As an example, one author outlined how to write for the fringe site WorldNetDaily: "Direct offense of Americans as a race are not published ('Your nation is a nation of complete idiots') . . . nor are vulgar reactions to the political work of Barack Obama."[117]

---

[113] [redacted]

[114] **(U)** *Ibid.*

[115] **(U)** Shaun Walker, "Salutin' Putin: Inside a Russian troll House," *The Guardian*, April 2, 2015.

[116] [redacted]

[117] **(U)** Max Seddon, "Documents Show How Russia's Troll Army Hit America," *BuzzFeed*, June 2, 2014.

(U) Developing and applying a familiarity with the American political space was also a critical function of the IRA trolling operation. According to a former employee interviewed by the news outlet *Dozhd*, IRA personnel were required to study and monitor tens of thousands of comments in order to better understand the language and trends of internet users in the United States. The ex-troll indicated that they were taught to avoid crude and offensive language that would be off-putting to the typical online reader.[118] According to the former employee, the IRA office dedicated to inflaming sentiments in the United States was prohibited from promoting anything about Russia or President Putin—primarily because, in the IRA's assessment, Americans do not normally talk about Russia. "Our goal wasn't to turn the Americans toward Russia . . . . Our task was to set Americans against their own government: to provoke unrest and discontent, and to lower Obama's support ratings."[119] IRA employees were trained to understand and exploit the nuances of politically sensitive issues in America, including taxes, LGBT rights, and the Second Amendment. Once IRA employees better understood the political fault lines and how Americans naturally argued online, their job was to incite them further and try to "rock the boat."[120]

(U) More recent open source reporting has provided fresh insight into the inner workings and goals of the IRA operation. Marat Mindiyarov, a former IRA troll, outlined for the Washington Post in 2018 how important Facebook became to the IRA. Mindiyarov described how workers in the Facebook Department of the IRA were paid twice as much and included a younger, more pop culturally literate crowd. In order to graduate to the Facebook Department, these trolls had to take a test to prove their English language skills, their ability to comment on American political nuance, and to confirm they had the necessary opposition to the United States.[121]

VI. (U) IRA ACTIVITIES AGAINST THE UNITED STATES IN 2016

A. (U) Origins of IRA Activity in the United States

(U) The IRA's foray into influence operations targeting the 2016 election began with a 2014 intelligence-gathering mission to the United States undertaken by two female employees: Anna Bogacheva and Aleksandra Krylova.

(U) Bogacheva worked for the IRA from the spring of 2014 to the fall of 2016.[122] Krylova, who began her employment in St. Petersburg in the fall of 2013 at the latest, rose to

---

[118] **(U)** Meduza, "An ex-St. Petersburg 'troll' speaks out," October 15, 2017 (summarizing an interview with "Maxim" by *Dozhd*).
[119] **(U)** *Ibid.*
[120] **(U)** *Ibid.*
[121] **(U)** Anton Troianovski, "A former Russian troll speaks: 'It was like being in Orwell's world,'" *Washington Post,* February 17, 2018.
[122] **(U)** Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election – Unraveling the Russia Story So Far," *The New York Times,* September 20, 2018: https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html?rref=collection%2Fsectioncollection%2Fpolitics.

become the IRA's third-highest ranking employee by the spring of 2014. Both secured visas to visit the United States in June 2014, and the two made stops in "Nevada, California, New Mexico, Colorado, Illinois, Michigan, Louisiana, Texas, and New York," according to the IRA indictment.[123]

[redacted] Operating as a reconnaissance team for the IRA, the two were sent to collect intelligence to be used in the organization's information warfare against the United States. Prior to the trip, they had worked with their colleagues to plan itineraries and purchase equipment, including "cameras, SIM cards, and drop phones." They also worked on various "evacuation scenarios" and other security measures for their trip.[124] Their visit likely helped the IRA refine tactics to be used on social media, but the trip represents only a small part of the wider operational effort to track and study Americans' online activities, understand U.S. political and social divisions, impersonate U.S. citizens online, and ultimately engage in information warfare against the United States. [redacted]

(U) According to the Special Counsel's Office, by April 2014, the IRA had formed a new department inside the larger organization that was focused solely on the U.S. population. Referred to as the "translator project," and alternately as the "Translator Department," the American department of the operation would grow to over 80 employees by July 2016.[126] By the summer of 2016, at the height of the U.S. campaign season, the "translator project" employees were posting more than 1,000 pieces of content per week, reaching between 20 and 30 million people in the month of September alone.[127] In addition, the IRA employees began contacting unwitting U.S. persons to better refine their tactics and targets. In one communication, an IRA operative posed as an American and spoke with a Texas-based grassroots organization, learning from the conversation that they should focus their activities on "purple states like Colorado, Virginia & Florida."[128]

---

[123] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[124] **(U)** *Ibid.*

[125] [redacted]

[126] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018); Special Counsel Robert S. Mueller, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, March 2019, Volume I, p. 26.

[127] **(U)** *See* Hannah Levintova, "Russian Journalists Just Published a Bombshell Investigation About a Kremlin-Linked 'Troll Factory,'" *Mother Jones*, October 18, 2017. Original report in Russian available at https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1.

[128] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[129] [redacted]

[130] **(U)** *Ibid.*

[131] [redacted]

[132] **(U)** *Ibid.*

(U) The IRA built a wide-ranging information operation designed to complement these other Russian influence activities directed toward interfering with and undermining U.S. democracy in 2016. The expanse and depth of this effort would only be understood in the aftermath of that campaign.

B. (U) IRA Operations Explicitly Targeting the 2016 U.S. Election

(U) At the direction of the Kremlin, the IRA sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump.[133]

(U) The overwhelming majority of the content disseminated by the IRA did not express clear support for one presidential candidate or another. Instead, and often within the context of the election or in reference to a candidate, most IRA content discreetly messaged narratives of disunity, discontent, hopelessness, and contempt of others, all aimed at sowing societal division. Nevertheless, a significant body of IRA content dealt with the election, and specifically the Republican and Democrat candidates. The TAG study led by Renee DiResta concluded that for all data analyzed, which included data captured before and after the 2016 U.S. election, roughly 6 percent of tweets, 18 percent of Instagram posts, and 7 percent of Facebook posts from IRA accounts mentioned Donald Trump or Hillary Clinton by name. On Facebook, that percentage translated to 1,777 posts that specifically mention Hillary Clinton (or a derivative moniker), which in turn generated over 1.7 million user interactions or engagements.[134]

(U) Numbers of posts are an imperfect and potentially misleading evidentiary base for drawing conclusions about motivations and objectives. The relatively low number of IRA Facebook and Twitter account posts that specifically mention either candidate is not dispositive of the IRA's intent to influence voters. In practice, the IRA's influence operatives dedicated the balance of their effort to establishing the credibility of their online personas, such as by posting innocuous content designed to appeal to like-minded users. This innocuous content allowed IRA influence operatives to build character details for their fake personas, such as a conservative Southerner or a liberal activist, until the opportune moment arrived when the account was used to deliver tailored "payload content" designed to influence the targeted user. By this concept of operations, the volume and content of posts can obscure the actual objective behind the influence operation. "If you're running a propaganda outfit, most of what you publish is factual so that

---

[133] **(U)** ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment (Declassified Version), January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.; Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller, III, March 2019.

[134] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

you're taken seriously," Graphika CEO and TAG researcher John Kelly described to the Commttee, "[T]hen you can slip in the wrong thing at exactly the right time."[135]

(U) The tactic of using select payload messages among a large volume of innocuous content to attract and cultivate an online following is reflected in the posts made to the IRA's "Army of Jesus" Facebook page. The page, which had attracted over 216,000 followers by the time it was taken down by Facebook for violating the platform's terms of service, purported to be devoted to Christian themes and Bible passages. The page's content was largely consistent with this façade. The following series of posts from the "Army of Jesus" page illustrates the use of this tactic, with the majority of posts largely consistent with the page's theme, excepting the November 1, 2016 post that represents the IRA's payload content:

- October 26, 2016: "There has never been a day when people did not need to walk with Jesus."
- October 29, 2016: "I've got Jesus in my soul. It's the only way I know. . . . Watching every move I make, guiding every step I take!"
- October 31, 2016: "Rise and shine—realize His blessing!"
- October 31, 2016: "Jesus will always be by your side. Just reach out to Him and you'll see!"
- November 1, 2016: "HILLARY APPROVES REMOVAL OF GOD FROM THE PLEDGE OF ALLEGIANCE."
- November 2, 2016: "Never hold on anything [sic] tighter than you holding unto God!"

(U) This pattern of character development, followed by confidence building and audience cultivation, punctuated by deployment of payload content is discernable throughout the IRA's content history.

(U) The IRA's ideologically left-leaning and right-leaning social media accounts posted content that was political in nature and made reference to specific candidates for President. Hillary Clinton, however, was the only candidate for President whose IRA-posted content references were uniformly negative. Clinton's candidacy was targeted by both the IRA's left and right personas, and both ideological representations were focused on denigrating her. As Renee DiResta notes, the political content of the IRA, "was unified on both sides in negativity towards Secretary Clinton."[136] The IRA's left-leaning accounts focused their efforts on denigrating

[135] **(U)** John Kelly, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[136] **(U)** Renee DiResta, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

Clinton and supporting the candidacy of either fellow Democrat candidate Bernie Sanders or Green Party candidate Jill Stein, at the expense of Hillary Clinton. Posts from the IRA's right-leaning accounts were unvaryingly opposed to Clinton's candidacy.

(U) In contrast to the consistent denigration of Hillary Clinton, Donald Trump's candidacy received mostly positive attention from the IRA's influence operatives, though it is important to note that this assessment specifically applies to pre-election content. The Committee's analysis indicates that post-election IRA activity shifted to emphasize and provoke anti-Trump sentiment on the left. DiResta's team assesses that in relation to pre-election content: "The majority of the political content was anti-Hillary Clinton; there appeared to be a consistent preference for then-candidate Donald Trump, beginning in the early primaries. . . . There was no pro-Clinton content."[137]

(U) Evidence of an overarching pro-Trump and anti-Clinton bias leading up to Election Day 2016 is also found in information obtained by Special Counsel's Office. For instance, IRA employees were directed to focus on U.S. politics and to "use any opportunity to criticize Hillary and the rest (except Sanders and Trump—we support them)."[138] Another IRA employee was criticized internally for having a "'low number of posts dedicated to criticizing Hillary Clinton' and was told 'it is imperative to intensify criticizing Hillary Clinton' in future posts."[139] Content and hashtags produced by IRA employees included "#Trump2016," "#TrumpTrain," "#MAGA," "#IWontProtectHillary," and "#Hillary4Prison."[140]

(U) One communication obtained by the Committee details an IRA employee's description of Election Day 2016, from the vantage of an information warfare operative: "On November 9, 2016, a sleepless night was ahead of us. And when around 8 a.m. the most important result of our work arrived, we uncorked a tiny bottle of champagne . . . took one gulp each and looked into each other's eyes. . . . We uttered almost in unison: 'We made America great.'"[141]

(U) Further, the IRA's attempts to engage political activists by using false U.S. personas to "communicate with unwitting members, volunteers, and supporters of the Trump Campaign involved in local community outreach, as well as grassroots groups that supported then-candidate Trump."[142]

---

[137] **(U)** Renee DiResta, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.
[138] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[139] **(U)** *Ibid.*
[140] **(U)** *Ibid.*
[141] [redacted]
[142] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

(U) In addition to denigrating Hillary Clinton, voter suppression among left-leaning audiences appears to have been another political goal of the IRA's influence operatives. Young Mie Kim, a digital advertisement research expert from the University of Wisconsin, has closely analyzed the IRA's Facebook advertisements. On the basis of Kim's analysis, three types of voter suppression campaigns on Facebook and Instagram emerge, including: "a) turnout suppression/election boycott; b) third-candidate promotion; and c) candidate attack, all targeting nonwhites or likely Clinton voters."[143] Kim found no evidence of a comparable voter suppression effort that targeted U.S. voters on the ideological right.

(U) Renee DiResta found similar evidence:

> *Voter suppression narratives were in [the data], both on Twitter (some of the text-to-vote content) and within Facebook, where it was specifically targeting the Black audiences. So the groups that they made to reach out to Black people were specifically targeted with 'Don't Vote for Hillary Clinton,' 'Don't Vote At All,' 'Why Would We Be Voting,' 'Our Votes Don't Matter,' [and] 'A Vote for Jill Stein is Not a Wasted Vote.'*[144]

(U) TAG researcher Phil Howard's findings support DiResta's assessment. Howard found that while both the ideological right and left in America were targeted:

> *The main difference is that where Conservative and right-wing voters were actively encouraged to get behind Trump's campaign, other voters were encouraged to boycott the election, vote for someone other than Clinton, and become cynical of the political process in general.*[145]

(U) Underscoring the insidiousness of the IRA's information warfare campaign, influence operations were conducted in cognizance of the U.S. political schedule and political events. Modifying their tactics and strategy to reflect real-life occurrences, the IRA's operatives would increase their activity around events relevant to the campaign schedule. This included pre-election events, like "candidate debates, [the] Republican convention, [and] Trump crossing the delegate threshold."[146] For example, "significant bursts of IRA activity" coincided with the third Democratic primary debate in January 2016, the sixth Republican primary debate in January 2016, the presidential debates between Clinton and Trump in the fall of 2016, and on

---

[143] **(U)** Young Mie Kim, "Uncover: Strategies and Tactics of Russian Interference in US Elections," Project DATA, University of Wisconsin, Madison, September 4, 2018, https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/09/Uncover.Kim_.v.5.0905181.pdf.

[144] **(U)** Renee DiResta, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[145] **(U)** Phil Howard, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[146] **(U)** Renee DiResta, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

Election Day 2016.[147] More broadly, the volume of posts originating from IRA accounts on Facebook and Instagram increased over the period between the national political conventions in July 2016 and Election Day.[148]

(U) The IRA's information warfare campaign also responded to real-world political events. For example, the IRA promoted multiple stories and narratives calling into question the state of Hillary Clinton's health after she fell ill at a September 11 memorial service in New York City in September 2016. IRA influence operatives posted phrased content on Twitter using hashtags that made the content easily discoverable to other Twitter users searching for content related to Clinton's health, including #HillarySickAtGroundZero, #ClintonCollapse, #ZombieHillary, and #SickHillary. According to researchers at Clemson University, IRA accounts tweeted these hashtags hundreds of times. As one of those researchers, Darren Linvill, points out:

> *You can see the peak times they tweet. You can see that they shift from hour to hour. One hour, they'll tweet their left-wing accounts, and the next hour they'll tweet their right-wing accounts. . . . You can see very clearly that it is one organization, and it has applied human capital as is needed, depending on what's happening politically, what current events are.*[149]

[redacted] A particular spike in IRA activity on October 6, 2016, stands out as an anomaly deserving further scrutiny. As reported by the *Washington Post* and noted by the Clemson research team, IRA influence operatives posted, at a pace of about a dozen tweets per minute, nearly 18,000 messages from their Twitter accounts on October 6, 2016. This spike in activity came a day prior to WikiLeaks's publication of emails stolen by the Russian GRU from the account of Hillary Clinton's campaign chairman, John Podesta. According to the researchers, on October 6 and 7, IRA Twitter accounts—particularly those accounts emulating ideologically left-leaning personas—significantly increased the volume of their content posting, with 93 of the "Left Troll" accounts posting content that could have directly reached other Twitter accounts 20 million times on those two days.[150] While no clear connection between the spike in IRA Twitter activity and WikiLeaks' release of the emails has been established, the Clemson researchers speculate that the timing was not coincidental: "We think that they [the IRA] were trying to activate and energize the left wing of the Democratic Party, the Bernie wing basically, before the WikiLeaks release that implicated Hillary in stealing the Democratic primary."[151] [redacted]

---

[147] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[148] **(U)** *Ibid.*

[149] **(U)** Jim Galloway, "Clemson researchers crack open a Russian troll factory," *Associated Press,* August 7, 2018.

[150] **(U)** Craig Timberg and Shane Harris, "Russian operatives blasted 18,000 tweets ahead of a huge news day during the 2016 presidential campaign. Did they know what was coming?" *Washington Post*, July 20, 2018.

[151] **(U)** *Ibid.*

[redacted]

(U) As detailed by the Special Counsel's Office, IRA operations to support Trump also involved activities inside the United States. For example, IRA operatives were able to organize and execute a series of coordinated political rallies titled, "Florida Goes Trump," using the Facebook group "Being Patriotic," the Twitter account @March_for_Trump, and other fabricated social media personas. Masquerading as Americans, IRA operatives communicated with Trump Campaign staff, purchased advertisements promoting these rallies on Facebook and Instagram, contacted grassroots supporters of then-candidate Trump, solicited U.S. citizens to participate in these events, and even paid select participants to portray Hillary Clinton imprisoned in a cage that had been constructed on a flatbed truck for this purpose.[153]

C. (U) Other IRA Operations Targeting U.S. Politicians and Society

(U) The IRA targeted not only Hillary Clinton, but also Republican candidates during the presidential primaries. For example, Senators Ted Cruz and Marco Rubio were targeted and denigrated, as was Jeb Bush.[154] Even after the 2016 election, Mitt Romney—historically critical of Russia and who memorably characterized the country as the United States' "number one geopolitical foe" during a 2012 presidential debate—was targeted by IRA influence operatives while being considered for Secretary of State in the Trump administration. Content posted from IRA social media pages and accounts referred to Romney as a "two headed snake" and a "globalist puppet," and IRA operatives posted the hashtag "#NeverRomney," in an effort to undermine his potential nomination.[155] On November 28, 2016, over 216,000 followers of the IRA's "Being Patriotic" Facebook page received the following post in their News Feed: "Romney was one of the first men who started the NeverTrump movement. It will be a terrible mistake if Trump sets him as the next secretary of state."

(U) In addition, the IRA "had a strategic goal to sow discord in the U.S. political system," which included—but was not limited to—targeting the 2016 U.S. presidential election.[156] John Kelly found that "[i]t's a far more sophisticated an attack than just caring about an election. And it's not just one election they care about. They care about the electoral system."[157] Darren Linvill echoed this point, concluding "[I]n general, there's been too much

---

[152] [redacted]

[153] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[154] **(U)** *Ibid*; Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018: https://www.newknowledge.com/articles/the-disinformation-report/.

[155] **(U)** Rob Barry and Shelby Holliday, "Russian Trolls Tried to Torpedo Mitt Romney's Shot at Secretary of State," *Wall Street Journal*, March 8, 2018.

[156] **(U)** Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[157] **(U)** John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

focus on Russian interference in the election. It's much more than that. It's interference in our society, in our culture, in our political conversation."[158]

[redacted]

[redacted]

(U) No single group of Americans was targeted by IRA information operatives more than African-Americans. By far, race and related issues were the preferred target of the information warfare campaign designed to divide the country in 2016. Evidence of the IRA's overwhelming operational emphasis on race is evident in the IRA's Facebook advertisement content (over 66 percent contained a term related to race) and targeting (locational targeting was principally aimed at "African-Americans in key metropolitan areas with well-established black communities and flashpoints in the Black Lives Matter movement"), as well as its Facebook pages (one of the IRA's top-performing pages, "Blacktivist," generated 11.2 million engagements with Facebook users), its Instagram content (five of the top 10 Instagram accounts were focused on African-American issues and audiences), its Twitter content (heavily focused on hot-button issues with racial undertones such as the NFL kneeling protests), and its YouTube

[158] **(U)** Jim Galloway, "Clemson researchers crack open a Russian troll factory," *Associated Press,* August 7, 2018.
[159] [redacted]
[160] **(U)** *Ibid.*
[161] **(U)** *Ibid.*
[162] **(U)** *Ibid.*
[163] **(U)** *Ibid.*

activity (96 percent of the IRA's YouTube content was targeted at racial issues and police brutality).

(U) The IRA's exploitation of racial tensions in an attempt to sow societal discord in the United States is not a new tactic for Russian influence operations. Rather, it is the latest incarnation of a long-standing Russian focus. Historically, the KGB's active measures program also made race a central feature of its operational targeting. As KGB archivist Vasili Mitrokhin noted: "The attempt to stir up racial tensions in the United States remained part of Service A's stock-in-trade for the remainder of the Cold War." For example, before the Los Angeles Olympics in 1984, KGB officers mailed falsified communications from the Ku Klux Klan to the Olympic committees of African and Asian countries. KGB officers also forged letters that were "sent to sixty black organizations giving fictitious details of atrocities committed by the [Jewish Defense] League against blacks."[164]

(U) As the TAG study led by Renee DiResta concluded:

> *The most prolific IRA efforts on Facebook and Instagram specifically targeted Black American communities and appear to have been focused on developing Black audiences and recruiting Black Americans as assets. . . . While other distinct ethnic and religious groups were the focus of one or two Facebook Pages or Instagram accounts, the Black community was targeted extensively with dozens; this is why we have elected to assess the messaging directed at Black Americans as a distinct and significant operation.*[165]

(U) In March 2018, the *Wall Street Journal* was among the first to report on a series of elaborate efforts by IRA operatives to target, coopt, and incite African-Americans to participate in real world activities the IRA promoted online. African-Americans targeted on social media were asked to deepen their engagement with IRA operatives—from signing petitions to teaching self-defense training courses. In one instance cited by the *Wall Street Journal*, operatives used the IRA Facebook page, "Black4Black," to solicit from African-American-led businesses in Cleveland, Ohio personal information in exchange for free promotions on social media.[166] IRA operatives also spearheaded and funded a self-defense program that entailed African-American trainers being paid to teach courses in their communities. As part of this operation, an African-American activist was paid roughly $700 to teach 12 self-defense classes in a local park under the auspices of the IRA-administered "BlackFist" Facebook page.[167]

---

[164] **(U)** Christopher M. Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive & the Secret History of the KGB*, Basic Books, 1985, p. 244.

[165] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[166] **(U)** Shelby Holliday and Rob Barry, "Russian Influence Campaign Extracted Americans' Personal Data," *Wall Street Journal,* March 7, 2018.

[167] **(U)** *Ibid.*

(U) Although the specific objectives behind the IRA's efforts to animate American social media users to organize around political and cultural identification is not entirely evident from the available data, the general intent to foment and promote divisiveness and discord amongst the American populace is strongly evidenced, as are the desire and capability of the IRA to effectively coopt unwitting Americans.

D. (U) IRA Use of Paid Advertisements

(U) Paid advertisements were not key to the IRA's activity, and moreover, are not alone an accurate measure of the IRA's operational scope, scale, or objectives, despite this aspect of social media being a focus of early press reporting and public awareness. According to Facebook, the IRA spent a total of about $100,000 over two years on advertisements—a minor amount, given the operational costs of the IRA are estimated to have been around $1.25 million dollars a month. The nearly 3,400 Facebook and Instagram advertisements the IRA purchased are comparably minor in relation to the over 61,500 Facebook posts, 116,000 Instagram posts, and 10.4 million tweets that were the original creations of IRA influence operatives, disseminated under the guise of authentic user activity. Further, numerous high-profile U.S. persons, such as Roger Stone, Michael McFaul, and Sean Hannity, unwittingly spread IRA content by liking IRA tweets or engaging with other IRA social media content, enhancing the potential audience for IRA content by millions of Americans.

(U) An analysis of the audiences targeted for receipt of those advertisements on Facebook nonetheless indicates that the IRA's use of advertising was consistent with its overall approach to social media. In particular, the IRA targeted some election swing states with advertisements that leveraged socially incendiary and divisive subjects. According to the report produced by the TAG working group led by Phil Howard and John Kelly, Facebook users in swing states were targeted 543 times, out of 1,673 instances of location targeting by the IRA. Additionally, in 342 instances, areas with significant African-American populations were targeted by the IRA with Facebook advertisements. TAG researchers believe that the targeting had more to do with race than a state's role in the Electoral College or status as a swing state:

> *We found from the data that location targeting of ads was not used extensively by the IRA, with only 1,673 different instances of location targeting, by 760 ads. These ads were usually used to target African Americans in key metropolitan areas with well-established black communities and flashpoints in the Black Lives Matter movement. Some make reference, for example, to Ferguson, MO, and a smaller group of ads that marketed rallies and demonstrations to users living in particular places.*[168]

[168] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018: https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

(U) The parameters and key terms the IRA employed in targeting its Facebook advertisements suggests a sophisticated understanding of where the rawest social sensitivities lie beneath the surface of the American political debate. Darren Linvill noted that the IRA had a "keen understanding of American psychology," they knew "exactly what buttons to press," and operated with "industrial efficiency."[169] Even so, the IRA failed to take advantage of more sophisticated targeting capabilities available to Facebook advertising customers. For example, IRA operatives did not utilize the "Custom Audiences" feature which would have allowed them to upload outside data and contact information, and permitted more advanced micro-targeting of their advertisements.[170]

[redacted]

E. (U) The IRA Information Warfare Campaign

[redacted]

[169] **(U)** Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election – Unraveling the Russia Story So Far," *New York Times,* September 20, 2018.

[170] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf ("The targeting for the IRA ads that we have identified and provided to the Committee was relatively rudimentary, targeting broad locations and interests, and did not use a tool known as Contact List Custom Audiences.")

[171] [redacted]

[172] **(U)** *Ibid.*

[173] [redacted]

(U) Disinformation experts agree with Prigozhin's assessment. Clint Watts, in March 2017 testimony to the Committee: "Over the past three years, Russia has implemented and run the most effective and efficient influence campaign in world history."[174]

(U) Eugene Rumer elaborated on Watts' point in offering this summary in March 2017 testimony to the Committee:

> *Russian meddling in the 2016 U.S. Presidential election is likely to be seen by the Kremlin as a major success regardless of whether its initial goal was to help advance the Trump candidacy. The payoff includes, but is not limited to a major political disruption in the United States, which has been distracted from many strategic pursuits; the standing of the United States and its leadership in the world have been damaged; it has become a common theme in the narrative of many leading commentators that from the pillar of stability of the international liberal order the United States has been transformed into its biggest source of instability; U.S. commitments to key allies in Europe and Asia have been questioned on both sides of the Atlantic and the Pacific. And last, but not least, the Kremlin has demonstrated what it can do to the world's sole remaining global superpower.*[175]

(U) Thomas Rid echoed this conclusion before the Committee: "The great Active Measures campaign of 2016 will be studied in intelligence schools for decades to come, not just in Russia of course but in other countries as well."[176]

F. (U) Ongoing IRA Activities

(U) IRA activity on social media did not cease, but rather increased after Election Day 2016. Evidence from well-known IRA accounts confirms that Russia-based operatives continued to be actively exploiting divisive social issues in the United States well after the 2016 election. After Election Day, Left-leaning IRA accounts were promoting hashtags such as "#Impeach45," "#Resist," and "#GunReformNow." Complementary right-leaning IRA accounts were focused on the NFL kneeling controversy, as well as hashtags critical of the FBI, such as the "#ReleaseTheMemo" meme. After the election, IRA operatives orchestrated disparate political rallies in the United States both supporting president-elect Trump, and protesting the results of the election. A mid-November 2016 rally in New York was organized around the theme, "show your support for President-Elect Donald Trump," while a separate rally titled, "Trump is NOT my President," was also held in New York, in roughly the same timeframe.[177]

---

[174] **(U)** Clint Watts, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.
[175] **(U)** Eugene Rumer, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.
[176] **(U)** *Ibid.*
[177] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

(U) More recent social media activity attendant to the 2018 midterm elections indicates ongoing influence operations emanating from Russia. A September 2018 criminal complaint brought by the U.S. Attorney's Office for the Eastern District of Virginia against Elena Alekseevna Khusyaynova, an employee of the IRA who allegedly served as the chief accountant for the IRA, alleges that Khusyaynova sought to "interfere with U.S. political and electoral processes, including the 2018 U.S. elections."[178]

[redacted]

VII. (U) IRA USE OF SOCIAL MEDIA BY PLATFORM

(U) Facebook. Russia's influence operatives have found appeal in the cost-effectiveness of Facebook pages as a targeted communications medium. Data provided to the Committee by Facebook indicates that the IRA used to its advantage many of Facebook's features, beyond purchased advertising and pages, including the "events," messenger," and "stickers" features. The IRA also exploited Instagram—a photo- and video-sharing social networking service owned by Facebook.

(U) The first specific public warning about Russian activity on the Facebook platform came in September 2017, when Facebook announced the discovery of "approximately $100,000 in ad spending from June of 2015 to May of 2017—associated with roughly 3,000 ads—that was

[178] **(U)** Indictment, *United States v. Elena Alekseevna Khusyaynova,* Case 1:18-MJ-464 (E.D. Va. Sept. 28, 2018).
[179] [redacted]
[180] **(U)** *Ibid.*
[181] [redacted]

connected to about 470 inauthentic accounts and pages in violation of [Facebook's] policies."[182] Though not explicitly identified by Facebook at the time, the platform later attributed the subject accounts, pages, and advertisements to the IRA. Ongoing scrutiny of activity on its platform eventually led Facebook to a significantly larger body of non-advertisement content ("organic activity") that originated from these same IRA accounts. This content had been engineered to appear American. Facebook's initial discovery of the IRA-purchased advertisements was an essential first step in uncovering the IRA's 2016 information warfare campaign.

(U) Facebook Advertisements

(U) The Committee's analysis of the IRA-purchased advertisements indicates that the vast majority neither mention expressly the U.S. presidential election, nor explicitly advocate voting for or against a particular presidential candidate. Roughly five percent of the advertisements viewed prior to the election (77 of 1,519) included text referencing Hillary Clinton or Donald Trump. Forty of the post-election advertisements tied to the IRA referenced one of these candidates. The Committee found the content of these advertisements to be substantially consistent with Facebook's public statements that the advertisements overwhelmingly pertained to divisive and inflammatory U.S. social issues. The subject of these advertisements spanned the ideological and political spectrum, ranging from race, sexuality, and gender identity, to immigration and Second Amendment rights. A number of the advertisements encouraged Facebook users to follow IRA-created pages dedicated to these issues, from which the IRA could manufacture and disseminate organic content on any number of politically charged subjects directly to their page followers. According to Committee analysis of materials provided by Facebook, almost all the advertisements were purchased with Russian rubles.

(U) Facebook estimates that 11.4 million people in the United States saw at least one of the 3,393 advertisements ultimately determined to have been purchased by the IRA.[183] Modelling conducted by Facebook indicates that 44 percent of the total user views of these advertisements ("impressions") occurred before the election on November 8, 2016, with 56 percent of the impressions taking place after the election. Roughly 25 percent of the ads were never seen by anyone.[184]

(U) The IRA used Facebook's geographic targeting feature to channel advertisements to intended audiences in specific U.S. locations. About 25 percent of the advertisements purchased by the IRA were targeted down to the state, city, or in some instances, university level. Specific content narratives emerge in connection with targeted locations. For instance, Michigan and Wisconsin (32 and 55 pre-election advertisements, respectively) were targeted with

[182] **(U)** Alex Stamos, "An Update on Information Operations on Facebook," Facebook, September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update/.
[183] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf.
[184] **(U)** *Ibid.*

advertisements overwhelmingly focused on the subject of police brutality. Facebook indicates that the IRA did not leverage the platform's Custom Audiences tool, which would have entailed uploading or importing an externally held list of advertisement targets or contact data, revealing the IRA's efforts were not as sophisticated or potentially effective as they could have been.[185]

(U) IRA-Generated Facebook Content

(U) While early media reporting on the IRA's Facebook activity focused on purchased advertising, the organic content generated by IRA influence operatives on their Facebook pages far surpassed the volume of targeted advertisements. That IRA organic content reached a significantly larger U.S. audience.

(U) Facebook's initial public disclosures about IRA activity identified 470 pages and accounts as originating with the IRA. The dataset furnished to the Committee includes over 60,000 unique organic posts from 81 of the pages Facebook associated with the IRA. An estimated 3.3 million Facebook users followed IRA-backed pages, and these pages are the predicate for 76.5 million user interactions, or "engagements," including 30.4 million shares, 37.6 million likes, 3.3 million comments, and 5.2 million reactions. Facebook estimates that as many as 126 million Americans on the social media platform came into contact with content manufactured and disseminated by the IRA, via its Facebook pages, at some point between 2015 and 2017. Using contrived personas and organizations, IRA page administrators masqueraded as proponents and advocates for positions on an array of sensitive social issues. The IRA's Facebook effort countenanced the full spectrum of American politics, and included content and pages directed at politically right-leaning perspectives on immigration policy, the Second Amendment, and Southern culture, as well as content and pages directed at left-leaning perspectives on police brutality, race, and sexual identity.

(U) Demonstrative of the range of themes the IRA targeted on its Facebook pages, the 10 most active IRA-administered Facebook pages include: "Stop A.I." (an abbreviation for "Stop All Invaders," the page was focused on illegal immigration); "Being Patriotic" (right-leaning themes, including Second Amendment rights); "Blacktivist" (targeted at African-Americans, and focused on African-American cultural issues and police brutality); "Heart of Texas" (right-leaning themes and Texas secession); "United Muslims of America" (targeted at refugee rights and religious freedom); "Brown Power" (targeted at Latino heritage and immigrant rights); "South United" (focused on Southern culture, conservative issues); "BM" (racial equality and police brutality); "LGBT United" (sexual and gender identity rights); and "Army of Jesus" (conservative, Christian themes). "BM" was a replacement page for the IRA's "Black Matters US" page, which Facebook took down in 2016. The IRA used the BM Facebook page to direct users to the Black Matters US website.[186]

---

[185] **(U)** *Ibid.*

[186] **(U)** Craig Timberg and Tony Romm, "New report of Russian disinformation prepared for the Senate, shows the operation's scale and sweep," *Washington Post*, December 17, 2018.

(U) The IRA influence operatives responsible for these pages created fake online personas with a specific, readily discernible social agendas in order to attract similarly minded Facebook users. The operatives then used divisive content to anger and enrage the curated audience. The findings of the TAG study lead by Phil Howard and John Kelly explain the strategy behind the IRA's Facebook pages:

> *The IRA messaging [had] two strategies. The first involved appealing to the narratives common within a specific group, such as supporting veterans and police, or pride in race and heritage, as a clickbait strategy to drive traffic to the Facebook and Instagram pages the IRA set up. . . . Then the pages posted content that intended to elicit outrage from these groups.*[187]

(U) The IRA's development of Facebook pages and cultivation of followers was painstaking and deliberate. This resulted in the IRA creating top-performing pages that enabled sustained, long-term interaction with Americans on the very issues that drive Americans apart. The "Stop A.I." page eventually attracted nearly 12.5 million engagements, while the "Blacktivist" page garnered almost 11.2 million.

(U) The IRA's Facebook pages were not just channels for disseminating content across the social media platform. The IRA also used its Facebook presence to provoke real world events, including protests, rallies, and spontaneous public gatherings or "flashmobs." Facebook identified at least 130 events that were promoted on its platform as a result of IRA activity. These events were promoted by, and attributed to, 13 of the IRA's Facebook pages. Approximately 338,300 genuine Facebook user accounts engaged with content promoting these events. 62,500 Facebook users indicated their intention to attend the event, while another 25,800 users evinced interest in the event.[188]

(U) An early example of the IRA's experimentation with social media and real world events occurred in the spring of 2015, when IRA operatives attempted to induce a mass gathering in New York City by offering free hot dogs. According to the findings of an investigation into the IRA by Russian media outlet RosBiznesKonsalting (RBC), the success in attracting unwitting Americans to the IRA's promotion of the "event" on Facebook prompted the IRA's operatives to begin using the social media platform's "events" feature much more proactively. The RBC report concluded, "From this day, almost a year and a half before the election of the

---

[187] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[188] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf.

US President, the 'trolls' began full-fledged work in American society."[189] The RBC investigation assesses that the IRA eventually spent about $80,000 to support 100 U.S. activists, who organized 40 different protests across the United States.[190]

(U) Over the course of 2016, IRA influence operatives trained particular focus on agitating political events and protests in the United States. One August 20, 2016, event promoted by the "Being Patriotic" page (over 216,000 followers) attempted to instigate flashmobs across Florida in support of Republican candidate for president, Donald Trump. Actual events promoted as "Florida Goes Trump" gatherings took place in Ft. Lauderdale and Coral Springs, Florida.[191]

(U) A May 2016, real world event that took place in Texas illustrates the IRA's ideological flexibility, command of American politics, and willingness to exploit the country's most divisive fault lines. As publicly detailed by the Committee during a November 1, 2017 hearing, IRA influence operatives used the Facebook page, "Heart of Texas" to promote a protest in opposition to Islam, to occur in front of the Islamic Da'wah Center in Houston, Texas. "Heart of Texas," which eventually attracted over 250,000 followers, used targeted advertisements to implore its supporters to attend a "Stop Islamization of Texas" event, slated for noon, May 21, 2016. Simultaneously, IRA operatives used the IRA's "United Muslims for America" Facebook page and its connection to over 325,000 followers to promote a second event, to be held at the same time, at exactly the same Islamic Da'wah Center in Houston. Again, using purchased advertisements, the IRA influence operatives behind the "United Muslims for America" page beseeched its supporters to demonstrate in front of the Islamic Da'wah Center—this time, in order to "Save Islamic Knowledge." In neither instance was the existence of a counter-protest mentioned in the content of the purchased advertisement.

(U) The competing events were covered live by local news agencies, and according to the Texas Tribune, interactions between the two protests escalated into confrontation and verbal attacks. The total cost for the IRA's campaign to advertise and promote the concomitant events was $200, and the entire operation was conducted from the confines of the IRA's headquarters in Saint Petersburg. Social media researcher John Kelly characterized the IRA's operational intent as "kind of like arming two sides in a civil war so you can get them to fight themselves before you go and have to worry about them."[192]

(U) Analysis of the dataset made available to the Committee indicates that IRA operatives also took advantage of the Facebook recommendation algorithm, an assessment

---

[189] **(U)** *See* Hannah Levintova, "Russian Journalists Just Published a Bombshell Investigation About a Kremlin-Linked 'Troll Factory,'" *Mother Jones*, October 18, 2017. Original report in Russian available at https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1.

[190] **(U)** *Ibid.*

[191] **(U)** Ben Collins, Gideon Resnick, et al., "Exclusive: Russians Appear to Use Facebook to Push Trump Rallies in 17 U.S. Cities," *The Daily Beast,* September 20, 2017.

[192] **(U)** John Kelly, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

Facebook officials have corroborated. When asked by Senator Susan Collins whether Facebook's recommendation engine ever suggested content created by IRA operatives to Facebook users, Facebook officials admitted that "This happened in some cases," adding that IRA content was "sometimes recommended when people followed similar pages."[193]

(U) In order to maximize the speed and scale of Russia's information warfare campaign, IRA operatives utilized the Facebook platform, and almost the entirety of its suite of features and capabilities, exactly as it was engineered to be used.

(U) Instagram. The use of Instagram by the IRA, and Instagram's centrality as a channel for disseminating disinformation and societally divisive content, has escaped much of the media and public attention that has focused on other social media platforms.

(U) IRA influence operatives in St. Petersburg, Russia, first posted on Instagram in January 2015—at the same time as their first posts on Facebook. Ultimately, IRA activity and engagement with Americans through Instagram accounts dramatically eclipsed the comparable interaction achieved through Facebook pages.[194]

(U) Data provided to the Committee indicates that the IRA used 133 Instagram accounts to publish over 116,000 posts. By comparison, the IRA used Facebook pages to publish over 60,000 posts. Engagement with fellow platform users was also significantly greater on Instagram, where IRA accounts accumulated 3.3 million followers and generated 187 million total engagements. By comparison, the IRA's Facebook page audience of 3.3 million produced 76 million virtual interactions. As Renee DiResta assessed in testimony to the Committee, "Instagram dramatically outperformed Facebook in terms of reach and in terms of likes and in terms of engagement, on a per-post [basis]."[195]

(U) The tactics IRA operatives used on the Instagram platform were consistent with those employed on the Facebook platform. The IRA's Instagram accounts focused on both the political left and right in America, and exploited the social, political, and cultural issues most likely to incite impassioned response across the ideological spectrum. Significantly, a discernible emphasis on targeting African-Americans emerges from analysis of the IRA's Instagram activity.[196]

---

[193] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf.

[194] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[195] **(U)** Renee DiResta, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[196] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

(U) The size, scope, and intended U.S. audience of the IRA's Instagram activity is reflected in the account names of the top 10 IRA Instagram accounts by follower numbers:

- "@Blackstagram_" targeted African-American cultural issues, amassed over 300,000 followers, and generated over 28 million interactions on the Instagram platform.
- "@american.veterans" was aimed at patriotic, conservative audiences, collected 215,680 followers, and generated nearly 18.5 million engagements.
- "@sincerely_black_" built a following of 196,754 Instagram users.
- "@rainbow_nation_us" emphasized sexual and gender identity rights and built a following of 156,465 users.
- "@afrokingdom_" had 150,511 followers on Instagram.
- "@_american.made" focused on conservative and politically right-leaning issues, including Second Amendment freedoms, and built a following of 135,008.
- "@pray4police" amassed 127,853 followers.
- "@feminism_tag" had 126,605 followers.
- "@_black_business" built a following of 121,861 Instagram users.
- "@cop_block_us" was followed by 109,648 Instagram users.

(U) In total, over the course of more than two years spent as an instrument for foreign influence operations, 12 of the IRA's Instagram accounts amassed over 100,000 followers, and nearly half of the IRA's 133 Instagram accounts each had more than 10,000 followers. On the basis of engagement and audience following measures, the Instagram social media platform was the most effective tool used by the IRA to conduct its information operations campaign.[197]

(U) Despite the high Instagram engagement numbers reported to the Committee through the TAG social media research effort, in testimony to the Committee, Facebook representatives indicated that Instagram content reached just 20 million users. In relation to the Facebook estimate, the published findings of the working group led by TAG researcher Renee DiResta contest that "the Instagram number is likely lower than it should be" and advocate for additional

[197] **(U)** The IRA also purchased targeted advertisements on Instagram. The data associated with these purchases was included in the total Facebook advertisements production to the Committee in the fall of 2017. The 3,393 advertisements purchased by the IRA included both Facebook and Instagram buys. Because the Facebook and Instagram buys were produced together, the Committee's analysis has also grouped them together, and these advertisements are collectively addressed in the above treatment of the IRA's use of Facebook advertisements.

research on Instagram content and activities.[198] Additional data and analysis concerning IRA activity on Instagram are required to resolve this discrepancy.

(U) Twitter. Though Twitter has fewer U.S. users than Facebook (68 million monthly active users on Twitter in the United States compared to 214 million Facebook users), Twitter is an extremely attractive platform for malicious influence operations like those carried out by the IRA due to its speed and reach. In 2017 testimony to the Committee, disinformation expert Thomas Rid identified Twitter as one of the more influential "unwitting agents" of Russian active measures.[199] Available data on the IRA's activity on the Twitter platform reinforces this assessment. As of September 2018, Twitter had uncovered over 3,800 accounts tied to the IRA.[200] According to data provided to the Committee by Twitter, those accounts generated nearly 8.5 million tweets, resulting in 72 million engagements on the basis of that original content.[201,202] More than half (57 percent) of the IRA's posts on Twitter were in Russian, while over one-third (36 percent) were in English.[203] Twitter estimates that in total, 1.4 million users engaged with tweets originating with the IRA.

(U) The activity of IRA influence operatives on Twitter outpaced the IRA's use of Facebook and Instagram. TAG members Phil Howard and John Kelly noted in their publicly released analysis of IRA activity:

> *The volume of Twitter posts made available to us is much larger than the volume of Facebook ads, Facebook posts, and Instagram posts. The average monthly*

---

[198] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[199] **(U)** Thomas Rid, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[200] **(U)** Twitter provided the Committee with a significant amount of data (including tweet content, handle names, engagement activity, and other metadata) for each of the over 3,800 accounts they identified as being linked to the IRA. That unique dataset was provided in installments that began in the fall of 2017. In October 2018, Twitter published a large archive of this information for the public to examine, including all tweets from the IRA-linked accounts. The Committee commends Twitter for its decision to publicize the data from these accounts and urges Twitter leadership to continue to make available to the public any future influence operation activities. The Committee urges other social media companies to take comparable steps to increase transparency and allow the public, outside researchers, investigators, and media to more fully examine the scope and scale of these types of influence operations as a matter of corporate responsibility and public service.

[201] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[202] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[203] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

> *Twitter post volume is over fifty thousand tweets per month, while the average monthly volume of Facebook ads, Facebook posts, and Instagram posts is in the hundreds to low thousands, never exceeding the six thousand mark.*[204]

(U) It appears from the data that the IRA, or a predecessor of the organization, began posting on Twitter in 2009, mostly in the Russian language and with a focus on the domestic Russian audience. These accounts continued to target Russia-internal issues and audiences until they were closed down in 2017.[205] It wasn't until 2013 that accounts tied to the IRA began to target a U.S. audience with English language tweets.[206]

(U) According to Phil Howard and John Kelly, the activity on Twitter constitutes the IRA's first use of a social media platform to conduct information warfare against the United States. The IRA effort shortly thereafter incorporated additional social media platforms including YouTube, Instagram, and Facebook:

> *It appears that the IRA initially targeted the US public using Twitter, which it had used domestically in Russia for several years. But as the IRA ramped up US operations toward the end of 2014, this dataset suggests that the IRA began leveraging other platforms in sequence: YouTube (here measured via Twitter citations of YouTube content), Instagram, and lastly Facebook.*[207]

(U) Initially, the IRA's Twitter activity targeting a U.S. audience was constrained to a relatively low operational tempo, approximating an initial test phase. By 2014 and 2015, however, the IRA's U.S.-focused efforts had significantly intensified. The elevated level of activity was sustained all the way through the 2016 presidential election campaign period, and spiked with an anomalous peak in activity immediately following the election, in November 2016. By mid-2017, U.S.-focused IRA activity on Twitter surpassed the IRA's domestic, Russia-focused information operations on the platform.[208] All Twitter accounts known to be associated with the IRA were suspended by the company by late 2017, and data associated with these accounts was turned over to the Committee.

(U) The data furnished to the Committee suggests IRA influence operatives probably used automated accounts to amplify payload content by tweeting and retweeting selected Twitter messaging. DiResta elaborated on the IRA's use of automated bots: "In the course of a similarity analysis we discovered still-active bots that were likely part of a commercially acquired or repurposed botnet."[209]

---

[204] **(U)** *Ibid.*
[205] **(U)** *Ibid.*
[206] **(U)** *Ibid.*
[207] **(U)** *Ibid.*
[208] **(U)** *Ibid.*
[209] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

(U) In addition to the Twitter accounts identified by the company as tied to the IRA, Twitter uncovered 50,258 automated accounts that they believe to be tied to Russia. These bot accounts were issuing tweets containing election-related content during the 2016 U.S. presidential election campaign period.[210] Although Twitter could not definitively link these bot accounts directly to the IRA, they illustrate the vulnerability of U.S. democratic processes to automated influence attacks, and the scale of the effort emanating from Russia to exploit that vulnerability. The coordinated activity of multiple bot accounts on social media represents an additional element of the foreign influence threat. According to platform monitoring reports prepared for officials in the United Kingdom, an estimated 2,800 automated accounts believed linked to Russia posted content concerning the 2018 poison attack on Sergei Skripal and his daughter in Salisbury, England, in an effort to provoke uncertainty over culpability for the attack.[211]

(U) The IRA's influence operatives dedicated significant effort to repurposing existing fake Twitter accounts, and creating new ones, that appeared to be owned by Americans. These accounts were used to build American audiences, accrue account followers, and amplify and spread content produced by the IRA. An analysis of the IRA's Twitter accounts illuminates the strategy and objectives behind its Twitter activity. Clemson researchers, led by Darren Linvill and Patrick Warren, collected all of the tweets from all the IRA-linked accounts between June 19, 2015, and December 31, 2017.[212] After removing from the sample all non-English accounts and those that did not tweet at all, the team was left with 1.875 million tweets associated with 1,311 IRA usernames.

(U) After conducting an analysis of all the content that IRA influence operatives manufactured, the Clemson researchers separated the IRA-affiliated accounts into five categories of social media platform activity. According to this analysis, "Within each type, accounts were used consistently, but the behavior across types was radically different." Characterizing the IRA Twitter effort as "industrial," the researchers described the campaign as "mass produced from a system of interchangeable parts, where each class of part fulfilled a specialized function."[213] The researchers named the account types: Right Troll, Left Troll, Newsfeed, Hashtag Gamer, and Fearmonger.

- **(U) Right Troll.** This was the largest and most active group of IRA-affiliated accounts. The 617 Right Troll Twitter accounts tweeted 663,740 times and cultivated nearly a million total followers. Clemson researchers characterized these accounts as focused on spreading "nativist and right-leaning populist messages." They strongly supported the

[210] **(U)** Jack Dorsey, Hearing before the Senate Select Committee on Intelligence, September 5, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[211] **(U)** Deborah Haynes, "Skripal attack: 2,800 Russian bots 'sowed confusion after poison attacks,'" *The Times UK*, March 24, 2018.
[212] **(U)** Darren Linvill and John Walker, "Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building," Clemson University, https://www.rcmediafreedom.eu/Publications/Academic-sources/Troll-Factories-The-Internet-Research-Agency-and-State-Sponsored-Agenda-Building.
[213] **(U)** *Ibid.*

candidacy of Donald Trump, employed the #MAGA hashtag, and attacked Democrats. Although nominally "conservative," Clemson researchers found that the IRA accounts rarely promoted characteristically conservative positions on issues such as taxes, regulation, and abortion, and instead focused on messaging derisive of Republicans deemed "too moderate" (including at the time Senators John McCain and Lindsey Graham).[214] The accounts generally featured very little in the way of identifying information, but frequently used profile pictures of "attractive, young women."

- **(U) Left Troll.** The second largest classification of IRA-affiliated Twitter accounts, consisting of around 230 Twitter profiles that generated 405,549 tweets, was Left Troll. The focus of the Left Troll Twitter accounts was primarily issues relating to cultural identity, including gender, sexual, and religious identity. Left Troll accounts, however, were acutely focused on racial identity and targeting African-Americans with messaging and narratives that mimicked the substance of prominent U.S. activist movements like Black Lives Matter. Left Troll accounts directed derisive content toward moderate Democrat politicians. These accounts targeted Hillary Clinton with content designed to undermine her presidential campaign and erode her support on the U.S. political left.

- **(U) News Feed.** Designed to appear to be local news aggregators in the United States, News Feed Twitter accounts would post links to legitimate news sources and tweet about issues of local interest. Examples of the IRA's news-oriented influence operative accounts on Twitter include @OnlineMemphis and @TodayPittsburgh. About 54 IRA accounts share the characteristics of this classification of Twitter profile, and they were responsible for 567,846 tweets.

- **(U) Hashtag Gamer.** More than 100 of the IRA's Twitter accounts were focused almost exclusively on playing "hashtag games," a word game popular among Twitter users. At times, these games were overtly political and engineered to incite reactions on divisive social issues from both the left and the right ends of the ideological spectrum.

- **(U) Fearmonger.** Finally, the IRA's 122 Fearmonger Twitter accounts were specifically dedicated to furthering the spread of a hoax concerning poisoned turkeys during the Thanksgiving holiday of 2014. The Fearmonger Twitter accounts tweeted over 10,000 times.

(U) The IRA's influence operatives coordinated across these Twitter account classifications to attack and defend both sides of socially divisive issues, particularly with respect to race relations and cultural divisions. An example of the IRA's ability to capitalize on both sides of a public debate can be found in the issue of NFL players kneeling in protest of police brutality and racism. Twitter accounts tied to the IRA from both the left and right side of the ideological spectrum used the topic to channel inflammatory content toward targeted, and ideologically like-minded, audiences. A Left Troll account, @wokeluisa, tweeted in support of

[214] **(U)** Jim Galloway, "Clemson researchers crack open a Russian troll factory," *Associated Press,* August 7, 2018.

Colin Kaepernick and the NFL protests on March 13, 2018, prompting 37,000 forwarded retweets. Simultaneous to this, and in the direction of the ideologically opposite audience, @BarbaraForTrump, a Right Troll account, was tweeting content hostile to the protests.[215]

(U) The Twitter data provided to the Committee shows that the IRA's influence operatives used multiple false personas to incite division and antipathy along a host of ideological fissures, simultaneously taking and attacking all sides of the arguments, all from the same internet protocol (IP) address. As TAG consultant John Kelly uncovered:

> *It was literally the same computer that was registering and operating the America accounts, pretending to be right and pretending to be left. So imagine it's the same guy, and the same people, and they got their two little marionette things with their puppets dancing on either end of a string. And they are playing them together. They are inhabiting both sides and figuring out ways to play them off against each other.*[216]

(U) As was the case with IRA activity on Facebook and Instagram, influence operatives based in Russia spent months developing fake Twitter personas and cultivating networks of supporters and followers among sympathetic and agreeable Americans. For example, 118 accounts secured more than 10,000 followers, and six accounts built followings of over 100,000 Twitter users.

(U) One of the IRA's most successful fake Twitter profiles was the @TEN_GOP account. By the time Twitter shut down the @TEN_GOP account in August 2017, it had amassed over 150,000 followers. By contrast, the legitimate Twitter account for the Tennessee Republican Party (@tngop) had 13,400 followers. Despite three separate requests by the actual Tennessee Republican Party organization to take down the account, @TEN_GOP was successful in deceptively injecting its inflammatory content into the political mainstream throughout 2016 and 2017.[217] Quotes and content from IRA influence operatives using the @TEN_GOP Twitter account were widely cited in press articles and mainstream media, and retweeted by celebrities and politicians, including several Trump campaign affiliates, including Donald Trump Jr., Kellyanne Conway, and Lieutenant General Michael Flynn (U.S. Army, retired).[218]

(U) As Clint Watts has described, influence operations like the @TEN_GOP effort can be extremely successful once the content filters into the mainstream press: "If you can get

---

[215] **(U)** Laura Rosenberger, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

[216] **(U)** John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[217] **(U)** Kevin Collier, "Twitter Was Warned Repeatedly About This Fake Account Run By a Russian Troll Farm and Refused to Take it Down," *BuzzFeed News,* October 18, 2017.

[218] **(U)** Philip Bump, "At least five people close to Trump engaged with Russian Twitter trolls from 2015 to 2017," *Washington Post,* November 2, 2017.

indigenous content, turn that into a conspiracy, and filter that into the mainstream media, that's a textbook case. . . . As an information warfare missile, that was a direct hit."[219]

(U) Another example of an effective IRA influence operation carried out on Twitter was conducted using the @Jenn_Abrams account. The persona associated with @Jenn_Abrams had accounts on multiple platforms, but most notably amassed over 80,000 followers on Twitter. This persona would tweet about everything from segregation to the futility of political correctness, and she would eventually be cited by more than 40 U.S. journalists before being taken down by Twitter in late 2017. John Kelly was among those following @Jenn_Abrams on Twitter. In testimony during a closed Committee hearing, Kelly described the ability of IRA influence operatives to infiltrate entire swaths of the political ecosystem on Twitter, of either ideological persuasion, using the persona:

> *Now . . . we're lighting up Jenn Abrams' account and all of the people following her are lit up. . . . So she had almost the entirety of the activist right, a good bit of the activist left, because remember the IRA has puppets on both sides – they are actually the same people running the machines – building her credibility. And then down below she's managed to make inroads and followership among the mainstream conservative part of that network, and she's even got a few of the mainstream liberal folks following her.*[220]

(U) The IRA was also successful using Twitter accounts feigning left-leaning ideological sentiment. An example cited by Laura Rosenberger in testimony to the Committee, @wokeluisa – which was still active in 2018 and had over 50,000 followers – claimed to be an African-American political science major in New York. Content produced under the guise of this persona would eventually appear "in more than two dozen news stories from outlets such as BBC, USA Today, Time, Wired, Huffington Post, and BET."[221]

(U) While original content creation was a preoccupation largely reserved for IRA operatives on Facebook and Instagram, the IRA's Twitter accounts were used to amplify events and promote the dissemination of content already existing on social media. This distinction notwithstanding, the Twitter platform was an integral tool for IRA operatives. As Renee DiResta detailed in her team's report:

> *Our impression of the IRA's Twitter operation is that it was largely opportunistic real-time chatter; a collection of accounts, for example, regularly played hashtag games. There was a substantial amount of retweeting. By contrast, Facebook and Instagram were used to develop deeper relationships, to create a collection of*

[219] **(U)** Brandy Zadrozny and Ben Collins, "How a right-wing troll and a Russian Twitter account created 2016's biggest voter fraud story," *NBC News,* October 30, 2018.
[220] **(U)** John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.
[221] **(U)** Laura Rosenberger, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

substantive cultural media pages dedicated to continual reinforcement of in-group and out-group ideals for targeted audiences. Twitter was, however, a part of the cross-platform brand building tactic; several of the Facebook, Instagram, Tumblr, and Reddit pages had associated Twitter accounts.[222]

(U) In a similar conclusion outlining the importance of Twitter to the IRA's effort to influence the thinking of Americans, Phil Howard and John Kelly found the following:

...the IRA Twitter data shows a long and successful campaign that resulted in false accounts being effectively woven into the fabric of online US political conversations right up until their suspension. These embedded assets each targeted specific audiences they sought to manipulate and radicalize, with some gaining meaningful influence in online communities after months of behavior designed to blend their activities with those of authentic and highly engaged US users.[223]

(U) Google. To a lesser but still critically important extent, Google and its numerous subsidiary platforms were also utilized and exploited by the IRA to the same end, in distinct ways. According to data provided to the Committee by Google, and additional public disclosures, numerous Google-affiliated platforms were utilized by IRA operatives, including YouTube, Google+, Gmail, Google's various advertisement platforms, Search, and Google Voice.

(U) There is little evidence that the IRA's operational efforts were as reliant on Google's products as they were on Facebook, Instagram, or Twitter to execute the most outwardly visible aspects of their information warfare campaign. The design, nature, and intended use of most Google products probably lies at the heart of this imbalance. Although Gmail accounts were used by IRA operatives to establish account profiles on other social media platforms, Google's products are generally not conducive to the rapid, expansive public dissemination of content that makes Facebook and Twitter attractive to influence operatives. Google's then-Senior Vice President and General Counsel, Kent Walker, testified to the Committee in November 2017, "Google's products didn't lend themselves to the kind of micro-targeting or viral dissemination that these [IRA] actors seemed to prefer."[224]

---

[222] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[223] **(U)** Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization in the United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

[224] **(U)** Kent Walker, Hearing before the Senate Select Committee on Intelligence November 1, 2017, available at https://www.intelligence.senate.gov/hearings/open.

(U) IRA operatives were not, however, entirely absent from Google and its subsidiaries. Among the Google products that contributed to the wide-ranging character of the IRA's information warfare campaign, YouTube was by far the most utilized by operatives. In addition to IRA activity on YouTube, Google also uncovered evidence that Russian operatives utilized some of the company's advertisement products and services during the 2016 election campaign period. Using Gmail accounts connected to the IRA, influence operatives reportedly purchased $4,700 worth of search advertisements and more traditional display advertisements in relation to the 2016 presidential election.[225]

(U) Americans also engaged with a separate $53,000 worth of politically themed advertisements that either had a connection to a Russian internet or physical building address, or had been purchased with Russian rubles. It is unclear, however, whether these ads are tied to the Russian government. The content of these ads spans the political spectrum, and features messages alternately disparaging and supporting candidates from both major political parties, as well as the then incumbent U.S. President. The total amount of advertisement spending related to the election on Google AdWords was about $270 million, making the Russia-linked purchases on the Google platform miniscule by comparison. Gmail addresses and other Google applications were also utilized to establish accounts on both Facebook and Twitter. According to Renee DiResta, "YouTube, G+, and other properties were leveraged to either host content or to support personas."[226]

(U) As a tool of information warfare, the Google "Search" application presents a distinct method for broadly disseminating disinformation. Google's search engine is by far the most utilized on the internet, however Google has been criticized for its failure to address issues with its PageRank algorithm. Periodically, particularly in the context of fast breaking news, Google's algorithm can elevate extremist content or disinformation to the top of certain searches. Days after the 2016 presidential election, a falsified media account of President-elect Donald Trump having won the popular vote briefly ranked higher than stories that accurately reflected the U.S. popular vote result.[227]

(U) Google was quick in responding to and addressing the misleading 2016 popular vote search results, but the example illustrates that the Google platform's search results feature is not impervious to manipulation designed to spread deceptive and misleading information. Public statements by Google representatives emphasize that the company realizes no business interest or advantage in the selective promotion of falsified news stories, extremist content, and conspiracy theories.

(U) As Laura Rosenberger testified to the Committee, "Another way the Russian government distorts the information space is through manipulating search results. Just Google

---

[225] **(U)** *Ibid.*

[226] **(U)** Renee DiResta, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

[227] **(U)** Philip Bump, "Google's top news link for 'final election results' goes to a fake news site with false numbers," *Washington Post,* November 14, 2016.

any geopolitical issue of significance to Moscow—MH-17, the White Helmets, the Novichok poisonings in the UK—and you will be served up a set of top results consisting of outlandish conspiracy theories emanating from Russia."[228]

(U) Private sector entities around the world dedicate sustained effort to manipulating the Google Search algorithm for commercial benefit. "Search-engine optimization," which entails maximizing the likelihood of favored content appearing among the highest ranked query results, is a standard marketing firm capability routinely used in the promotion of businesses and products. The IRA's 2016 information warfare campaign featured some of the same capabilities. According to the Department of Justice indictment, the IRA devoted an entire department to search-engine optimization, the objective of which was the elevation of the IRA's content in the search results of Americans, in furtherance of the IRA's 2016 information warfare campaign.[229]

(U) YouTube. Distinct from Facebook and Twitter, the YouTube platform is not independently conducive to rapid and expansive content sharing. Achieving the "viral" spread of YouTube videos generally entails capitalizing on the reach and magnitude of Facebook and Twitter networks to spread links to the video hosted on YouTube.

(U) Data provided to the Committee by YouTube concerning IRA-associated content and accounts indicates that IRA influence operatives began posting videos to YouTube as early as September 2015. More than 1,100 videos, or 43 hours of content, were eventually posted on 17 YouTube channels the IRA established. Two of these channels were overtly political in character, and focused on the 2016 U.S. presidential election.[230]

(U) The overwhelming preponderance of the video content posted to the IRA's YouTube channels was aimed directly at the African-American population. Most of the videos pertained to police brutality and the activist efforts of the Black Lives Matter organization. Posted to 10 of the IRA's YouTube channels, were 1,063 videos—or roughly 96 percent of the IRA content—dedicated to issues of race and police brutality. The names of the IRA's YouTube channels were consistent with the posted video content and included "Black Matters," "BlackToLive," "Cop Block US," "Don't Shoot," and "PoliceState." The content of the videos posted to those channels exploits issues of extraordinary sensitivity inside the African-American community. It is difficult to reconcile this fact with public testimony to the Committee by a Google representative that, "The videos were not targeted to any particular sector of the US population as that's not feasible on YouTube."[231]

---

[228] **(U)** Laura Rosenberger, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

[229] **(U)** Indictment, *United States v. Internet Research Agency, et al.*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[230] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.

[231] **(U)** Kent Walker, Hearing before the Senate Select Committee on Intelligence November 1, 2017, available at https://www.intelligence.senate.gov/hearings/open.

(U) Only 25 videos posted to the IRA's YouTube channels featured election-related keywords in the title. All of the IRA's politically-oriented videos were thematically opposed to the Democrat candidate for president, Hillary Clinton. Some of the videos featured expressly voter suppressive content intended to dissuade African-American voters from participating in the 2016 presidential election, while others encouraged African-Americans to vote for Jill Stein.

(U) YouTube continues to be the propaganda vehicle of choice for Russia's state-sponsored news organization, RT (formerly Russia Today). As of February 2019, RT had nearly 3.3 million global subscribers on its YouTube channel. In 2013, RT was the first self-described "news channel" to break 1 billion views on YouTube, and in 2017, RT's YouTube channel accumulated its five billionth view. RT's social media presence and activities were outlined in the January 6, 2017 Intelligence Community Assessment, in an annex to the unclassified version of the report.[232]

(U) Reddit. IRA influence operatives were active on the Reddit platform during the 2016 presidential election campaign period, in part it appears, to test audience reaction to disinformation and influence campaign content before its dissemination through other social media platform channels.

(U) Motivated by the fall 2017 revelations of significant IRA activity on the Facebook and Twitter platforms, Reddit conducted an internal investigation into whether IRA activity had taken place on its platform. The results of Reddit's internal investigation, which were shared with the Committee, indicate that IRA influence operatives were active on the platform and attempted to engage with American Reddit users. Internal investigators characterized 944 Reddit accounts as "suspicious," imparting that investigators judged there was a "high probability" that the accounts were linked to the IRA.[233] Analysis of the accounts indicates that nearly three-quarters (662 accounts) achieved zero karma points, indicative of minimal engagement by the broader Reddit user base.

(U) According to Reddit, the 944 evaluated accounts were responsible for around 14,000 posts. Of those posts that contained socially or politically divisive content, most were thematically focused on police brutality, issues of race, and the disparagement of Hillary Clinton. A Reddit account with the username Rubinjer, the most popular of the accounts Reddit investigators assessed as probably linked to the IRA, posted a video that falsely claimed to depict Hillary Clinton engaged in a sex act. The video, which was ultimately posted on a separate website dedicated to pornographic content and viewed more than 250,000 times, was created by the IRA's influence operatives.[234] The same Reddit account was used to promote a videogame titled Hilltendo, in which players maneuver an animated Hillary Clinton as the avatar deletes emails and evades FBI agents. IRA influence operatives attempted to achieve viral

---

[232] **(U)** ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," *Intelligence Community Assessment (Unclassified Version),* January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[233] **(U)** Reddit, Submission to SSCI, April 10, 2018.
[234] **(U)** Ben Collins, "Russia-Linked Account Pushed Fake Hillary Clinton Sex Video," *NBC News,* April 10, 2018.

dissemination of the video game across social media, weeks prior to the 2016 election.[235] IRA influence operatives also used Reddit as a platform for Russia-friendly narratives. As Laura Rosenberger testified to the Committee: "On Reddit, multiple IRA-generated memes posted to the 'r/funny' sub-reddit were targeted at discouraging United States support for Montenegrin-accession to NATO, attempting to portray Montenegrins either as free riders or as protestors resisting this move."[236]

(U) In Reddit's assessment, IRA information warfare activity on its platform was largely "unsuccessful in getting any traction." The company judges that most Russian-origin disinformation and influence content was either filtered out by the platform's moderators, or met with indifference by the broader Reddit user base. In an April 2018 statement, Reddit CEO, Steve Huffman, stated that the investigations had "shown that the efforts of [Reddit's] Trust and Safety Team and Anti-Evil teams are working," and that the "work of [Reddit] moderators and the healthy skepticism of [Reddit] communities" made Reddit a "difficult platform to manipulate."[237] Nevertheless, the largely anonymous and self-regulated nature of the Reddit platform makes it extremely difficult to diagnose and attribute foreign influence operations. This relative user autonomy and the dearth of information Reddit collects on its users make it probable that Reddit remains a testbed for foreign disinformation and influence campaigns.

(U) Tumblr. Following Facebook's September 2017 disclosures about IRA activity on the platform, Tumblr conducted an internal investigation to determine whether Russia-based operatives had also been active on Tumblr.[238] The ensuing investigation uncovered 84 accounts determined to be associated with the IRA. Most of the accounts were created in 2014 or 2015, and did not exhibit indications of automation. The IRA-associated Tumblr accounts generated about 100,000 posts, and were engaged significantly with authentic (non-IRA) user accounts on Tumblr. Tumblr estimates that IRA influence operatives used the platform to interact with 11.7 million unique U.S. users, and nearly 30 million unique users globally. Tumblr did not find any indication that IRA operatives purchased advertisements through the platform's advertising feature.[239]

(U) Tumblr's investigative findings indicate that content posted to the IRA's accounts was focused primarily on politics and divisive social issues. A discernible effort to focus content delivery toward African-Americans is evident in the Tumblr account names the IRA chose, and the content those accounts posted. Among the IRA's Tumblr profile names were:

---

[235] **(U)** Jose Pagliery and Donie O'Sullivan, "Russians released anti-Clinton video game weeks before election," *CNN Business*, March 8, 2018.

[236] **(U)** Laura Rosenberger, Written Statement, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.

[237] **(U)** Steve Huffman, "Reddit's 2017 transparency report and suspect account findings," Reddit, April 10, 2018, https://www.reddit.com/r/announcements/comments/8bb85p/reddits_2017_transparency_report_and_suspect/

[238] **(U)** Tumblr is a New York-based social networking and micro-blogging site that was created in 2007, and eventually acquired by Verizon and placed under the umbrella subsidiary, Oath, Inc. (later, renamed Verizon Media).

[239] **(U)** SSCI staff interview with Oath/Tumblr on Russian influence, April 20, 2018.

"aaddictedtoblackk," "black-to-the-bones," "blackness-by-your-side," "blacknproud," and "bleepthepolice."[240] Jonathan Albright, a researcher at the Tow Center for Digital Journalism at Columbia University, is unequivocal in concluding that on Tumblr, the IRA's influence operatives deliberately focused on messaging young African-American with narratives and payload content: "The evidence we've collected shows a highly engaged and far-reaching Tumblr propaganda-op targeting mostly teenage and twenty-something African-Americans."[241]

(U) As was the case on other social media platforms, IRA influence operatives used Tumblr accounts to build audiences of like-minded Americans, into which they would sow socially and politically divisive content. As reported in *BuzzFeed*, a Tumblr account named "4mysquad," which was later revealed by Tumblr to be operated by the IRA, dealt almost exclusively with issues of sensitivity to the African-American community. On occasion, political content promoting the presidential campaign of Bernie Sanders, or criticizing Hillary Clinton was posted to this account. As an example, "4mysquad" posted a video of Clinton calling young black gang members "superpredators," which generated more 50,000 engagements with authentic Tumblr users.[242] Over time, however, the IRA's influence operatives took the messaging broadcast via the "4mysquad" Tumblr account further than the credulity of some users would allow. As one former follower of the account was quoted, after "4mysquad" began posting content promoting the presidential campaign of Donald Trump, "I unfollowed him and the thing that was a red flag was that it was supposedly a black liberal blog that at some point started rooting for Trump to win."[243]

(U) Tumblr shared the results of the 2017 internal investigation with federal law enforcement. In the fall of 2018, law enforcement reciprocally alerted Tumblr to potential IRA operational activity tied to the U.S. 2018 mid-term elections taking place on the platform. On the basis of this insight, Tumblr identified 112 accounts tied to what was identified as an influence operation, indicating that Russia-based influence operatives continue to exploit the Tumblr platform targeting the United States.[244]

(U) In addition to the internal investigation into IRA activities on Tumblr, Oath's security team also searched the company's other digitally-based platforms, uncovering 484 Yahoo email accounts associated with other publicly identified IRA account information. Most of the Yahoo email accounts were used to establish profiles and enable commenting on other social media platforms.[245] Oath's internal security investigation also uncovered a small number

[240] **(U)** Tumblr, "Public record of usernames linked to state-sponsored disinformation campaigns," March 23, 2018, https://staff.tumblr.com/post/180179385310/keeping-our-promise-to-be-transparent-about.
[241] **(U)** Craig Silverman, "Russian Trolls Ran Wild on Tumblr and the Company Refuses to Say Anything About It," *BuzzFeed News,* February 6, 2018.
[242] **(U)** *Ibid.*
[243] **(U)** *Ibid.*
[244] **(U)** Tumblr Staff, "Keeping our promise to be transparent about state-sponsored disinformation campaigns," Tumblr, November 16, 2018, https://staff.tumblr.com/post/180179385310/keeping-our-promise-to-be-transparent-about.
[245] **(U)** SSCI staff interview with Oath/Tumblr on Russian influence, April 20, 2018.

of accounts with some indications of association with the IRA on Flickr, a photo and video hosting service. Only four of the seven Flickr accounts investigators found associated with the IRA had posted images.[246]

(U) LinkedIn. LinkedIn discovered that IRA-linked activity occurred on the platform during the period of the 2016 presidential election. In the course of an internal investigation initiated after the fall 2017 Facebook disclosures, LinkedIn uncovered 91 accounts and five fake company pages believed to be tied to the IRA. Most of the accounts were established in 2015. About 24 of the accounts never posted content to the platform. Eighty percent of the content posted from these accounts generated no engagement from any other LinkedIn users. None of the accounts is known to have purchased ads or any promoted content on the platform.[247] However a common IRA approach involved establishing credibility by creating multiple social media accounts across an array of platforms, under the same falsified American persona.

(U) Though foreign influence operational activity on LinkedIn appears to be limited, the platform and its users are a significant target for foreign intelligence services. LinkedIn users submit, and make publicly accessible, significant personal and professional data in the pursuit of networking opportunities and to attract potential employers. This renders the platform a valuable source of information on an array of sensitive intelligence targets—including the identities of government employees, active duty military personnel, cleared defense contractors, and others. As Director of the U.S. National Counterintelligence and Security Center William Evanina has stated, LinkedIn "makes for a great venue for foreign adversaries to target not only individuals in the government, formers, former CIA folks, but academics, scientists, engineers, anything they want. It's the ultimate playground for (intelligence) collection."[248]

(U) Other Platforms. Medium, a popular online publishing platform, and Pinterest, a photo- and image-focused social media platform with over 250 million active users, both publicly acknowledged the discovery of IRA influence operative activity on their platforms. The Committee's TAG researchers also discovered IRA activity on other popular internet sites, including Vine, Gab, Meetup, VKontakte, and LiveJournal. Even browser extensions, music applications, and games, like Pokémon Go were incorporated into the IRA's influence operation.[249] As Renee DiResta notes, the widespread use of numerous applications and platforms illustrates "the fluid, evolving, and innovative tactical approach the IRA leveraged to interfere in US politics and culture."[250]

---

[246] **(U)** *Ibid.*
[247] **(U)** Blake Lawit, General Counsel, LinkedIn, *Letter to SSCI,* December 21, 2018.
[248] **(U)** Jonathan Landay and Warren Strobel, "Exclusive: U.S. Accuses China of "Super Aggressive" Spy Campaign on LinkedIn," *Reuters,* August 31, 2018.
[249] **(U)** Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes of the Internet Research Agency," *New Knowledge*, December 17, 2018, https://www.newknowledge.com/articles/the-disinformation-report/.
[250] **(U)** *Ibid.*

VIII. (U) OTHER RUSSIAN SOCIAL MEDIA INFORMATION WARFARE EFFORTS

A. (U) Main Intelligence Directorate (GRU)

(U) Other Russian government-funded and -directed entities, particularly the Russian intelligence services, also conducted social media efforts directed at the 2016 U.S. election. The Russian GRU conducted a wide variety of activities on social media. In January 2018 written responses to Committee inquiries, Facebook confirmed the presence of activity attributed to the GRU (also known as Fancy Bear or APT28) on its platform: "We have also tracked activity from a cluster of accounts we have assessed to belong to a group, APT28, that the U.S. government has publicly linked to Russian military intelligence services and the 'DCLeaks' organization."[251]

(U) Much of the activity related to APT28 found by Facebook in 2016 appeared to Facebook security experts as consistent with more typical offensive cyber activities, generally attributed to foreign intelligence services, including the targeting and attempted hacking of "employees of major U.S. political campaigns." However, Facebook later detected the APT28 group's engagement in what they described as "a new kind of behavior" later in the summer of 2016. Facebook uncovered GRU attempts to engage in influence activities, namely, "the creation of fake personas that were then used to seed stolen information to journalists." As Facebook notes, "These fake personas were organized under the banner of an organization that called itself 'DCLeaks.'"[252]

(U) The GRU's direct role in the 2016 information warfare campaign was publicly exposed in yet another indictment obtained in July 2018 by the Special Counsel's Office. This indictment against the GRU ("the GRU indictment") outlined very specific details about the GRU's online influence operations.

(U) The GRU indictment charged a number of GRU operatives, including Aleksandr Vladimirovich Osadchuk, a colonel in the Russian military and the commanding officer of the GRU's unit 74455. The Special Counsel's Office described Unit 74455's role in the GRU's influence operation: "Unit 74455 assisted in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU."

(U) The public accounting from the Special Counsel's Office also reveals the cross-platform character of these information operations, which involved several of the social media companies, including Facebook and Twitter.[253]

---

[251] **(U)** Colin Stretch, Responses by Facebook to SSCI Questions for the Record from hearing on November 1, 2017, submitted January 8, 2018, available at https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf

[252] **(U)** *Ibid.*

[253] **(U)** Indictment, *United States v. Viktor Borisovich Netyksho, et al.,* Case 1:18-cr-00215-ABJ (D.D.C. July 13, 2018).

(U) On *or about June 8, 2016, and at approximately the same time that the dcleaks.com website was launched, the Conspirators created a DCLeaks Facebook page using a preexisting social media account under the fictitious name "Alice Donovan." In addition to the DCLeaks Facebook page, the Conspirators used other social media accounts in the names of fictitious U.S. persons such as "Jason Scott" and "Richard Gingrey" to promote the DCLeaks website.*[254]

(U) *On or about June 8, 2016, the Conspirators created the Twitter account @dcleaks_. The Conspirators operated the @dcleaks_ Twitter account from the same computer used for other efforts to interfere with the 2016 U.S. presidential election. For example, the Conspirators used the same computer to operate the Twitter account @BaltimoreIsWhr, through which they encouraged U.S. audiences to "[j]oin our flash mob" opposing Clinton and to post images with the hashtag #BlacksAgainstHillary.*[255]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[254] **(U)** *Ibid.*
[255] **(U)** *Ibid.*

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

256 [redacted]

- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

- [redacted]

- [redacted]

[redacted]

(U) According to FBI:

[redacted]

[redacted]

[redacted]

(U) A 2017 analysis by cybersecurity company FireEye outlined additional personas assessed to be associated with Kremlin-linked organizations. From FireEye's report: "We assess, with varying respective degrees of confidence, that Russian state-sponsored actors leveraged at least six false 'hacktivist' personas over the course of 2016 to conduct a series of information operations designed to further Russian political interests."[258] Personas attributed to Russian state sponsors included Guccifer 2.0, DCLeaks, @anpoland (Anonymous Poland), Fancy Bears' Hack Team, @pravsector (Pravvy Sektor), and Bozkurt Hackers.[259]

(U) According to the 2017 analysis by FireEye: "Personas engaged in highly organized, systematized, and in some cases semi-automated social media dissemination campaigns to promote leaks and associated political narratives to media outlets and other influencers, in order to generate mainstream coverage and public attention." The activities included "cadres of Twitter accounts repetitively publishing identical tweets promoting threat activity. [The accounts were] [d]esigned to further spread awareness of incidents and boost the credibility of the personas by creating a grassroots impression that more genuine Twitter users are talking about incidents than is accurate."[260]

(U) Even as late as the fall of 2018, Facebook continued to find activity attributed to the GRU. In August 2018, Facebook announced additional actions against "Pages, groups and accounts that can be linked to sources the US government has previously identified as Russian military intelligence services."[261] As detailed by this enforcement of Facebook's terms of service, Russian-backed influence operations did not stop after the 2016 U.S. election.

---

[257] **(U)** FBI, Written response to SSCI inquiry of January 3, 2019, March 1, 2019.
[258] **(U)** FireEye, "Anatomy of Russia's 2016 Influence Operations: Hacks, leaks, and the manipulation of political opinion," FireEye, Inc., October 2017.
[259] **(U)** The *New York Times* reported in September 2017 about activity sponsored by Anonymous Poland Twitter accounts that were involved in spreading political disinformation during the 2016 U.S. election. Their article noted "last October [2016], hundreds of Anonymous Poland Twitter accounts posted a forged letter on the stationery of the conservative Bradley Foundation . . . purporting to show that it had donated $150 million to the Clinton campaign. The foundation denied any such contribution, which would have been illegal and . . . highly unlikely."
[260] **(U)** FireEye, "Anatomy of Russia's 2016 Influence Operations: Hacks, leaks, and the manipulation of political opinion," FireEye, Inc., October 2017.
[261] **(U)** Facebook Newsroom, "Taking Down More Coordinated Inauthentic Behavior," Facebook, August 21, 2018, https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/.

B. [redacted]

[redacted]

- [redacted]

- [redacted]

---

[262] [redacted]

[263] **(U)** *Ibid.*

[264] **(U)** *Ibid.*

[265] [redacted]

[266] **(U)** *Ibid.*

[267] **(U)** *Ibid.*

[redacted]

- [redacted]

- [redacted]

C. (U) Other Russian Government Activities

(U) In fall 2016, an FBI contractor analyzed a pro-Russian network of 13 Twitter accounts. The account @TeamTrumpRussia was the central node in this network. According to FBI:

> **(U)** *@TeamTrumpRussia and the other 12 accounts had a total of 1,504,511 followers at the time the contractor collected its data (17 to 19 October 2016). Four of the 13 accounts had a reciprocal relationship with Sergey Nalobin, an employee of Russia's Ministry of Foreign Affairs (MFA), whose Twitter profile states he is responsible for "digital diplomacy and social media." In August 2015, the United Kingdom refused to extend Nalobin's visa because of his involvement with a UK political group called "Conservative Friends of Russia," according to open source reporting.*
>
> **(U)** *The FBI contractor found over 70 percent of the network's Tweets contained links to Websites "outside of the mainstream US press, and are known to be*

[redacted]

[268] [redacted]

[269] [redacted]

[270] **(U)** *Ibid.*

[271] [redacted]

[272] **(U)** *Ibid.*

highly supportive of the Trump campaign. Of those sites, a number are also known to overtly draw content from Russian disinformation sites or are suspected of more covert connections to the Kremlin."

[redacted] *A second report produced by the contractor examined the network's efforts to promote allegations of voter fraud in advance of the election,* [redacted]

[redacted]

IX. (U) U.S. GOVERNMENT RESPONSE

(U) Throughout the 2016 U.S. presidential election campaign period, the IRA was a largely obscure entity operating far from America's borders inside a stand-alone building in St. Petersburg, Russia. Despite the fact that the IRA began planning and implementing its electoral interference as early as 2014, its existence and activities were not well known to the wider American public and the U.S. Government until well after the election had passed. Even the January 6, 2017 Intelligence Community Assessment, authored as the Intelligence Community's comprehensive account of Russia's attack on the U.S. election, made no more than a passing reference to the cadre of professional trolls housed in the IRA.[275] In early September 2017, Facebook—under significant pressure from this Committee and the broader United States Congress—disclosed a collection of accounts linked to the IRA, beginning to bring the scope of

[273] **(U)** FBI, Written response to SSCI inquiry of January 3, 2019, March 1, 2019.

[274] [redacted]

[275] [redacted]

the IRA's electoral activities into focus.[276] The criminal nature of the IRA's interference crystallized with the Special Counsel's public indictment in February 2018.[277]

(U) Some of the starkest early insights into IRA activities for western audiences were reported by *The Guardian*'s Shaun Walker in his April 2015 report, "Salutin' Putin," and by Adrian Chen in *The New York Times Magazine* investigative report on the IRA, "The Agency."[278] These investigative reports take on new significance in light of the Committee's work.

(U) The U.S. Intelligence Community's ability to identify and combat foreign influence operations carried out via social media channels has improved since the 2016 U.S. presidential election. Communication and information sharing between government agencies and the social media companies has been a particular point of emphasis, and the Committee strongly supports these efforts. Characterizing the company's present relationship with Federal law enforcement, Twitter representatives have informed the Committee, "We now have well-established relationships with law enforcement agencies active in this arena, including the Federal Bureau of Investigation Foreign Influence Task Force and the U.S. Department of Homeland Security's Election Security Task Force."[279] Facebook has made similar representations to the Committee:

> *After the election, when the public discussion of 'fake news' rapidly accelerated, we continued to investigate and learn more about the new threat of using fake accounts to amplify divisive material and deceptively influence civic discourse. We shared what we learned with government officials and others in the tech industry. Since then, we also have been coordinating with the FBI's Counterintelligence Division and the DOJ's National Security Division. We are also actively engaged with the Department of Homeland Security, the FBI's Foreign Influence Task Force, and Secretaries of State across the US on our efforts to detect and stop information operations, including those that target elections.*[280]

(U) This progress notwithstanding, it is important to memorialize the state of information sharing between law enforcement and the social media companies in fall 2016. The FBI was examining social media content for its potential as a means of effectuating foreign influence operations in 2016, but mostly through contractors:

---

[276] **(U)** Alex Stamos, Facebook, "An Update on Information Operations on Facebook," September 6, 2017: https://newsroom.fb.com/news/2017/09/information-operations-update/.

[277] **(U)** The first publicly available insight into the IRA, however, came several years prior as a result of the efforts of a small number of diligent and prescient reporters. By 2015, Russian reporters, including Andrei Soshnikov who went undercover as a troll in the IRA in 2013, had begun to expose the inner workings of the IRA.

[278] **(U)** Shaun Walker, "Salutin' Putin: Inside a Russian troll House," *The Guardian*, April 2, 2015; Adrian Chen, "The Agency," *The New York Times Magazine*, June 2, 2015.

[279] **(U)** Sean Edgett, Letter to SSCI Chairman Richard Burr and Vice Chairman Mark Warner, January 25, 2019.

[280] **(U)** Facebook, Letter to SSCI Chairman Richard Burr and Vice Chairman Mark Warner, February 26, 2019

(U) *In October 2016, the Counterintelligence Division tasked a contractor to identify Russian influence activity on Twitter. The FBI contractor collected and analyzed a sample of Twitter activity conducted by an overtly pro-Russian network of 13 Twitter accounts and their followers, including automated accounts, which promoted US election-related news and leaked Democratic party emails published by WikiLeaks.*[281]

(U) The apparently outsourced nature of this work is troubling: it suggests FBI either lacked resources or viewed work in this vein as not warranting more institutionalized consideration. None of the resulting analysis or even notice of the underlying activity appears to have been communicated to the social media company in question prior to the election. Twitter's General Counsel told the Committee in January 2019: "To the best of our knowledge, Twitter received no information from the U.S. government in advance of the 2016 election about state sponsored information operations."[282]

(U) Facebook, however, had more robust information exchange with law enforcement in 2016: "In several instances before the 2016 U.S. election, our threat intelligence team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials, and they subsequently shared useful feedback with us."[283] Still, it was incumbent on Facebook to initiate the dialogue with law enforcement, and the exchange of information was predicated on Facebook bringing foreign influence activity directed at Americans to the attention of the FBI.

[redacted]

[redacted] Reflecting on the U.S. Government's handling of social media in the context of Russia's influence operations, former Deputy National Security Advisor for Strategic Communications Ben Rhodes commented [redacted]

[281] **(U)** FBI, Written response to SSCI inquiry of January 3, 2019, March 1, 2019.
[282] **(U)** Sean Edgett, Letter to SSCI Chairman Richard Burr and Vice Chairman Mark Warner, January 25, 2019.
[283] **(U)** Facebook, Letter to SSCI Chairman Richard Burr and Vice Chairman Mark Warner, February 26, 2019
[284] **(U[redacted])** Committee transcript of September 15, 2017 interview of [redacted] CIA.

[redacted] Commenting on the [redacted] Former Homeland Security Advisor Lisa Monaco offered a [redacted]

[redacted]

(U) Further increasing this challenge, detecting foreign influence operations on social media becomes more difficult as enabling technologies improve. In addition to the growing number of actors engaged in social media-facilitated, online manipulation efforts, the technology that aids in developing more realistic and convincing propaganda material also continues to advance.

(U) The ongoing development of artificial intelligence and improvements to false video and image "Deepfake" techniques are making it more difficult to spot fake content, manipulated videos, and forged recordings online. "Deepfakes" entail using artificial intelligence-based technology to create or alter video content so that it appears to present something that did not actually occur. Although these capabilities are relatively nascent, they are being perfected at a pace that eclipses the effort to create the technology for detecting and mitigating fraudulent media content.

(U) Advanced micro-targeting in the commercial sector is also rapidly becoming more effective. Propagandists will be able to continue to utilize increasingly advanced off-the-shelf capabilities to target specific individuals with highly targeted messaging campaigns.

---

[285] **(U)** SSCI Transcript of the Interview with Benjamin J. Rhodes, Former Deputy National Security Adviser for Strategic Communications, July 25, 2017.
[286] **(U)** *Ibid.*
[287] **(U)** SSCI transcript of the Closed Hearing on White House Awareness of and Response to Russian Active Measures, July 17, 2018.
[288] **(U)** SSCI Transcript of the Interview with John Carlin, Former Assistant Attorney General for National Security, September 25, 2017.

(U) Automation is also getting better. Bots—already advanced in sophistication relative to predecessor generations—are becoming harder and harder to detect. Researchers, including Emilio Ferrara and his team from the University of Southern California and the University of Indiana, have studied the increasing sophistication of automated accounts. Their research suggests a detection "arms race," between the purveyors of automated activity and those intent on its reliable identification, similar to the fight against the indiscriminate dissemination of commercial content to vast unsoliciting audiences, or "spam," in the past.[289]

(U) In addition, as the larger social media platforms begin to increase their detection capabilities, disinformation tactics have begun to shift to accommodate those changes. Influence operatives have begun to move away from targeting Facebook and Twitter newsfeeds, transitioning to messaging platforms like WhatsApp, Telegram, and WeChat. These direct interactions are much harder to detect and if these tactics are scaled, they could have a significant effect on target audiences.

(U) The evolution and proliferation of the core influence techniques used by the IRA could jeopardize facets of American society that have yet to be attacked by influence operatives. The same bots, trolls, click-farms, fake pages and groups, advertisements, and algorithm-gaming the IRA used to conduct an information warfare campaign can be repurposed to execute financial fraud, stock-pumping schemes, digital advertising manipulation, industrialized marketing of counterfeit prescription drugs, and scaled deceptions that spread malware.

[redacted] Facebook CEO Sheryl Sandberg testified to the Committee in 2018 that, "Our focus is on inauthenticity, so if something is inauthentic, whether it's trying to influence domestically or trying to influence on a foreign basis—and actually a lot more of the activity is domestic—we take it down."[291] But as the IRA's approach suggests, the current constructs for removing influence operation content from social media are being surpassed by foreign influence operatives, who adapt their tactics to either make their inauthenticity indiscernible, their automated propagation too rapid to control, or their operations compliant with terms of service.

(U) An October 2018 report provided to the Committee by social media analytics firm Graphika indicates that Russian disinformation efforts may be focused on gathering information and data points in support of an active measures campaign targeted at the 2020 U.S. presidential

---

[289] **(U)** Emilio Ferrara, et al., "The Rise of Social Bots," *Communications of the ACM*, July 2016, Volume 59, Number 7, 96-104, https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext#R22.

[290] [redacted]

[291] **(U)** Sheryl Sandberg, Hearing before the Senate Select Committee on Intelligence, September 5, 2018, available at https://www.intelligence.senate.gov/hearings/open.

election. The USA Really website and its affiliated social media channels, which have been linked to the IRA on the basis of technical findings, have "engaged in a number of campaigns seemingly focused on gathering personal information (emails, phone numbers, and bank details) of US-based audiences sympathetic to Russian disinformation topics."[292]

X. (U) THE COMMITTEE'S REVIEW OF RUSSIA'S USE OF SOCIAL MEDIA

(U) Throughout 2017, 2018, and 2019, in addition to its review of classified information on the topic, the Committee worked to elevate public awareness of the threat posed by Russia online, an effort that included applying pressure on social media companies to more fully examine their platforms for suspected Russian government activities.

(U) On March 30, 2017, the Committee held a public hearing for the purpose of discussing Russian malign influence efforts. The hearing, entitled "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," included testimony from a number of expert witnesses who provided insights into the mechanics of Russian influence operations and warned that Russian social media manipulation "has not stopped since the election in November and continues fomenting chaos amongst the American populace."[293] Committee Members joined witnesses in calling on social media companies to do more to uncover the Russian active measures activities occurring on their platforms. In the wake of the hearing, the Committee publicly and privately pressed social media companies to release more information about the activity of Russian actors on social media in the lead-up to the 2016 election.

(U) On April 27, 2017, Facebook released a white paper detailing an array of malicious information operations by organized actors on the Facebook social media platform.[294] Though the paper implicitly attributed the operations to Russian intelligence actors, the company had yet to uncover the substantial operational activity of the IRA.[295] Finally, in late summer 2017, Facebook notified the Committee of its findings from an internal information security investigation which uncovered 470 accounts, groups, and pages linked to the IRA.[296]

---

[292] **(U)** Graphika Strategic Assessment, *USA Really Shows a New Face of Russian Disinformation Efforts Against the US*, October 10, 2018.

[293] **(U)** Clint Watts, Written Testimony, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate.gov/hearings/open.

[294] **(U)** Jen Weedon, William Nuland, and Alex Stamos, "Information Operations and Facebook," Facebook Newsroom, April 27, 2017, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

[295] **(U)** The Facebook white paper specifically stated that Facebook was not in a position to make "definitive attribution" to the actors sponsoring this activity. However, it was willing to publicly say that the data it uncovered "does not contradict the attribution provided by the U.S. Director of National Intelligence in the report dated January 6, 2017." This is a clear reference to Russian-linked activity. Alex Stamos, one of the authors of the white paper, also made clear to SSCI staff in a briefing around that time that indicators pointed to Russian-linked intelligence activity.

[296] **(U)** Facebook briefed Committee staff on its findings on September 6, 2017, and publicized those same findings later that day.

(U) The subsequent September 2017 release of IRA-linked account information by Facebook publicly confirmed the existence of IRA-purchased advertisements. This precipitated audits at Twitter, Google, YouTube, Reddit, and other social media companies, which uncovered additional accounts and activity originating with the IRA. As more and more information became public, the wide-ranging and cross-platform nature of the attack emerged. The Committee made formal requests to multiple social media companies for any data associated with these operations, in order to better assess Russia's tactics and objectives. On the basis of negotiations with the Committee, several companies—including Facebook, Twitter, and Google—furnished varying quantities of data not previously released.

(U) Beginning with an initial delivery of metadata and content in late 2017, Facebook, Twitter, and Google provided the Committee with information relating to a number of IRA-affiliated social media accounts, including advertisements purchased in connection with those accounts, consisting of:

- Metadata and content associated with 81 Facebook Pages, including approximately 61,500 unique Facebook organic posts and 3,393 paid advertisements;
- Similar information from nearly 116,000 Instagram posts across 133 Instagram accounts;
- Metadata and content of approximately 10.4 million tweets across 3,841 Twitter accounts, as well as unique account information; and,
- Approximately 1,100 YouTube videos (43 hours of video) across 17 account channels.

(U) Each of these accounts and their associated activities were determined to be connected to the IRA by the social media companies themselves, based on the companies' internal investigations.[297] This cooperation by the social media companies secured for the Committee a significant and unique dataset on which to base further study into IRA activities. Much of the analysis in this report derives from that initial dataset.[298] The datasets provided to the Committee demonstrate the IRA's tactics and capabilities, and add depth to the public's understanding of how the IRA conducted its information warfare campaign against the United States in 2016.

(U) In order to thoroughly examine this sizeable aggregation of technical data, the Committee sought assistance from the TAG. At the Committee's request, the two TAG working

[297] **(U)** The Committee has not attempted to make an independent determination as to the accuracy of the social media companies' internal investigations or the true provenance of the accounts themselves, though the Committee does believe that the data provided is almost certainly not the entirety of the IRA's activity on these platforms. Subsequent reporting and additional research from outside analysts have corroborated much of the original attribution from the companies.

[298] **(U)** Twitter has since published its entire dataset on IRA-linked activity. On October 17, 2018, Twitter publicly released all the accounts and related content it has identified so far as associated with the activities of the IRA, dating back to 2009.

groups each conducted an independent, expert analysis of the social media company-provided dataset. Combining this dataset with the TAG's own internal research and data analytic capabilities, the TAG working groups studied U.S. social media platforms for indications of additional and undiscovered Russian foreign influence activity. Ultimately, the three TAG working group leads provided their findings and analysis to the Committee in a series of presentations that included staff briefings, a closed Member briefing, and a full Committee public hearing held on August 1, 2018.

(U) The TAG working groups each published their findings in two public reports that were released on December 17, 2018. The efforts of the TAG working groups, and the team leads specifically, resulted in two valuable publications that have significantly informed the Committee's understanding of Russia's social media-predicated attack against our democracy. The Committee supports the general findings of the TAG working groups, and notes that much of this Volume's analysis is derived from their work. The two reports are attached as addendums to this Volume.

XI. (U) RECOMMENDATIONS

(U) This challenge requires an integrated approach that brings together the public and private sectors. This approach must be rooted in protecting democratic values, including freedom of speech and the right to privacy. The Federal government, civil society, and the private sector, including social media and technology companies, each have an important role to play in deterring and defending against foreign influence operations that target the United States.

A. (U) Industry Measures

(U) The Committee recommends that social media companies work to facilitate greater information sharing between the public and private sector, and among the social companies themselves about malicious activity and platform vulnerabilities that are exploited to spread disinformation. Formalized mechanisms for collaboration that facilitate content sharing among the social media platforms in order to defend against foreign disinformation, as occurred with violent extremist content online, should be fostered. As researchers have concluded: "Many disinformation campaigns and cyber threats do not just manipulate one platform; the information moves across various platforms or a cyber-attack threatens multiple companies' network security and data integrity. There must be greater cooperation within the tech sector and between the tech sector and other stakeholders to address these issues."[299] The Committee agrees.

(U) This should not be a difficult step. Models for cooperation already exist and can be developed further:

[299] **(U)** *Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation*, Stern Center for Business and Human Rights, New York University, November 3, 2017, http://www.stern.nyu.edu/experience-stern/faculty-research/harmful-content-role-internet-platform- companies-fighting-terrorist-incitement-and-politically.

- **(U)** Google, Facebook, Twitter, and Microsoft already maintain a common database of digital fingerprints identifying violent extremist videos. These four companies also participate in a Cyberhate Problem-Solving Lab run by the Anti-Defamation League's Center for Technology and Society.

- **(U)** Dozens of tech companies participate in the Global Network Initiative, a tech policy forum devoted to protecting digital rights globally.

- **(U)** Other examples include the Global Internet Forum to Counter Terrorism, whose goal is to substantially disrupt terrorists' ability to disseminate violent extremist propaganda, and glorify real-world acts of violence; and the National Cyber Forensics and Training Alliance, a nonprofit partnership between industry, government, and academia that enables cooperation to disrupt cyber-crime.

- **(U)** Two models from the world of financial intelligence are the UK's Joint Money Laundering Intelligence Taskforce and the United States' Financial Crimes Enforcement Exchange.

(U) At the urging of the Committee, social media companies have begun to share indicators, albeit on an ad hoc basis.

(U) The Committee further recommends that social media companies provide users with:

- **(U)** Greater transparency about activity occurring on their platforms, including disclosure of automated accounts (i.e., bots);

- **(U)** Greater context for users about why they see certain content;

- **(U)** The locational origin of content; and,

- **(U)** Complete and timely public exposure of malign information operations.

(U) Social media platforms are not consistent in proactively, clearly, and conspicuously notifying users that they have been exposed to these efforts, leaving those who have been exposed to the false information or accounts without the knowledge they need to better evaluate future social media content that they encounter. Notifications to individual users should be clearly stated, device neutral, and provide users all the information necessary to understanding the malicious nature of the social media content or accounts they were exposed to.

(U) Finally, the analytic and computational capabilities of outside researchers should be put to greater use by the social media companies. Although social media companies have released some data about the manipulation of their platforms by foreign actors, the Committee recommends that social media companies be more open to facilitating third-party research

designed to assist them in defending their platforms from disinformation campaigns. The results of collaboration with outside researchers should be shared with users who have been exposed to disinformation.

B. (U) Congressional Measures

(U) The Committee recommends that Congress consider ways to facilitate productive coordination and cooperation between U.S. social media companies and the pertinent government agencies and departments, with respect to curtailing foreign influence operations that target Americans—to include examining laws that may impede that coordination and cooperation. Information sharing between the social media companies and law enforcement must improve, and in both directions. Data must be shared more quickly and in a more useful manner. This will improve the ability of social media companies to quickly identify and disclose malign foreign influence operations to the appropriate authorities, and it will improve the ability of law enforcement agencies to respond in a timely manner.

(U) Informal channels of communication may not be sufficient to accomplish this goal. As part of its examination, Congress must assess whether formalized information sharing between law enforcement and social media companies is useful and appropriate. Certain statutory models already exist, such as U.S. Code, Title 18, Section 2258A (Reporting requirements of providers). That section requires social media companies to report any apparent violations of laws relating to child sexual exploitation to the National Center for Missing and Exploited Children (NCMEC). NCMEC is a private, non-profit entity that serves a statutorily authorized clearinghouse role: it receives the providers' reports, assesses the reports for criminality and threats to children, and refers them to the appropriate law enforcement authorities for action. Formalizing a relationship between social media companies and the government does present some legal considerations,[300] but these should not be prohibitive.

(U) Further, the Committee recommends that Congress examine legislative approaches to ensuring Americans know the sources of online political advertisements. The Federal Election Campaign Act of 1971 requires political advertisements on television, radio and satellite to disclose the sponsor of the advertisement. The same requirements should apply online. This will also help to ensure that the IRA or any similarly situated actors cannot use paid advertisements for purposes of foreign interference.

(U) Finally, Congress should continue to examine the full panoply of issues surrounding social media, particularly those items that may have some impact on the ability of users to masquerade as others and provide inauthentic content. Issues such as privacy rules, identity

[300] **(U)** For example, courts have considered whether NCMEC and providers should be considered state actors and therefore subject to Constitutional requirements such as the Fourth Amendment when identifying and sharing child exploitation material with law enforcement. *See, e.g.*, *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018) (holding that provider acted in a private capacity when identifying and reporting child exploitation images to NCMEC); *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) (holding that NCMEC was a state actor when reviewing and reporting child exploitation material to law enforcement).

validation, transparency in how data is collected and used, and monitoring for inauthentic or malign content, among others, deserve continued examination. In addition, Congress should monitor the extent to which social media companies provide users with the information laid out in section A and, if necessary, take remedial steps.

C. (U) Executive Branch Measures

(U) The Committee recommends that the Executive Branch should, in the run up to the 2020 election, reinforce with the public the danger of attempted foreign interference in the 2020 election.

(U) Addressing the challenge of disinformation in the long-term will ultimately need to be tackled by an informed and discerning population of citizens who are both alert to the threat and armed with the critical thinking skills necessary to protect against malicious influence. A public initiative—propelled by federal funding but led in large part by state and local education institutions—focused on building media literacy from an early age would help build long-term resilience to foreign manipulation of our democracy. Such an effort could benefit from the resources and knowledge of private sector technology companies.

(U) Additionally, and in concert with initiatives that heighten public awareness about disinformation, media organizations should establish guidelines for using social media accounts as sources, to guard against quoting falsified accounts or state-sponsored disinformation.

(U) The Committee further recommends that the Executive Branch stand up an interagency task force to continually monitor and assess foreign country's use of social media platforms for democratic interference. The task force should periodically advise the public and Congress on its findings and issue annual reports providing recommendations to key actors, including executive branch departments and agencies, industry, and civil society. The task force should also develop a deterrence framework to inform U.S. Government responses to foreign influence efforts using social media.

(U) The Committee further recommends that the Executive Branch develop a clear plan for notifying candidates, parties, or others associated with elections when those individuals or groups have been the victim of a foreign country's use of social media platforms to interfere in an election. The plan should provide standards for deciding who to notify and when, and should clearly delineate which agencies are responsible for making the notifications and to whom.

D. (U) Other Measures

(U) The Committee recommends that candidates, campaigns, surrogates for campaigns, and other public figures engaged in political discourse on social media be judicious in scrutinizing the sources of information that they choose to share or promote online. Such public figures, precisely because of the reach of their networks, are valuable targets for adversaries, and can quickly be co-opted into inadvertently promoting a foreign influence operation.

(U) Amplification of foreign content, intentional or otherwise, is celebrated by those like the IRA, who wish to enflame our differences in order to advance their own interests. The Committee recommends that all Americans, and particularly those with a public platform, take on the responsibility of doing due diligence in their use of social media, so as to not give greater reach to those who seek to do our country harm.

(U) The Committee recommends the implementation of a Public Service Announcement (PSA) campaign, potentially by the social media industry or by government actors, that promotes informed social media behavior and raises awareness about various types of foreign influence and interference activity that is targeting American citizens, businesses, and institutions. Foreign influence campaigns that target social media users in the United States should receive similar attention to the dangers of smoking and the environmental risks of pollution. Broader exposure of specific foreign government linkages to social media content and influence activities would handicap the effectiveness of information operations.

[redacted]

XII. (U) Additional Views of Senator Wyden

(U) If American democracy is going to withstand the onslaught of foreign government influence campaigns targeting U.S. elections, our government must address the problem of targeted ads and other content tailored to consumers' demographic and political profiles. Targeted influence campaigns can weaponize personal information about Americans, not just to manipulate how, or whether they vote, but to identify and use real individuals to amplify content and influence like-minded followers. Targeted influence campaigns are far more effective and cost-efficient than blanket dissemination of propaganda. They are also more deceptive and substantially harder to identify and expose.

(U) While the Committee's description of Russia's 2016 influence campaign is deeply troubling, even more sophisticated and effective options are available to adversaries who buy, steal, or otherwise obtain information about the Americans they are seeking to influence. This threat is increased due to the availability of ad micro-targeting services offered by social media and online advertising companies, particularly those that deliver ads to specific Americans based on a list of email addresses or telephone numbers provided by an advertiser. Such ad targeting systems are highly prone to abuse when coupled with private information about Americans, which is widely available because of weak corporate data security and privacy practices, the absence of strong privacy laws, and the booming market for commercial data brokers, whose practices are largely unregulated. Each of these problems demands an effective response.

(U) The Committee report states that, in 2016, IRA operators did not take advantage of all of Facebook's targeting capabilities, including "Custom Audiences," which would have allowed the Russians to use outside data and contact information to conduct "advanced micro-targeting."[1] The danger posed by these services is magnified by the ease with which personal data can be purchased or stolen by a foreign adversary with advanced cyber capabilities. Indeed, as the Department of Justice's indictment against the IRA revealed, the IRA used stolen identities of real Americans to create accounts and post content, purchase advertising on social media sites and finance their influence activities through Pay Pal.[2]

(U) In the wake of the 2016 influence campaign by Russia, the social media companies announced transparency measures that allow the recipients of targeted ads to understand how they were selected to see the ads. However, these transparency measures only apply when the tech companies are doing the targeting on behalf of the advertiser, for example when an advertiser asks Facebook to deliver its ads to a particular age and gender demographic. The companies' ad transparency systems do not apply to services like Custom Audiences through which the platform merely serves as a messenger for ads directed according to a list of targets obtained by the malign influencer from a data broker or a hacked database. I have already publicly called on the social media platforms to voluntarily suspend the use of Custom Audiences and other micro-targeting services for political and issue ads, and I repeat that call

[1] (U) Facebook has acknowledged that the IRA used custom audiences based on user engagement with certain IRA pages. *See* Responses by Facebook to Questions for the Record from Senator Wyden from hearing on September 5, 2018, submitted October 26, 2018, p. 45.

[2] (U) Indictment, *United States of America v. Internet Research Agency et al.*, Case 1:18-cr-00032-DLF (D.D.C. February 16, 2018).

[redacted]

[redacted]

here.[3] Until Facebook, Google, and Twitter have developed effective defenses to ensure that their ad micro-targeting systems cannot be exploited by foreign governments to influence American elections, these companies must put the integrity of American democracy over their profits.

(U) At the Committee's September 5, 2018, hearing, I asked Facebook's Chief Operating Officer Sheryl Sandberg and Twitter's Chief Executive Officer Jack Dorsey whether increased protections and controls to defend personal privacy should be a national security priority. Both witnesses answered in the affirmative. Weak data privacy policies increase the ability of foreign adversaries to micro-target Americans for purposes of election interference. Facebook's total failure to prevent Cambridge Analytica and Aleksandr Kogan from obtaining sensitive personal data about Facebook users, as well as Facebook's troubling data-sharing partnerships with Chinese smart phone manufacturers, demonstrate clear gaps in federal data privacy laws and highlight obvious weaknesses that could be exploited in future influence campaigns.[4]

(U) Broad, effective data security and privacy policies, implemented across the platforms and enforced by a tough, competent government regulator, are necessary to prevent the loss of consumers' data and the abuse of that data in election influence campaigns. Congress should pass legislation that addresses this concern in three respects. First, the Federal Trade Commission must be given the power to set baseline data security and privacy rules for companies that store or share Americans' data, as well as the authority and resources to fine companies that violate those rules. Second, companies should be obligated to disclose how consumer information is collected and shared and provide consumers the names of every individual or institution with whom their data has been shared. Third, consumers must be given the ability to easily opt out of commercial data sharing.

(U) Companies that hold private information on Americans also must do far more to protect that information from hacking. That includes telecommunications companies that hold information about customers' communications, web browsing, app usage and location. Too much of this information is held for too long, increasing the risk that it will be hacked. Besides strengthening their cyber security practices, companies can take steps to delete consumer information as soon as it is not absolutely necessary for business purposes.

(U) Increased transparency is another critical priority if the United States is to defend itself against foreign election influence campaigns. A clear lesson from 2016 is that the U.S. public needs information about influence campaigns prior to the election itself. That includes information about U.S. adversaries' attempts to undermine some candidates while assisting others. In 2016, the specific intent of the Russians was not made public during the election. Intelligence related to Russian intent was not even made available to the full Committee until after the election, at which point I and other members called for its declassification. And it was not until the publication of the Intelligence Community Assessment in January 2017 that the public was finally provided this information.

---

[3] **(U)** Donie O'Sullivan, "Senator calls on Facebook and Google to ban political ad targeting," *CNN*, August 14, 2019.

[4] **(U)** *See* Responses by Facebook to Questions for the Record from Senator Wyden from hearing on September 5, 2018, submitted October 26, 2018, pp. 46-55.

[redacted]

[redacted]

[redacted][5] Between now and the 2020 election, the Intelligence Community must find ways to keep the U.S. public informed not only of individual influence operations, but the Community's assessment of the goals and intent of Russia and other foreign adversaries.

[5] [redacted] National Intelligence Council, Sense of the Community Memorandum, "[redacted]," September 13, 2019.

[redacted]