Summer 2020

Targeted Disinformation Warfare: How and Why Foreign Efforts are Effective, and Recommendations for Impactful Government Action

Ethan Guge

Targeted Disinformation Warfare: How and Why Foreign Efforts are Effective, and Recommendations for Impactful Government Action

Ethan Guge
Political Science
Iowa State University
2020

Executive Summary

Targeted disinformation campaigns are a cheap and effective way to create real harms that have a society-wide impact. This form of information warfare capitalizes on inherent features of the internet messaging platforms and the free nature of democratic societies to spread false and malicious content designed to increase discord by exacerbating existing social and political chasms, promote chaos and fear, and generate distrust toward government. A better understanding and immediate action to mitigate this problem are vital. Right now, Russia is in the process of using online disinformation to influence American democracy in the lead up to the 2020 election[1]. Additionally, Russian efforts are being employed to spread lies about the current ongoing global health emergency caused by Covid-19[2]. Even more alarming are indications that China is beginning to use these very tactics of information warfare to promote fear and panic regarding Covid-19[3].

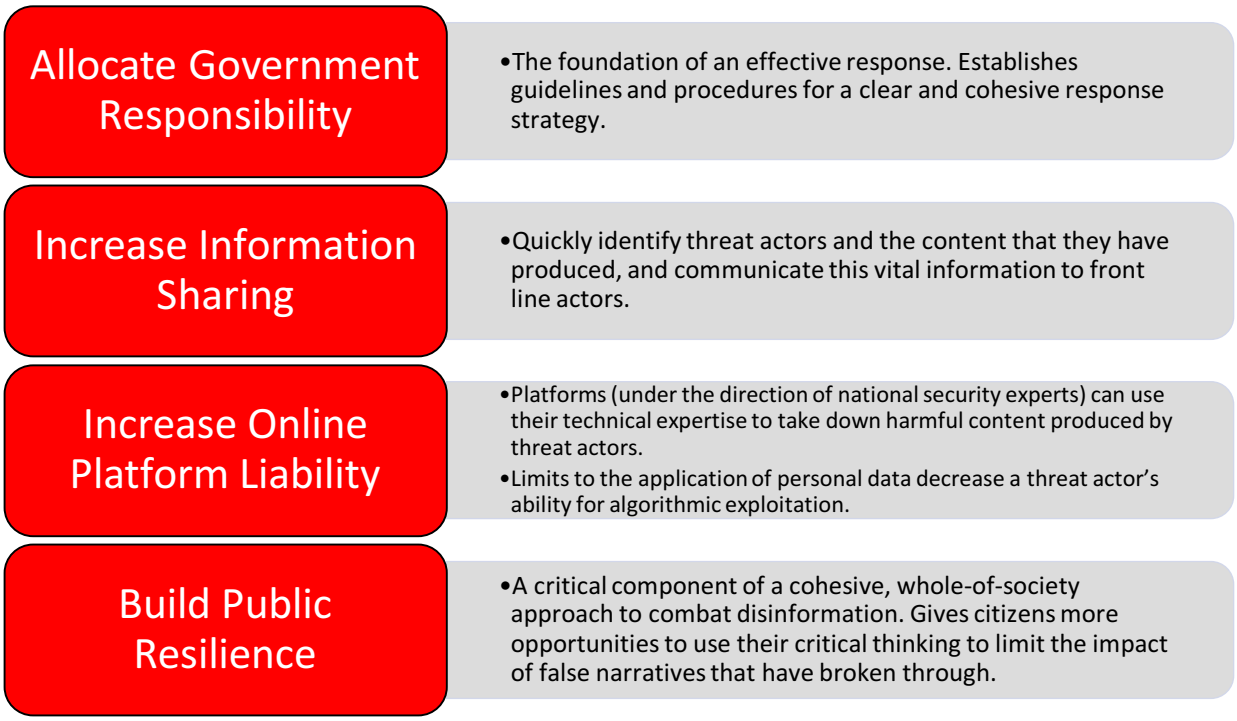
The following model illustrates the tactics used by foreign disinformation actors. Using knowledge of existing political and social fissures within a society, foreign disinformation actors target specific populations for influence. First, false and malicious content is created to appeal to these pre-determined audiences. These false narratives are then spread into the information ecosystems of societies through the manipulation of online social media platform algorithms that are designed to increase user activity and advertising revenue.

Goal: *Spread false and malicious content to exacerbate existing societal tensions, stoke negative emotions, and promote chaos, discord, and distrust.*

Create	***Push***	***Share and Discuss***	***Challenge***
Create false and malicious content to be distributed to a target audience that picks up on divisive social and political issues.	Amplify malicious content by manipulating social media platform algorithms and inflating popularity statistics through bots to increase content exposure and the appearance of legitimacy.	Interact with unwitting members of the public to promote false narratives, stoke negative emotions, and get domestic voices to spread disinformation on their own accord.	Maintain false social media accounts to interact with the public using inflammatory messaging to add chaos to the information landscape, increase anger, and distrust. Disinformation has now become a real part of everyday conversation.

[1] Rosenberg, M., Perlroth, N., & Sanger, D. E. (2020, January 10). 'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020. Retrieved from https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html
[2] Barnes, J. E., Rosenberg, M., & Wong, E. (2020, March 28). As Virus Spreads, China and Russia See Openings for Disinformation. Retrieved from https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html
[3] Wong, E., Rosenberg, M., & Barnes, J. E. (2020, April 22). Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say. Retrieved from https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html?action=click&module=Top Stories&pgtype=Homepage

Immediate government action can be taken to combat the threat of targeted online disinformation campaigns. The following response framework has four components to address each stage of the disinformation model: allocating government responsibility, increasing information-sharing capabilities, increasing online platform reliability, and building public resilience.



Introduction

The purpose of this analysis is to give a historical overview of foreign state-backed disinformation efforts, insight into modern disinformation tactics and why they are effective, and apply this analysis to a real-world scenario to inform the general public and key decision-makers while identifying potential areas of government action to combat this threat. Modern disinformation campaigns are being utilized to sow discord in the American democratic system. They creatively use social media platforms to plant and spread false narratives designed to generate chaos and distrust within a targeted environment. These tactics are low cost and have the potential for a devastating impact. Currently, this form of information warfare is being conducted by foreign state actors and is a threat that will not dissipate without effective government action. Disinformation tactics are so destructive because they use precise aspects of democratic societies to create harm, at the same time eroding the very mechanisms used to generate solutions to challenging issues.

The subsequent analysis seeks to answer two specific research questions. First, what are the tactics of modern disinformation campaigns, and why are they so effective? Second, what government action can be taken to combat the threat of targeted disinformation campaigns that effectively focuses on the specific aspects of modern disinformation efforts while being mindful of threats to civil liberties and the need for a swift, bi-partisan response? Undoubtedly, a greater

understanding of the intricacies of targeted disinformation warfare, and the highlighting of potential bi-partisan government action can lead to progress on this issue. These questions are examined through the lens of disinformation efforts supported by the Russian government. Russian backed targeted disinformation campaigns and their historical development are both well documented and pertinent to American national security. The threat posed by Russia is high. However, targeted disinformation warfare extends beyond Russia and can be utilized by a wide range of state actors that wish to harm free democratic societies.

Overview of Disinformation

What sets disinformation apart is the intention of an actor. While misinformation is the sharing of false information that is believed to be accurate, disinformation is the spread of false and inflammatory information, correct or otherwise, by an actor with the intent to mislead and cause harm[4]. The ultimate objective of modern disinformation actors is to create a disorganized and chaotic information landscape[5]. As disinformation spreads, consumers will have an increasingly difficult time distinguishing what information is real and what is not.

The consequences of targeted disinformation campaigns, also known as information warfare, are far-reaching. For example, purposefully dishonest news stories can lead to more emotional reactions among the public[6]. Disinformation efforts focus on exacerbating existing social and political cleavages within a society and thus have the potential to increase existing divisions[7]. The combination of social divisiveness, heightened emotional states, and a chaotic information landscape produced by disinformation makes instances of harassment and violence within targeted societies more likely[8]. Disinformation efforts, apart from increasing general discord within a targeted environment, also have the potential to harm personal reputations[9], financial markets[10], and public health[11] [12].

---

[4] Claire Wardle, "Information Disorder: The Essential Glossary," First Draft. Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School, July 2018, https://firstdraftnews.org/wpcontent/uploads/2018/07/infoDisorder_glossary.pdf?x19860.

[5] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," Atlantic Council, June 13, 2019, https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/.

[6] Katie Langin, "Fake News Spreads Faster than True News on Twitter—Thanks to People, Not Bots," Science, March 8, 2018, https://doi.org/10.1126/science.aat5350.

[7] Lisa Reppell and Erica Shein, "Disinformation Campaigns and Hate Speech: Exploring the Relationship and Programming Interventions," International Foundation for Electoral Systems, April 2019, https://www.ifes.org/sites/default/files/2019_ifes_disinformation_campaigns_and_hate_speech_briefing_paper.pdf.

[8] Paul Mozur, "A Genocide Incited on Facebook, With Posts From Myanmar's Military," New York Times, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

[9] Amanda Seitz, "NOT REAL NEWS: Anderson Cooper Didn't Fake Flood Broadcast," AP NEWS, September 18, 2018, https://www.apnews.com/f1b624dc8154458d8c193d3d6be341de; "2019 Brand Disinformation Impact Study," New Knowledge, January 2019, https://www.newknowledge.com/articles/2019-brand-disinformation-impact-study/.

[10] Max Fisher, "Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?," Washington Post, April 23, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tippedstock-market-by-136-billion-is-it-terrorism/.

[11] Marc Trotochaud and Matthew Watson, "Misinformation and Disinformation: An Increasingly Apparent Threat to Global Health Security," The Bifurcated Needle, Center for Health Security, John Hopkins University, November 29, 2018, http://www.bifurcatedneedle.com/new-blog/2018/11/29/misinformation-and-disinformation-an-increasingly-apparent-threat-toglobal-health-security.

[12] Emma Woollacott, "The Viral Spread Of Ebola Rumors," Forbes, October 9, 2014, https://www.forbes.com/sites/emmawoollacott/2014/10/09/the-viral-spread-of-ebola-rumors/#191c27f219d8.

Targeted disinformation threatens democratic societies in particular. Democratic societies rely upon public support to advance policy initiatives[13]. Informed, rational, and civil debate is vital to form favorable public opinion, the lifeblood of democracy[14]. In a chaotic information landscape, such as that produced by targeted disinformation, rational discussion is made more difficult, leading to a decreased ability to build a public consensus and thus limiting the ability of democratic governments to enact meaningful change. Public opinion influences every area of government operation, including foreign policy. For example, it was public opinion that ultimately led to the withdrawal of US troops from the Vietnam War, rather than actual battlefield results[15].

Background of Russian Disinformation Efforts

Governments of nation-states have always been interested in actively shaping public opinion. For instance, the British army utilized false news stories about the German military to form British public opinion during the First World War[16]. Also, Nazi Germany extensively tried to influence public opinion, of both their citizens and those of foreign countries, during the Second World War[17]. Additionally, and perhaps most pertinent to current US foreign policy, the Soviet Union utilized disinformation through tactics termed "active measures" against the west during the Cold War[18].

The Soviet strategy of active measures, which sought to control and influence the press and public opinion in pre-determined foreign countries, has long been a critical component of Russian foreign policy[19]. Efforts to spread disinformation have become a vital component following the collapse of the Soviet Union. Information warfare that utilizes targeted disinformation allows Russia to exert influence despite its reduced economic and military capabilities. Active measures were regarded as an "equalizer," making up for hard-power weaknesses in comparison to western states[20].

During the Cold War, active measures were central to Soviet intelligence operations. These tactics of subversion were designed to weaken western democracies, drive wedges within

---

[13] Cheryl Boudreau and Scott A. Mackenzie, "Wanting What Is Fair: How Party Cues and Information about Income Inequality Affect Public Support for Taxes," The Journal of Politics 80, no. 2 (2018): 367–81, https://doi.org/10.1086/694784.

[14] Eggers, W.D., & O'Leary, J. (2009). *If we can put a man on the moon….: Getting big things done in government (Chapter 3).* Boston, MA: Harvard Business Press. ISBN 1422166368.

[15] W.L. Lunch and P. W. Sperlich, "American Public Opinion and the War in Vietnam," Political Research Quarterly 32, no. 1 (January 1979): 21–44, https://doi.org/10.1177/106591297903200104; William M. Darley, "War Policy, Public Support, and the Media," The US Army War College Quarterly: Parameters, 2005, 121–34, https://ssi.armywarcollege.edu/pubs/parameters/articles/05summer/darley.pdf.

[16] Roy Greenslade, "First World War: How State and Press Kept Truth Off the Front Page," The Guardian, July 27, 2014, https://www.theguardian.com/media/2014/jul/27/first-world-war-state-press-reporting.

[17] Nicholas O'Shaughnessy, "The Nazis' Propaganda Trick: Invite the Public to Help Create an Alternate Reality," Slate, March 14, 2017, https://slate.com/news-and-politics/2017/03/how-nazi-propaganda-encouraged-the-masses-to-co-produce-a-falsereality.html.

[18] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference (Strategic Perspectives, No. 11)," Strategic Perspectives, June 2012, https://doi.org/10.21236/ada577586.

[19] Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections*, *15*(1), 5-31.

[20] DISINFORMATION: A PRIMER IN RUSSIAN ACTIVE MEASURES AND INFLUENCE CAMPAIGNS. HEARING BEFORE THE SELECT COMMITTEE ON INTELLIGENCE OF THE UNITED STATES SENATE ONE HUNDRED FIFTEENTH CONGRESS FIRST SESSION. (2017, March 30). Retrieved from https://www.govinfo.gov/content/pkg/CHRG-115shrg25362/html/CHRG-115shrg25362.htm

domestic populations, and sow discord among western alliances[21]. Russian active measures, first utilized in World War I and continued throughout World War II and the Cold War, were used specifically to target western liberal democracies and the NATO alliance[22]. The manipulation of information environments was considered a cheap and effective strategy to harm western rivals and one that traditional military alliances had trouble defending[23].

Russian active measures have long been employed against the United States. One of the best-known instances was the spread of disinformation about the AIDS epidemic in the US during the Cold War. False and conspiratorial news stories claiming that the US government manufactured and was responsible for the AIDS virus, ultimately spread their way into mainstream news coverage[24]. It is estimated that 10,000 different disinformation operations, involving 15,000 operatives, were carried out by the Soviet Union during the Cold War[25] [26]**.** Although the Cold War has ended, Russian active measures have not, and have given Russia a platform to further their foreign policy goals as western countermeasures have subsided[27].

Aspects of Modern Russian Disinformation Efforts

As times have changed, the theme of targeted disinformation campaigns has not. During the Cold War, Russian disinformation efforts continue to sow discord through the use of issues that elicit fear, such as nuclear war, environmental catastrophe, and the collapse of the world economy[28]. This strategy relies on mass hysteria as its main motivational force, playing on the hopes and fears of those living in western liberal democracies[29]. Currently, this strategy is being used to undermine western democracies to further Russia's foreign policy goals, such as the dissolution of NATO and the EU, as well as disrupt free and fair democratic elections, most notably in Germany, France, and the United States[30].

Current disinformation efforts aim to attack western liberal societies through citizens' relationships with their democratic institutions[31]. The main goal is for the information environment in democratic societies to be too confusing for ordinary consumers to accurately

---

[21] O1eg Kalugin, "Inside the KGB: An interview with retired KGB Maj. Gen. Oleg Kalugin," CNN, January J998.
[22] Roy Godson, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.govinfo.gov/content/pkg/CHRG-115shrg25362/html/CHRG-115shrg25362.htm
[23] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[24] Christopher M. Andrew and Vasili Mitrokhin, The Sword and the Shield: The Mitrokhin Archive & the Secret History of the KGB, Basic Booksi 1985, p. 244.
[25] Thomas Rid, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.intelligence.senate~gov/hearings/open.
[26] Dr. Roy Godson, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.govinfo.gov/content/pkg/CHRG-115shrg25362/html/CHRG-115shrg25362.htm
[27] Dr. Roy Godson, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.govinfo.gov/content/pkg/CHRG-115shrg25362/html/CHRG-115shrg25362.htm
[28] Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections*, *15*(1), 5-31.
[29] Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections*, *15*(1), 5-31.
[30] Dr. Eugene Rumer, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.govinfo.gov/content/pkg/CHRG-115shrg25362/html/CHRG-115shrg25362.htm
[31] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

identify the truth of an issue[32]. This strategy looks not to directly convince or persuade, instead to distract and confuse, to increase distrust toward traditional media outlets and democratic institutions[33].

As with disinformation strategies employed during the Cold War, efforts are unconstrained by a particular ideology or viewpoint[34]. Throughout the world, disinformation efforts to exacerbate divides and create echo chambers of support favorable to Russian foreign policy positions are in effect. For instance, this strategy has been employed following the downing of Malaysian Airlines Flight 17 in Ukraine, chemical attacks in Syria, and the poisoning of intelligence operatives in England, all efforts utilizing both far-left and far-right messaging[35].

From Russia's perspective, the world has entered a second Cold War period that is being fought through the manipulation of information. Rather than create new divisions within a society, Russian active measures look to exploit ones that already exist with the hope of exacerbating existing weaknesses, increasing polarization, and overall increasing vulnerability[36]. According to experts on the information warfare frontlines, there are multiple long-term goals of modern Russian disinformation efforts[37]. These goals are to undermine citizen confidence and erode trust in democratic institutions, exacerbate divisive political fissures, popularize Russian foreign policy agendas, and create general distrust, confusion, and chaos – ultimately blurring the lines between fiction and reality.

Use of Social Media

Before the internet, Russian active measures sought to produce and spread disinformation through more traditional means. Early efforts were often carried out by individual actors on the ground, bringing with them higher risks and time inefficiencies[38]. However, targeted disinformation tactics have been updated by the introduction of the internet and social media. Russia has utilized the internet, in particular social media platforms, to effectively wage information warfare. Online social media platforms provide Russia with cheap, efficient, and effective access to foreign audiences while being able to deny any official involvement in a believable manner[39].

---

[32] Joby Warrick and Anton Troianovski, "Agents of doubt," Washington Post, December 10, 2018.
[33] Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," Institut~ of Modern Russia, 2014, https://imrussia.org/media/pdf/Research/Michael_ Weiss_ and _Peter_Pomerantsev _The_ Menace_ of_ Unreality.pdf.
[34] Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money," Institut~ of Modern Russia, 2014, https://imrussia.org/media/pdf/Research/Michael_ Weiss_ and _Peter_Pomerantsev _The_ Menace_ of_ Unreality.pdf.
[35] 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/pdli'information _manipulation_ rvb _ cle83 8736.pdf.
[36] Thomas Rid, Hearing before the Senate Select Committee. on Intelligence, March 30, 2017, available at https:1/www.intelligence.senate.gov/hearings/open.
[37] Clint Watts, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.govinfo.gov/content/pkg/CHRG-115shrg25362/html/CHRG-115shrg25362.htm
[38] Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections*, *15*(1), 5-31.
[39] Clint Watts, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://viww.intelligence.senate.gov/hearings/open.

Russian online efforts began domestically in the mid-2000s to suppress political opposition and have since turned toward western liberal democracies[40]**.** The impact of disinformation disseminated through social media platforms on democratic systems, especially ones with existing social divisions, is the main threat posed by disinformation campaigns[41]. Russia has become adept at identifying and influencing democratic elections, in particular, choosing close political contests where slight influences and stoking of existing tensions can have the most significant impact. For instance, in the 2016 US presidential campaign, alt-right audiences angry about immigration, automation, and economic hardship were prominently targeted for influence through social media[42].

The ability for Russian active measures to utilize social media platforms to spread false and damaging narratives has come with the rise of public internet use. The growth of public reliance on the internet and social media to obtain information has been steep, and will only continue. Following an explosion of interconnectivity, Wi-Fi, and smartphone use, social media platforms have become a primary source for news gathering around the world[43]. In general, younger people are relying less on television and more on social media for information and newsgathering. Currently, the evidence suggests that 68% of Americans get news from social media sources, and 43% of Americans get news directly from Facebook[44] [45]. Further, less than 38% relied on print media for news[46].

The capacity for users to share information online easily and quickly without the need to verify accuracy makes these platforms especially susceptible to targeted disinformation campaigns[47] [48]. As a result, 23% of Americans have inadvertently shared fake news online[49]. The inherent mechanisms of the internet provide disinformation actors with a great advantage. Tools such as account anonymity, unlimited audience access, low cost, and plausible deniability make targeted disinformation efforts exceedingly efficient and effective[50].

According to disinformation experts within the US intelligence community, social media

---

[40] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," CNA Analysis and Solutions, Occasional Paper Series, March 2017.
[41] Clint Watts, Hearing before the Senate Select Committee on Intelligence, March 30, 2017, available at https://www.govinfo.gov/content/pkg/CHRG-115shrg25362/html/CHRG-115shrg25362.htm
[42] Weisburd, A., Watts, C., & Berger, J. M. (2016). Trolling for Trump: How Russia is trying to destroy our democracy. *War on the Rocks*, *6*.
[43] "The Mobile Economy 2018," GSM Association, 2018, https://www.gsma.com/mobileeconomy/wpcontent/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf.
[44] "News Use Across Social Media Platforms 2018," Pew Research Center, September 12, 2018, https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/.
[45] A.W. Geiger, "Key Findings about the Online News Landscape in America," Pew Research Center, September 11, 2019, https://www.pewresearch.org/fact-tank/2019/09/11/key-findings-about-the-online-news-landscape-in-america/.
[46] Elisa Shearer, "Social Media Outpaces Print Newspapers in the U.S. as a News Source," Pew Research Center, December 10, 2018, https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/.
[47] Paul Oliver, "The State of Disinformation on Social Media," NYU Center for Data Science, April 23, 2018, https://medium.com/center-for-data-science/the-state-of-disinformation-on-social-media-397d3c30f56a.
[48] Mike Wood, "How Does Misinformation Spread Online?," *Psychology Today*, December 6, 2018, https://www.psychologytoday.com/us/blog/web-mistrust/201812/how-does-misinformation-spread-online.
[49] Denise-Marie Ordway, "Fake News and the Spread of Misinformation," Journalist's Resource, September 1, 2017, https://journalistsresource.org/studies/society/internet/fake-news-conspiracy-theories-journalism-research/.
[50] Weisburd, A., Watts, C., & Berger, J. M. (2016). Trolling for Trump: How Russia is trying to destroy our democracy. *War on the Rocks*, *6*.

increases the power of disinformation efforts in five key ways[51]. First, the insight into relationships and interests that social media provides, given the high number of individuals who place their data there, allow disinformation actors to target a particular audience efficiently and accurately. Second, online platforms provide the ability to create accounts anonymously, giving a place to effectively host content that can reach millions of people and the ability for official government actors to deny any involvement. Then, online platform algorithms can be manipulated through statistical inflation, mainly through the use of bots and strategically placed human-operated accounts, increasing the chances of disinformation being spread by innocent bystanders and seeping into the general public conversation.

If It Trends, It Becomes True

The revenue model of online platforms produces specific mechanisms that foreign disinformation actors can exploit. The issue of targeted disinformation campaigns is not a truth of information problem. Instead, it is a system manipulation problem[52]. Social media platforms offer uncensored communication channels that do not require an intermediary between creators and consumers[53]. The ease with which individuals can communicate provides an excellent outlet for free-speech. However, nefarious and insidious actors looking to cause damage can take advantage also.

There is a trade-off for the low barrier of entry. In exchange for free access, platform owners can freely gather user data, enabling advertisers and platforms to share content with specific users that conforms to their determined interests, sparing consumers from seeing content that they are not passionate about. Online platforms use customer data to study behavior to learn how to maximize a user's time spent online, increasing the effectiveness of targeted advertising and overall revenue generation[54].

Modern disinformation warfare is computationally driven and enhanced by the revenue models of online social media platforms. Platforms gain revenue from attention, such as clicks and shares, and have become experts at utilizing the attention of users. Platforms employ algorithms to show content to users for which they express a predisposition. This mechanism is a tool for propagandists. A piece of content, authentic or otherwise, can reach and influence a broad audience if it gains enough momentum through online platform algorithms. In other words, once something has trended, it can become real[55].

---

[51] Clint Watts, Statement Prepared for the U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism: "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions.", October 31, 2017. Retrieved from https://www.judiciary.senate.gov/imo/media/doc/10-31-17 Watts Testimony.pdf

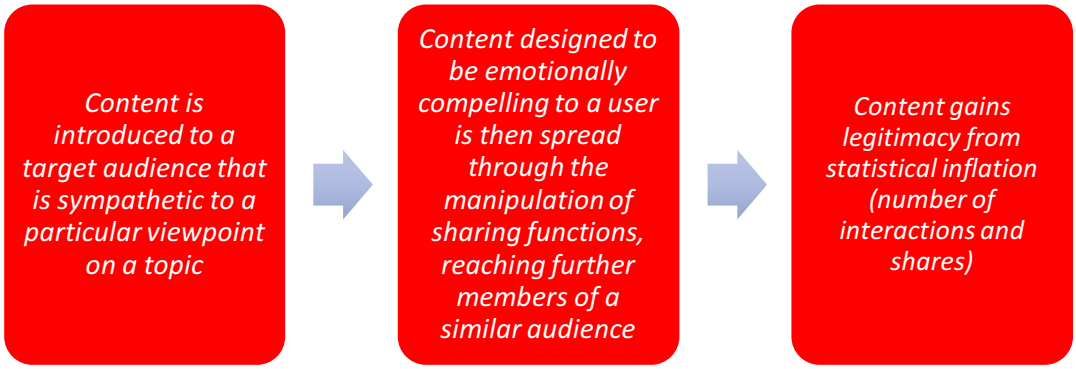
[52] Renee Diresta, Statement for the record from Renee DiResta, Director of Research, New Knowledge, October 1, 2018. Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/os-rdiresta-080118.pdf

[53] "Indicators of News Media," Gallup, Inc., 2018, https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/216/original/KnightFoundation_Panel4_Trust_Indicators_FINAL.pdf.

[54] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf

[55] Renée DiResta, "Computational Propaganda: If You Make It Trend, You Make It True," *The Yale Review*, October 12, 2018, https://yalereview.yale.edu/computational-propaganda.

Once a piece of content is trending, it gains legitimacy, especially in the eyes of sympathetic users. This process means that disinformation actors must simply amplify a false narrative to earn a certain amount of momentum and popularity to give it the appearance of truth, and thus influence over a target audience[56]. Online platforms have an incentive to utilize user data in this manner and display content that conforms to personal interests, increasing the revenue generated by selling online advertisements[57]. Here, the more alluring the content, the longer the time spent on a platform, and the higher the potential profit[58].



Within the scientific literature, two particular aspects inherent to online and social media platforms exacerbate the impact of disinformation efforts. The echo chamber phenomenon and homophilous sorting. First, online echo chambers are formed where users become more likely to see and interact with content that agrees with their worldview. Online platforms feed users what they want to know, not necessarily what they ought to know[59]. Platform search algorithms provide results tied to prior behavior, meaning content viewed will likely conform to a user's pre-existing biases, seeming more credible than content that does not[60]. Credibility is gained, especially with emotionally compelling information, as the emotional appeal of information will connect a user more strongly and outweigh one's interest in trustworthiness[61].

Second, going hand in hand with the formation of echo chambers is homophilous sorting. Homophilous sorting is the propensity of individuals who share the same perspective to form close-minded groups with one another[62]. The internet and social media have been shown to

---

[56] Renee Diresta. Statement for the record from Renee DiResta, Director of Research, New Knowledge, October 1, 2018. Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/os-rdiresta-080118.pdf
[57] Allcott Hunt and Matthew Gentzkow, "Social media and fake news in the 2016 election," *Journal of Economic Perspectives,* vol. 31, no. 2. 2017, pp. 1–28, https://web.stanford.edu/~gentzkow/research/fakenews.pdf.
[58] Tim Hwang, "Digital Disinformation: A Primer," Atlantic Council, September 2017, https://www.atlanticcouncil.org/wp-content/uploads/2017/09/Digital_Disinformation_Primer_web_0925.pdf.
[59] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf
[60] Denise-Marie Ordway, "What Research Says about How Bad Information Spreads Online," Journalist's Resource, July 19, 2018, https://journalistsresource.org/studies/society/news-media/fake-news-bad-information-online-research/.
[61] Joe Andrews, "Fake News Is Real - A.I. Is Going to Make It Much Worse," CNBC, July 12, 2019, https://www.cnbc.com/2019/07/12/fake-news-is-real-ai-is-going-to-make-it-much-worse.html
[62] McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. Annual review of sociology, 27(1), 415-444.

encourage the grouping together of like-minded individuals[63] [64] [65]. Search functions and online platform algorithms show users content that reinforces their previously held beliefs based on their history[66]. Homophilous sorting creates niches on online platforms where individuals become less likely to be exposed to information that challenges their perspectives[67]. As biases and prejudices are endlessly reinforced through personalized news feeds, individuals hear only their own opinion and have the ability to restrict themselves to only their point of view[68]. Due to these mechanisms of online platforms, ideological boundaries are rarely crossed. For instance, those who discuss political issues with others who share their perspective are more likely to end up in more extreme ideological positions[69].

Wired for Manipulation

The mechanisms of online communication platforms do not merge well with the human brain. In an already muddied and overwhelming information ecosystem, particular facts of how the human brain operates highlight just how vulnerable targeted populations are to information warfare. Individual concepts can illustrate how rational decision-making falters in the face of overwhelming amounts of information. The first concept is the majority illusion.

A majority illusion is created as a result of computational propaganda[70]. Here, particular members within a social network can give the appearance that an idea, opinion, or product is more popular than it is [71]. The more a piece of content is inflated statistically through the exploitation of social media algorithms, the more likely real people are to believe its credibility. In other words, the more attention something has, the more it has trended, the more truthful it looks to the human brain. When the information landscape is muddied, and the truth is indistinguishable from fiction in many areas, individuals resort to trusting information that supports their personal biases and preferences, especially the higher its popularity[72].

The second concept aiding disinformation actors is the vast array of confirmation biases that exacerbate the echo chamber phenomenon[73]. Confirmation bias is where individuals give unequal attention and weight to information that supports their position. As a result, individuals seek and interpret evidence in ways that are partial to existing beliefs. Personalized news feeds

---

[63] Adamic, L. A., & Glance, N. (2005, August). The political blogosphere and the 2004 US election: divided they blog. In Proceedings of the 3rd international workshop on Link discovery (pp. 36-43). ACM.
[64] Hargittai, E., Gallo, J., & Kane, M. (2008). Cross-ideological discussions among conservative and liberal bloggers. Public Choice, 134(1-2), 67-86.
[65] Conover, M. D., Ratkiewicz, J., Francisco, M., Gonçalves, B., Menczer, F., & Flammini, A. (2011, July). Political polarization on twitter. In Fifth international AAAI conference on weblogs and social media.
[66] Farrell, H. (2012). The consequences of the internet for politics. Annual review of political science, 15.
[67] Baum, M. A. (2011). Red state, blue state, flu state: Media self-selection and partisan gaps in swine flu vaccinations. *Journal of health politics, policy and law*, *36*(6), 1021-1059.
[68] *Sunstein, C. R. (2018). # Republic: Divided democracy in the age of social media. Chapter One. Princeton University Press.*
[69] *Van Alstyne, M., & Brynjolfsson, E. (2005). Global village or cyber-Balkans? Modeling and measuring the integration of electronic communities. Management Science, 51(6), 851–868. doi:10.2307/20110380.*
[70] Weisburd, A., Watts, C., & Berger, J. M. (2016). Trolling for Trump: How Russia is trying to destroy our democracy. *War on the Rocks*, *6*.
[71] Lerman, K., Yan, X., & Wu, X. Z. (2016). The" majority illusion" in social networks. *PloS one*, *11*(2).
[72] Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation*. Project on Computational Propaganda.
[73] Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. Review of General Psychology, 2(2), 175–220. doi:10.1037/1089-2680.2.2.175.

give aid to these unconscious forces and only increase one's selectiveness. Further, motivated skepticism is a concept which states that individuals tend to end up with more extreme positions after seeking out dissimilar information[74]. This effect causes individuals to evaluate similar arguments to their own higher than ones that are not. As with confirmation biases, social media algorithms exacerbate this concept by actively presenting users with arguments corresponding to their point of view. In the case of disinformation, as targeted individuals receive false narratives through the exploitation of online algorithms, this information can solidify incendiary ideological positions, decreasing civility as a result and causing overall harm to a democratic society.

Prior beliefs significantly impact individuals' evaluation of evidence, and humans will take advantage of opportunities to be selective. Humans are wired to limit their exposure to situations in which personal views may be threatened, and are more likely to select the information that conforms to their previously held social goals and beliefs[75]. For example, individuals are more likely to remember and believe the first sources of information they receive on a divisive topic[76]. Due to how crucial first impressions are to the recall and internalization of information, disinformation actors can quickly introduce and amplify narrative-shaping content on sensational issues to powerful effect.

Predispositions account for a large portion of individuals' overall information consumption[77]. For instance, individual preferences for newspaper content are related to one's sex, race, and level of education[78]. These preferences have also been shown regarding the selection of online news topics[79]. Additional research has demonstrated that individuals are more willing to choose online news outlets and news stories that run parallel to their ideological leanings[80] [81].

Further, an underlying factor is that emotions, rather than rationality, hold influence on human day-to-day decision making[82]. The fact that emotionality is more pervasive than rationality is evident from recent studies that examined voter allegiances in the 2016 US electoral campaign[83]. These studies provide support for the fact that it takes far more than mere facts and logic to change someone's mind. This difficulty is due to a tension in the brain between responding to new information and resisting overwhelming amounts of conflicting data[84]. The pressure here is

---

[74] Taber, C. S., & Lodge, M. (2006). Motivated skepticism in the evaluation of political beliefs. American Journal of Political Science, 50(3), 755–769. doi:10.1111/j.1540-5907.2006. 00214.x.

[75] Tewksbury, D., & Riles, J. M. (2015). Polarization as a Function of Citizen Predispositions and Exposure to News on the Internet. *Journal of Broadcasting & Electronic Media*, *59*(3), 381-398.

[76] Christopher Paul and Miriam Matthews, "The Russian 'Firehose ofFalsehood,' Propaganda Model," *RAND Corporation,* 2016, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

[77] Katz, E., Blumler, J. G., & Gurevitch, M. (1974). Utilization of mass communication by the individual. In J. G. Blumler & E. Katz (Eds.), The uses of mass communication: Current perspectives on gratifications research (pp. 19–32). Beverly Hills, CA: Sage.

[78] Bogart, L. (1989). *Press and public: Who reads what, when, where, and why in American newspapers*. Psychology Press.

[79] Dutta-Bergman, M. J. (2004). Complementarity in consumption of news types across traditional and new media. *Journal of Broadcasting & Electronic Media*, *48*(1), 41-60.

[80] Lyengar, S., & Hahn, K. S. (2009). Red media, blue media: Evidence of ideological selectivity in media use. Journal of Communication, 59, 19–39. doi:10.1111/j.1460-2466.2008.01402.x

[81] Knobloch-Westerwick, S., & Meng, J. (2009). Looking the other way: Selective exposure to attitude-consistent and counterattitudinal political information. Communication Research, 36, 426–448. doi:10.1177/0093650209333030

[82] Al-Rodhan, N. (2013). The Future of International Relations: A Symbiotic Realism Theory.

[83] Jacewicz, N. (2016, May 3). Why Trump and Clinton Voters Won't Switch: It's in Their Brains. Retrieved from https://www.scientificamerican.com/article/why-trump-and-clinton-voters-won-t-switch-it-s-in-their-brains/

[84] Fineberg, S. K., & Corlett, P. R. (2016). The doxastic shear pin: delusions as errors of learning and memory. *Cognitive neuropsychiatry*, *21*(1), 73-89.

enough to prevent opinion change altogether in the event of information overload. The internet and social media are home to overwhelming amounts of opinions and information, leading to information overload, only heightening this neurological phenomenon.

Additional evidence suggests that decision making regarding opinion change takes place in the self-reference section of the brain[85]. More specifically, opinion formation occurs through the construction of personal narratives that persist in the face of conflicting information. Paying attention to details that one would typically ignore floods the brain with contradictory information, and delusions are the brain's adaptation to facing this uncertainty. Misconceptions of this manner are primarily a survival mechanism[86]. In life-threatening situations, decisions need to be made quickly in the face of overwhelming amounts of conflicting data. Therefore, there is a trade-off between accuracy and speed in the brain.

Humans make decisions based on constructed narratives of self-reference. Once a decision has been made, the brain plays catch-up. Further evidence has supported the idea that decisions are prepared before the brain has fully processed all information[87]. This evidence is supported further regarding opinions held on issues ties to community values, such as abortion and gun rights[88]. Individuals tend to moderate their views on these issues as they are forced to explain the mechanisms behind their position. However, this does not hold for community value-based issues. Instead, opinion change for these issues hinges on one-to-one in-person conversations that help individuals relate to the group in question[89].

False narratives strategically spread and then amplified through social media can have an immense and destructive impact as a result. Foreign actors can utilize sensitive issues, such as race-relations or other issues tied to community values like abortion and gun rights, to spread disinformation effectively. Once false narratives successfully gather momentum, they will influence and drive individuals within particular communities toward harmful conclusions based on incorrect information that drives fear, anger, and discontent, weakening society and increasing polarization and distrust as a result.

Model of Targeted Disinformation

Foreign actors using modern disinformation tactics utilize a particular model to accomplish their foreign policy goals and produce chaos by spreading incendiary and false narratives within a target audience. These efforts look to first effectively create disinformation suitable for a particular target audience. Actors then use content amplification techniques through online social media platform algorithms to ensure a direct impact on an unwitting target audience. Specifically, intelligence experts at the center of combatting foreign targeted disinformation

---

[85] Izuma, K. (2013). The neural basis of social influence and attitude change. *Current opinion in neurobiology*, *23*(3), 456-462.
[86] Fineberg, S. K., & Corlett, P. R. (2016). The doxastic shear pin: delusions as errors of learning and memory. *Cognitive neuropsychiatry*, *21*(1), 73-89.
[87] Van Den Berg, R., Anandalingam, K., Zylberberg, A., Kiani, R., Shadlen, M. N., & Wolpert, D. M. (2016). A common mechanism underlies changes of mind about decisions and confidence. *Elife*, *5*, e12192.
[88] Fernbach, P. M., Rogers, T., Fox, C. R., & Sloman, S. A. (2013). Political extremism is supported by an illusion of understanding. *Psychological science*, *24*(6), 939-946.
[89] Broockman, D., & Kalla, J. (2016). Durably reducing transphobia: A field experiment on door-to-door canvassing. *Science*, *352*(6282), 220-224.

warfare have highlighted five steps that threat actors use: create, push, share, discuss, and challenge[90].

Create

Foreign disinformation actors create content to target specific audiences, picking up on already divisive themes[91]. An actor will first seek to analyze the target audience, determine how information flows through the target environment, and identify which societal fissures to exploit[92]. In this first stage, Russian disinformation efforts, in particular, use a blend of overt and covert operations. First, hacking and obtaining sensitive data that highlights relevant characteristics of a target audience, followed by spreading false narratives through the use of captured user data, often initially through state-funded online media sources[93].

The messaging topics of created content can be political, financial, or social. Social messages promote fear of global calamity and the collapse of the western liberal order, while political messages are designed to undermine political leaders and institutions[94]. Financial messages look to weaken confidence and trust in the free market[95]. Social messages are particularly dangerous because they pick up on divisive social issues easily gathered through user data on online social media platforms. This messaging looks to exacerbate social tensions and undermine the social fabric of society by promoting fear, discord, and distrust in the status quo[96].

After false and misleading content is created, a campaign is launched to deliver content to initial seeding locations such as online forums or social media platforms[97]. Delivery to these sources sets the stage, creating the illusion that there are multiple sources for a particular story. Written articles, blog posts, and social media posts are created as references, adding momentum to previously concocted false news stories. Here, operatives are performing what is known as

---

[90] Clint Watts, Hearing before the Senate Armed Services Committee, April 27, 2017, available at https://www.fj:Jri.org/wp-content/uploads/2017/04/Watts-Testimony-Senate-Arrried-Services-email-distro-Final.pdf.
[91] Clint Watts, Hearing before the Senate Armed Services Committee, April 27, 2017, available at https://www.fj:Jri.org/wp-content/uploads/2017/04/Watts-Testimony-Senate-Arrried-Services-email-distro-Final.pdf.
[92] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf
[93] Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *The New York Times Magazine,* September 13, 2017.
[94] Richard Gooding, "The Trashing of John McCain," *Vanity Fair*, September 24, 2008, https://www.vanityfair.com/news/2004/11/mccain200411; Jennifer Steinhauer, "Confronting Ghosts of 2000 in South Carolina," *New York Times*, October 19, 2007, https://www.nytimes.com/2007/10/19/us/politics/19mccain.html.
[95] A.J. Perez, "Bogus Nike Coupon featuring Colin Kaepernick offers discount to 'people of color,'" *USA Today*, September 13, 2018, https://www.usatoday.com/story/sports/nfl/2018/09/13/fake-nike-colin-kaepernick-coupon-offers-discount-people-color/1294875002/.
[96] William Broad, "Your 5G Phone Won't Hurt You But Russia Wants You to Think Otherwise," *New York Times*, May 12, 2019, https://www.nytimes.com › science › 5g-phone-safety-health-russia/.; https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html
[97] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf

"information laundering," or adding legitimacy to disinformation by discussing it, ultimately laying the groundwork for further spread and amplification[98].

Push

The second step is to amplify created content that supports false narratives. The manipulation of online social media platforms sharing functions and revenue generation algorithms pushes disinformation into mainstream conversations[99]. Strategic online social media accounts and "bots" work to amplify the number of views a piece of content receives. The idea is to earn the attention of a significant number of unwitting members of a target audience, and even members of the mainstream media[100].

Automated accounts, or "bots," are an essential aspect of pushing disinformation into the communication channels of a target audience. Bots are computer algorithms designed to execute specific online tasks autonomously and repetitively. By simulating the behavior of human actors in social networks, they can believably and strategically interact with others and share information on social media[101]. These social media automated accounts allow disinformation actors to easily amplify and spread content, creating the illusion of popularity, and thus add to its legitimacy. Altogether, 190 million automated accounts on social media platforms existed to amplify disinformation leading up to the 2016 US presidential election, more than half the population of the United States[102]. Overall, it is estimated that 45 percent of Russia's current activity on Twitter is through mostly automated accounts[103].

Modern foreign-backed disinformation efforts utilize every popular social media platform, such as Instagram, Reddit, YouTube, Tumblr, 4chan, and Pinterest[104]. Disinformation operatives use social media to spread disinformation and operate under two main principles: high volume and multiple channels. Threat actors use a wide variety of online methods to create a "fire hose of falsehood" through the sheer volume of false content spread to targeted audiences through a wide variety of channels[105]. High volume and repetition of disinformation messaging on a wide range of platforms flood the information landscape to overwhelm a target audience[106].

---

[98] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf

[99] Clint Watts, Hearing before the Senate Armed Services Committee, April 27, 2017, available at https://www.fj:Jri.org/wp-content/uploads/2017/04/Watts-Testimony-Senate-Arrried-Services-email-distro-Final.pdf.

[100] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf

[101] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019. https://www.cits.ucsb.edu/fake-news/spread.

[102] "How Is Fake News Spread? Bots, People like You, Trolls, and Microtargeting," Center for Information Technology and Society, U.C. Santa Barbara, accessed September 17, 2019. https://www.cits.ucsb.edu/fake-news/spread.

[103] 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.

[104] Laura Rosenberger, Written Testimony, Hearing before the Senate Select Committee on Intelligence, August l, 2018, available at https://\vww.intelligence.senate.gov/hearings/open.

[105] Christopher Paul and Miriam Matthews, "The Russian 'Firehose ofFalsehood,' Propaganda Model," *RAND Corporation,* 2016, https://www.rand.org/content/dam/rand/pubs/perspectives/PEl00/PE198/RAND_PE198.pdf

[106] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Additionally, speed is vital to modern disinformation efforts. Due to the importance of first impressions on the human mind, the rate of spread can have a significant effect on the influence of misleading content that discusses a sensitive, community-value based issue. Also, the sooner that false information seeps into a target audience, the more influential it becomes, and the more difficult it is to debunk given the slow decision-making apparatuses in western liberal democracies[107]. For instance, Russian active measures were being employed within hours of the downing of Malaysian Airlines Flight 17 over Ukraine, spreading conspiracy theories and false narrative surrounding the downing of the plane to benefit Russian interests[108].

Share and Discuss

As purposefully false information is pushed into the information ecosystem of a targeted audience, false narratives are further spread by domestic voices, adding to the illusion that a false narrative is legitimate. Individuals sympathetic to the interests of foreign actors, and covert social media accounts operated by foreign operatives discuss and share malicious content to make unwitting Americans feel as though improbable information is part of a legitimate conversation[109]. Here, there is a substantial reliance on "useful idiots" or unwitting Americans who pick up on and discuss false narratives[110]. Unwitting agents, such as useful idiots, are perceived to be sympathetic to an actor's cause but do not comprehend the objectives of their campaign. These innocent bystanders ultimately spread disinformation without knowing they are actively participating in information warfare[111]. Also, foreign operative-controlled online accounts will look to share incorrect information with key public figures in the online information space. These vital public figures will sympathize with a particular inflammatory viewpoint, have legitimate influence in some capacity, and carry a substantial online following[112].

A disinformation actor needs to control the effect of a false narrative and manipulate the reaction of a target audience. This control is gained through the infiltration of public online conversations, inciting conflict, and strengthening the illusion of consensus by trolling comment sections of online posts[113]. "Trolls" and covert operatives, backed by foreign actors, use online platforms to discuss content that connects with real people in the target audience. This organic connection is a vital pillar of disinformation efforts. Attraction and exploitation of real individuals in the target

---

[107] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[108] Margaret Harjmann, "Russia's 'Conspiracy Theory': MHl 7 Shot Down by Ukrainian Fighter Jet or Missile," *New York Magazine,·* July 22, 2014.

[109] Clint Watts, Hearing before the Senate Armed Services Committee, April 27, 2017, available at https://www.fj:Jri.org/wp-content/uploads/2017/04/Watts-Testimony-Senate-Arrried-Services-email-distro-Final.pdf.

[110] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf

[111] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf

[112] Clint Watts, Hearing before the Senate Armed Services Committee, April 27, 2017, available at https://www.fj:Jri.org/wp-content/uploads/2017/04/Watts-Testimony-Senate-Arrried-Services-email-distro-Final.pdf.

[113] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf

audience to "retweet" or spread content, or even to host events in the real world, is a primary goal of targeted disinformation campaigns[114].

Challenge

Lastly, false personas on online platforms look to heckle and troll to create confusion and chaos, making truth increasingly indistinguishable from fiction[115]. These "trolls" seek to stifle democratic debate online, overwhelming social media users with a glut of false information that works to promote doubt and paranoia[116]. "Trolling" is a prominent aspect of targeted disinformation campaigns. A "troll" is a real person who spreads inflammatory, aggressive, harassing, and misleading messages on online platforms to provoke emotional responses from other users of social media[117]. To advance the goals of disinformation operations, Russia has built trolling operations on an industrial scale, spreading disinformation and stoking emotional reactions both domestically and abroad[118]. For instance, Russian trolls have been hard at work for years, undermining political opposition to Vladimir Putin and supporting those who hold positions that align with Russian foreign policy aims[119]. During the onset of the conflict in Ukraine, Russian backed trolls aggressively attacked those with views opposite to Russian goals with offensive slurs, utilization of sarcasm, promoting false information with indigestible amounts of unsourced data, and overall seeking to emphasize and capitalize on social divisions[120].

Case Study – Russian Interference in the 2016 US Presidential Election

Overview

Leading up to and during the 2016 US presidential election, Russia conducted a targeted disinformation campaign to interfere with and undermine the American democratic system. Russian efforts were carried out through a privately contracted group called the Internet Research Agency (IRA), which was financially backed by the Kremlin[121] [122]. The IRA, at the

---

[114] https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[115] https://www.armed-services.senate.gov/imo/media/doc/Watts_04-27-17.pdf
[116] Adrian Chen, "The Real Paranoia-Inducing Purpose .ofRussian Hacks." *The New Yorker,* July 27, 2016.
[117] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[118] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[119] Miriam Elder; "Hacked emails allege Russian youth group Nashi paying bloggers," *The* Guardian. February - 7, 2012.
[120] Sanda Svetoka, et al., "Social Media as a Tool ofHybrid Warfare," NATO Strategic Communications Centre ofExcellence, May 2016, https://www.stratcomcoe.org/social-media-tool-hybrid-warfare.
[121] Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller, III, March 2019.
[122] Indictment, *United States v_ Internet Research Agency, et al_,* Case 1: 1 8-cr-00032-DLF (D.D.C. Feb. 16, ,2018).

behest of the Kremlin since 2013, looked to influence the 2016 presidential election by exacerbating existing societal tension[123] [124].

The IRA operated like an assembly line, generating false and misleading content on an industrial scale[125]. The IRA functioned like any stable PR or marketing organization would, making strategic business-like moves designed to reach as many people as possible[126]. In 2016, the IRA sought to impact the primary process for both parties directly, potentially ruining the hopes of candidates more hostile to Russian interests[127]. Recently, other initiatives to influence the democratic process have been used by Russia in places such as Syria and Ukraine[128].

Efforts to influence the 2016 US presidential election were part of a much broader campaign to harm the United States and western democracies. IRA efforts were one component of a comprehensive and sophisticated information warfare strategy to fuel discord and discontent in western democratic politics and society[129]. These recent and ongoing efforts do not obsess with the outcome of a single election. Instead, it is the downfall of the electoral system that is desired[130]. Undermining public faith in democracy and interfering with political conversations in western liberal states was the central goal during the run-up to the 2016 US presidential election[131].

With that overarching goal in mind, in 2016, the IRA engaged in a social media campaign designed to provoke and amplify social and political discord within the United States[132]. Russia's funding for the IRA was part of a more extensive information warfare operation entitled "Project Lakhta," to spread disinformation both within Russia and abroad[133]. IRA efforts to amplify false content, promote discord and divisiveness among targeted populations, and engage unwitting Americans are visible leading up to the 2016 US presidential election.

Create

First, the IRA would create fake, yet organic-looking, social media accounts, and online websites

---

[123] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[124] ODNI, "Assessing Russi.an Activities and Intentions in Recent US Elections," Intelligence Community Assessment (Declassified Version), January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_0l.pdf.

[125] Anton Troianovski, "A former Russian troll speaks: 'It was like being in Orwell's world,'" *Washington Post,* February 17, 2018.

[126] *Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Vol. 1,* Special Counsel Robert S. Mueller, III, March 2019.

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

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

[129] Indictment, *United States v_ Internet Research Agency, et al_,* Case 1: l 8-cr-00032-DLF (D.D.C. Feb. 16, ,2018).

[130] John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[131] Office of the Director ofNational Intelligence (ODNI), "Assessing Russian Activities and Intentions in Recent US Elections," *Intelligence Community Assessment (Unclassified Version),* January 6, 2017, https://www.dni.gov/filesfdocuments/ICA_2017_O1.pdf.

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

[133] Indictment, *United States v. Internet Research Agency, et al.,* Case 1: l 8-cr-00032-DLF (D.D.C. Feb. 16, 2018).

run by IRA employees to produce false and misleading content[134]. These fraudulent accounts and online sites would believably claim to be associated with US political and grassroots organizations, posing as groups with strong views on relevant and sensitive political and social issues in the United States[135]. Often, false narratives would be quickly picked up by Russian state media outlets such as Russia Today (RT). RT is Russia's foremost state-sponsored news organization and a propaganda vehicle of choice for the Russian government. RT created content, mainly disseminated through YouTube, has been viewed over five billion times and is a means to develop and pick up on other false narratives that have been concocted[136].

Overall, IRA efforts may have reached as many as 126 million people during the time leading up to and immediately following the 2016 election[137]. For instance, 81 Facebook pages associated with the IRA, followed by 3.3 million Americans, created 60,000 organic posts during this time[138]. In September of 2016 alone, around 1,000 pieces of IRA content were created weekly, reaching an estimated 20 to 30 million Americans[139]. These efforts, while centered around the time frame of the 2016 election, looked to accomplish more than influencing the election. Very little of the content created was in direct reference to any particular candidate[140]. Instead, IRA efforts showed a sophisticated understanding of American psychology, and where the rawest social sensitivities of the American political debate lied[141].

To help gain this understanding, the IRA sent a group of agents to America to determine divisive and exploitable social issues and talking points[142]. Agents ultimately picked up on sensitive topics such as race and religion that would become the focus of future efforts. Misleading content created on social media discussed these inflammatory subjects and sought to amplify divisive rhetoric and increase the polarity of political narratives[143]. Further, Russian intelligence services were able to exploit online social media platforms and hack into sensitive materials, providing further ammunition[144]. For instance, it was emails stolen by Russian intelligence

---

[134] *Report On The Investigation Into Russian Interference In The 2016 Presidential Election,* Special Counsel Robert S. Mueller, III, March 2019.
[135] *Report On The Investigation Into Russian Interference In The 2016 Presidential Election,* Special Counsel Robert S. Mueller, III, March 2019.
[136] ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," *Intelligence Community Assessment (Unclassified Version),* January 6, 2017, https://www.dni.gov/files/documentstICA_2017_O1.pdf
[137] *Report On The Investigation Into Russian Interference In The 2016 Presidential Election,* Special Counsel Robert S. Mueller, III, March 2019.
[138] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[139] 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/l l/59e0cl 7d9a79470e05a9e6cl.
[140] Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, RobertMatney, Ryan Fox, Dr. Jonathan Albright, and Ben Johnson, "The Tactics and Tropes ofthe Internet Research Agency," *New Knowledge,* December 17, 2018, littps://www.newknowl~dge.corri/articles/the-disinformation-report/.
[141] Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election - Unraveling the Russia Story So Far," *New York Times,* September 20, 2018.
[142] *Report On The Investigation Into Russian Interference In The 2016 Presidential Election,* Special Counsel Robert S. Mueller, III, March 2019.
[143] Weisburd, A., Watts, C., & Berger, J. M. (2016). Trolling for Trump: How Russia is trying to destroy our democracy. *War on the Rocks*, *6*.
[144] 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.

services that initiated the WikiLeaks publication just before the 2016 US presidential election[145].

These efforts are part of a broader operation to track and study the online activity of Americans and better understand the political and social divisions within the United States. IRA employees made strides to contact unwitting individuals in the US to refine information warfare tactics and targets. For instance, IRA operatives posed as Americans and spoke with specific grassroots organizations and learned to focus disinformation efforts on "purple" states, or states with ideological flexibility, such as Colorado, Virginia, and Florida[146]. Content material, social media account names, and specific target audiences reflect IRA efforts to research and exploit existing tensions, ultimately picking up on divisive social issues such as race, immigration, and the Second Amendment[147]. IRA operatives created content on IRA-run accounts that looked to capitalize on these hot-button societal divisions and stoke anger, provoke outrage and protest, increase distrust in government institutions, and ultimately push American citizens further away from one another.

IRA content creators would receive a list of "technical tasks" at the beginning of each workday that revolved around divisive themes and the latest news stories[148]. On relevant topics, IRA content creators were instructed to create "political intensity" by supporting radical groups and users that felt dissatisfied and discontented with current situations, and the political and social landscape in general[149]. IRA content creation activity would increase around campaign and elections events such as presidential debates and party conventions[150]. Efforts would also increase in response to real-world events, such as Hilary Clinton's physical collapse at the World Trade Center memorial while on the campaign trail[151].

Race and race-related issues were the primary targets of Russian disinformation efforts to sow discord and divide the US in 2016[152]. No single group of Americans was targeted by the IRA more than African-Americans. For instance, 66 percent of advertising done by the IRA on Facebook was concerned with topics related to race and was explicitly aimed at metro areas with high African American populations[153]. Also, the top-performing IRA operated Facebook page was centered on race-related issues, generating over 11 million engagements[154].

---

[145] 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.
[146] Indictment, *United States v. Internet Research Agency, et al.,* Case 1: 1 8-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[147]Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[148] Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[149] Indictment, *United States v. Internet Research Agency, et al.,* Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[150] Renee DiResta, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.
[151] Jim Galloway, "Clemson researchers crack open a Russian troll factory," *Associated Press,* August 7, 2018.
[152] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[153] Phil Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille Francois, "The IRA, Social Media and Political Polarization inthe United States, 2012-2018," *Computational Propaganda Research Project, Oxford Internet Institute,* December 2018: https://int.nyt.com/data/documenthelper/534-oxford-russia~intemet-research agency/c6588b4a7b940c551c38/optimized/full.pdf.
[154] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Push

The IRA, financed by Russian shell companies, worked to spread disinformation into indigenous audiences pre-determined to be susceptible to messaging on a specific topic[155]. Once created content is pushed into information circles, it becomes increasingly difficult to disprove. Successful IRA efforts weaved malicious narratives into regular conversations, even attracting high profile individuals to push false stories even further. For instance, high-profile individuals in the US, such as Roger Stone, Sean Hannity, and Donald Trump Jr., unwittingly spread content created by the IRA leading up to the 2016 election, undoubtedly growing the IRA's audience as a result[156].

A primary method that the IRA used to push disinformation was targeted online advertising. Over the two years leading up to the 2016 election, the IRA spent a total of $100,000 on targeted advertisements[157]. These advertisements reached out to specific populations, mostly in swing states, and primarily concerned incendiary and divisive political and social issues such as race, sexuality, gender, immigration, and Second Amendment rights. Most targeted advertisements encouraged social media users, particularly on Facebook, to follow IRA-created pages dedicated to these inflammatory issues. As audiences were drawn in from targeted advertising, organic content could directly entice those sympathetic to the theme of an IRA source. The IRA purchased around 3,400 Facebook and Instagram advertisements that were seen by an estimated 11.4 million Americans[158].

Another asset to the IRA is social media platform algorithms that are designed to recommend appropriate content to users that correspond to their interests. IRA created content, taking advantage of computational algorithms, was recommended to people following similar pages or who had viewed related content, making it relatively simple to spread falsehoods across a specific target audience[159]. IRA operatives utilized the mechanisms of online platforms to enhance the effectiveness of their operations precisely as they were engineered to be used. For instance, the IRA could use Facebook's geographic targeting feature to pump advertisements down to a specific state, city, neighborhood, or university[160].

---

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

[156] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[157] 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~intemet-research agency/c6588b4a7b940c551c38/optimized/full.pdf.

[158] 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,~enate.gov/sites/default/nles/documents/Facebook%20Response%20to%20Committee%20 QFRs.pdf.

[159] 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%20too/n'20Committee%20 QFRs.pdf.

[160] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Due to the speed and reach that it provides, Twitter is a particularly useful platform for pushing disinformation. Original content, primarily created on platforms such as Facebook and Instagram, was pushed out mainly through Twitter to vulnerable target audiences[161]. The sheer volume of posting and ease of spreading information via the "retweet" function assisted in reaching large amounts of people and obscuring the source and motivation for a particular false narrative[162]. The volume of IRA Twitter posts leading up to the 2016 election was overwhelming, averaging around 50,000 tweets per month[163]. Twitter eventually uncovered over 3,800 accounts related to the IRA, which generated approximately 8.5 million tweets with 72 million user engagements[164].

The use of automated accounts, or "bots," was heavily utilized on Twitter. This tool gave the IRA an ability to amplify and push out disinformation by inflating the popularity and reach of a post through the manipulation of the "retweet" function[165]. Content promoting false narratives would become popular than it was, increasing its ability to reach a target audience and appear as a genuine piece of credible information[166]. Twitter uncovered over 50,000 automated accounts tied to Russian disinformation efforts around the 2016 US presidential election[167].

One example of successful IRA efforts to push dishonest content on Twitter is the case of a fake Twitter account claiming to be related to the Republican Party in Tennessee. This phony account accumulated over 150,000 followers by the time it was shut down in 2017, and worked to push false and divisive content into the political mainstream during the run-up to the general election[168]. False narratives promoted from this account and amplified through the coordinated use of bots, found its way into the US mainstream media. For instance, content originating from the account was interacted with and spread by multiple individuals associated with the Trump campaign, such as Donald Trump Jr., Kellyanne Conway, and General Michael Flynn[169]. Eventually, content would appear in mainstream outlets such as the BBC, USA Today, and The Huffington Post[170]. Once content had been created and amplified into a target audience, and then

---

[161] 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/.

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

[163] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[164] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[165] 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] Renée DiResta, "Computational Propaganda: If You Make It Trend, You Make It True," *The Yale Review*, October 12, 2018, https://yalereview.yale.edu/computational-propaganda.

[167] Jack Dorsey, Hearing before the Senate Select Committee on Intelligence, September 5, 2018, available at https://www.intelligence.senate.gov/hearings/open.

[168] Kevin Collier, "Twitter Was Warned Repeatedly About This Fake Account Run By a Russian Troll Farm· and Refused to take it Down," *BuzzFeedNews,* October.18, 2017.

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

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

filtered into the mainstream media sources, it becomes nearly impossible to stop and has already accomplished its primary objective[171].

Share and Discuss

IRA operations then turned to more involved interaction with target audiences. Overall, IRA operatives look to stoke emotional reactions on inflammatory issues by weaving false, malicious narratives into the consciousness of unsuspecting members of the public. Once accomplished, members of a target audience will spread fake stories on their own, strengthening the illusion that disinformation on divisive social and political issues was accurate.

Leading up to the 2016 US presidential election, IRA employees operating false accounts worked to engage and increase public interaction with misleading content. IRA employees were tasked with creating and maintaining fake, yet believable online personas to seed false narratives into normal day-to-day online activities[172]. These personas looked to inflate audience participation, attract similarly-minded individuals, and then use divisive rhetoric to stoke negative emotions from the curated audience[173]. These IRA content administrators would portray themselves as proponents and advocates on an assortment of sensitive social issues such as immigration, Second Amendment rights, police brutality, race, and sexuality, both from left-wing and right-wing perspectives[174].

False accounts were successfully woven into the political discourse of the US during the 2016 election, gaining influence, engaging, manipulating, and radicalizing members of targeted online communities[175]. The IRA had an estimated 400 employees interacting with malicious content created by IRA pages[176]. IRA employees posted an average of 50 times per day and were expected to maintain a certain number of followers and level of audience interaction[177]. Operatives would make efforts to establish credibility with like-minded users by occasionally making detailed, innocuous, character-building posts, waiting for the opportune time to deliver inflammatory content. The objective was to weave propaganda into what appeared to be the everyday conversation of an ordinary American[178]. Publishing factual information increased the chance that audience members would take a phony account seriously, and increase the potency

---

[171] Brandy Zadrozny and Ben Collins, "How a right-wing troll and a Russian Twitter account cr~ated2016's biggest voter fraud story," *NBC News,* October 30, 2018.
[172] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[173] Clint Watts, Statement Prepared for the U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism: "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions.", October 31, 2017, Retrieved from https://www.judiciary.senate.gov/imo/media/doc/10-31-17 Watts Testimony.pdf
[174] DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., ... & Johnson, B. (2018). *The tactics & tropes of the Internet Research Agency*. New Knowledge.
[175] 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/c6588b4a7b940c55lc38/optimized/full.pdf.
[176] Adrian Chen, "The Agency," *The New York Times Magazine,* June 2, 2015.
[177] Max Seddon, "Documents Show How Russia's Troll Army Hit America," *BuzzFeed,* June 2, 2014.
[178] Adrian Chen, "The Agency," *The New York Times Magazine,* June 2, 2015.

of divisive content[179].

Additionally, the IRA, using false personas, would communicate with unwitting Americans and convince them to engage in offline activities[180]. The IRA would seek to persuade individuals to deepen their engagement with IRA operatives to create, organize, and promote real-life events such as political rallies[181]. Posing as grassroots activists, primarily on Facebook, IRA operatives would often organize two opposing ideological groups to come together at similar times and places to create images of conflict, generating opinions that the US was engulfed in racial and political strife[182]. At least 130 events were promoted and organized online as a result of IRA activity, and over 300,000 Facebook users engaged with content promoting these physical events[183]. Organizing physical events was Russia's way of arming opposing sides in an attempt to create civil conflict[184].

Organizing efforts primarily targeted African-American populations and hoped to develop and recruit particular individuals as assets[185]. IRA efforts sought to influence targeted individuals to sign petitions, stage events, and share personal information[186]. For instance, an IRA operated Facebook page called "Black4Black" got unaware businesses within the African-American community of Cleveland, Ohio, to give out personal information that would benefit IRA efforts in exchange for free promotion on social media[187]. Also, an IRA page called "BlackFist" was able to organize and fund a self-defense program for African-Americans in local parks[188].

Inciting political events and protest through social media became a central focus of IRA efforts leading up to the 2016 election[189]. During this period, the IRA would spend almost $100,000 supporting activists to organize 400 different protests and events across the United States[190]. An example of the IRA's commitment to insight negative emotions on inflammatory political and social issues can be seen in a real-world event organized by IRA operatives through Facebook in May of 2016. Here, IRA operatives, using Facebook's targeted advertising feature, manipulated anti-Muslimism groups through a right-wing Facebook page with a quarter of a million followers

---

[179] John Kelly, Hearing before the Senate Select Committee on Intelligence, August I, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[180] Indictment, *United States v. Internet Research Agency, et al.,* Case 1: l 8-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[181] Indictment, *United States v. Internet Research Agency, et al.,* Case 1: l 8-cr-00032-DLF (D.D.C. Feb. 16, 2018).
[182] *Report On The Investigation Into Russian Interference In The 2016 Presidential Election,* Special Counsel Robert S. Mueller, III, March 2019.
[183] 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] John Kelly, Hearing before the Senate Select Committee on Intelligence, August 1, 2018, available at https://www.intelligence.senate.gov/hearings/open.
[185] DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., ... & Johnson, B. (2018). *The tactics & tropes of the Internet Research Agency*. New Knowledge.
[186] Shelby Holliday and Rob Barry, "Russian Influence Campaign Extracted Americans' Personal Data," *Wall Street Journal,* March 7, 2018.
[187] Shelby Holliday and Rob Barry, "Russian Influence Campaign Extracted Americans' Personal Data," *Wall Street Journal,* March 7, 2018.
[188] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[189] 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.
[190] DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., ... & Johnson, B. (2018). *The tactics & tropes of the Internet Research Agency*. New Knowledge.

to organize an event called "Stop the Islamization of Texas." [191] On the opposing side, IRA operatives used the same means to arrange a similar event through the "United Muslims for America" Facebook group. The events organized by the IRA took place at the same time and place as each other in Houston, Texas. At the cost of just $200, the IRA organized events resulted in a physical confrontation and verbal abuse that was picked up and spread widely by local news agencies[192].

Challenge

Following election day in 2016, IRA activity would increase. IRA controlled accounts remained highly active and produced more than a million tweets on a typical day[193]. After content had been created, amplified, and effectively shared with target audiences, the IRA, using false personas, worked to interact with target audiences, further stoking emotional responses on inflammatory issues. Long after the 2016 presidential election, IRA operatives would simultaneously take polar opposite sides of an argument to play unwitting members of a target audience off of each other[194].

*IRA "*trolls" would monitor societal divisions and were ready to react when new events provoked unrest[195]. For instance, when NFL players began kneeling for the national anthem in the United States, IRA operatives took to social media for comment, appearing to represent both left and right sides of the ideological spectrum, spewing inflammatory content to galvanize like-minded supporters and fuel negative emotions[196]. Those performing this role within the IRA were taught how to comment on social media platforms without being detected, blocked, or removed altogether[197]. For instance, IRA trolls commenting on divisive issues were taught not to mention anything directly related to Russia or Vladimir Putin[198]. The goal was not to convince Americans of Russian foreign policy positions directly; it was to turn Americans against their government, digging up feelings of anger and discontent.

The IRA used their well-trained understanding of chasms in American discourse, such as taxation, race, gender and LGBT rights, and the Second Amendment, to "rock the boat" and increase polarization[199]. Understanding the American political environment is critical for the IRA

---

[191]Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[192]Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[193] 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.

[194] John Kelly, SSCI Transcript of the Closed Briefing on Social Media Manipulation in 2016 and Beyond, July 26, 2018.

[195] Shaun Walker, "Salutin" Putin: Inside a Russian Troll House," *The Guardian, April 2, 2015.*

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

[197] Max Seddon, "Documents Show How Russia's Troll Army Hit America," *BuzzFeed,* June 2, 2014

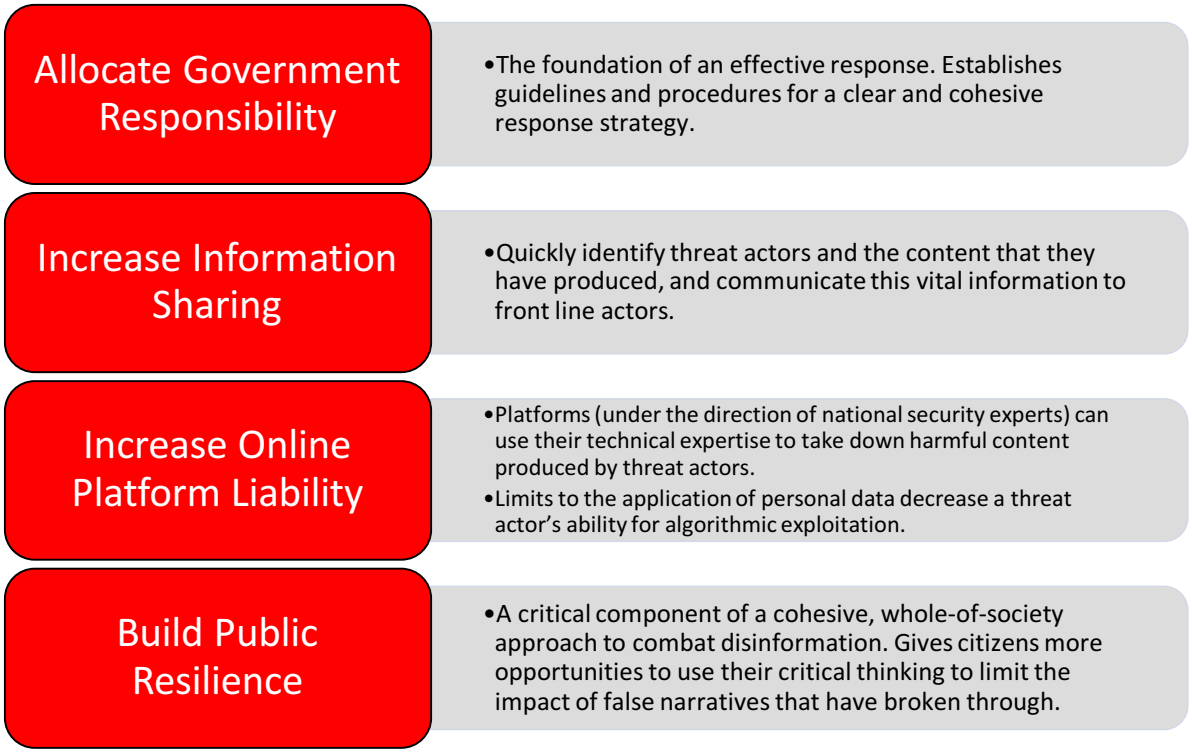
[198] Report of the Senate Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[199] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

trolling operation. IRA operatives would examine thousands of comments to gain a better understanding of trends and language used before strategically posting content that would look at home in a particular social media thread[200]. IRA trolls were paid based on their ability to maintain these real-looking personas on social media, and their ability to effectively attack and defend both sides of relevant issues such as race relations[201].

Russia's ability to play different ideological positions off of each other was a critical component of their strategy. For instance, following the 2016 election, IRA efforts shifted from focusing on provoking members of the far-Right, to stirring anti-Trump sentiment on the far-Left[202]. As Russian efforts to influence the 2020 election ramp up[203], it may be misguided to characterize those efforts in a way that makes it look like a pro-Donald Trump operation. Perhaps a greater focus on the overarching goals of Russian information warfare efforts would be beneficial, especially for framing the problem as a whole-of-society issue and getting the executive branch not to see efforts to call out Russian efforts as a challenge to the Presidential administration.

Recommendations



[200] Meduza, "An ex-St. Petersburg 'troll' speaks out", October 15, 2017, http://cs.brown.edu/people/jsavage/VotingProject/2017_10_15_Meduza_AnExStPetersburgTrollSpeaksOut.pdf
[201] Shaun Walker, "Salutin" Putin: Inside a Russian Troll House," *The Guardian, April 2, 2015.*
[202] Report of the Senate 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. (n.d.). Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[203] Goldman, A., Barnes, J. E., Haberman, M., & Fandos, N. (2020, February 20). Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump. Retrieved from https://www.nytimes.com/2020/02/20/us/politics/russian-interference-trump-democrats.html

The focus of the following recommendations is on government action to mitigate the impact of targeted disinformation campaigns. Given legitimate concerns over the restriction of First-Amendment rights, any effective government action must be bi-partisan, relatively uncontroversial, and easily implemented. As modern disinformation operations are not married to a particular election cycle, political candidate, or political party, efforts to combat them need to be sustainable in the long-term and involve a cohesive government approach.

With these concerns in mind, there are multiple options to combat targeted disinformation. US law prohibits foreign participation in US elections and permits extensive regulation of commercial advertising[204]. This fact gives ample room to develop a measured, bi-partisan, cohesive, and time-sensitive government response that covers each stage of the disinformation model. A practical, government-led response will have four main components. First, to allocate government responsibility. Second, to strengthen and promote methods of information sharing between the public and private sectors. Third, to increase the liability of online social media platforms. Lastly, to build resilience through public education.

Social media platforms have made recent efforts to combat disinformation, such as the use of third-party fact-checkers and a greater focus on identifying and deactivating inauthentic accounts[205] [206]. Also, Facebook and Instagram now permit organizations that buy political or issue-oriented advertising to run them only under identities that the platform has first verified[207]. In recent months, following the takedown of disinformation regarding the Hong Kong protests, Twitter updated its advertising policies whereby it "will not accept advertising from state-controlled news media entities. Any affected accounts will be free to continue to use Twitter to engage in the public conversation, just not our advertising products."[208]. Despite this, most efforts could be considered reactive and would benefit from centralized and cohesive government leadership. Since social media platforms have a financial incentive to permit content that attracts user attention, whether factual or false, they are unlikely to adjust their business models without external pressure[209].

Allocate Government Responsibility

The first step is to centralize counter-disinformation efforts and allocate responsibility to a single governmental party. No one section of the United States government explicitly accepts a leadership role in the area of foreign disinformation. An agency, such as the Department of

---

[204] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," Atlantic Council, June 13, 2019, https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/.
[205] "Working to Stop Misinformation and False News," Facebook, April 7, 2017, http://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news.
[206] Davey Alba, "Facebook Tightens Rules on Verifying Political Advertisers," New York Times, August 28, 2019, https://www.nytimes.com/2019/08/28/technology/facebook-election-advertising-disinformation.html.
[207] Nancy Scola, "Facebook Revamps Election Ad Rules amid Disinformation Fears," POLITICO, August 28, 2019, https://www.politico.com/story/2019/08/28/facebook-election-ad-rules-disinformation-1476638.
[208] "Information Operations Directed at Hong Kong," Twitter, August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html; "Updating Our Advertising Policies on State Media," Twitter, August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/advertising_policies_on_state_media.html.
[209] Michael Posner, "How Social Media Companies Need To Address Disinformation Globally," Forbes, June 16, 2019, https://www.forbes.com/sites/michaelposner/2019/06/16/how-social-media-companies-need-to-address-disinformationglobally/#2d2e178e3f9f.

Homeland security, should be designated as a lead agency on this issue[210]. Identifying and establishing a government agency to own the issue of targeted disinformation will have several positive impacts across each stage of the disinformation model.

First, all government actors could come together effectively and form best practices for combatting foreign disinformation. These best practices would spread to other areas on the frontline, creating a more cohesive and efficient response altogether. Additionally, this unified front could aggressively call out and respond to false narratives in a unified fashion, before they take on a power of their own. Second, this unification would centralize information sources, and lead to improved knowledge sharing with those in the private sector. Social media outlets such as Facebook have already accepted some responsibility for removing false and malicious content from their platform[211]. Strengthening the bond between them and the intelligence community would enhance efficiency, effectiveness, and the speed of which false narratives and their sources are identified and shut down.

These system-level improvements would combat foreign disinformation in its early phases. A better understanding of what particular activity to look for, and a clear, unified defense strategy would identify and eliminate false and malicious narratives before they spread into the information ecosystem. Also, a centralized government response that allows high-speed information sharing means a better overall understanding of disinformation actor intentions. Understanding these intentions is a critical component of defense and enables social media platforms to identify and take down disinformation more quickly and effectively[212]. Online platforms with greater access to real-time intelligence of how foreign actors are specifically targeting a particular audience allow for identifying threats more purposefully and efficiently[213].

Promote Information Sharing

Due to the complexities of modern disinformation efforts, cooperation is necessary to limit the spread of disinformation. It takes action from platforms themselves that understand the technology, governments to provide proper oversight, and independent researchers to continually offer insight. Investment into a multi-stakeholder approach that integrates government, private, and outside initiatives is critical to sharing information responding effectively. A multi-stakeholder approach is the status quo in other industries. Information sharing and analysis centers exist in health care, financial services, and aviation, and facilitate threat information sharing between the public and private sectors.

There are similar coalitions in the technology industry. For instance, the Global Internet Forum to Counter Terrorism (GICT) is a coalition where the UN, technology companies, non-

---

[210] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," Atlantic Council, June 13, 2019, https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/.
[211] Combating COVID-19 Misinformation Across Our Apps. (2020, May 7). Retrieved from https://about.fb.com/news/2020/03/combating-covid-19-misinformation/
[212] Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue, October, 2019. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf
[213] Clint Watts. Statement Prepared for the U.S. Senate Select Committee on Intelligence hearing: "Disinformation: A Primer In Russian Active Measures And Influence Campaigns." March 30, 2017. Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf

governmental organizations, and academics collaborate to disrupt extremist online content[214]. This coalition, formed through efforts of large technology companies in 2017, focuses on joint technology innovation, knowledge sharing, and conducting and funding research to identify and remove extremist content from online platforms more effectively[215]. A similar initiative to combat disinformation could use an independent advisory committee, as the GICT does, that includes government representatives to ensure action taken is in line with US national security interests.

Also, this initiative could utilize technological advances such as the Hash database formed through the GICT. The Hash database was developed as a tool to contain "hashes" or digital fingerprints of known terrorist images and videos which are shared with each company that joins the GIFCT's Hash Sharing Consortium[216]. Once a company has access to the hash database, it can deploy tools to automatically spot duplicates of the same content when it is uploaded on their platform. There is an existing tool in the disinformation space, called 'Hamilton 68', that could play a similar role. "Hamilton 68" is an online dashboard launched through the Alliance for Securing Democracy that provides a real-time look into Russian propaganda and disinformation efforts online. This initiative would assist online platforms, governments, and independent researchers to share valuable information, rather than operating independently. Hamilton 68 is a system that brings together messaging from overt and covert Russian propaganda outlets, and automated accounts to identify central themes and messaging priorities. The project's stated objective is to help identify Russian messaging themes and detect active disinformation campaigns as soon as they begin[217].

Exposing these themes puts a spotlight onto actor intentions and makes disinformation easier to identify and remove before it spreads. Efforts such as this will be crucial to provide social media companies the information necessary to take down accounts and pages that are spreading disinformation swiftly. Multi-stakeholder initiatives such as this ought to be backed by the federal government. Identifying relevant foreign disinformation sources and their messaging themes is a meticulous and tiresome process, and efforts to make the job of social media platforms simpler would have a substantial impact.

Increase Online Platform Liability

Due to the inherent revenue models of social media platforms, a valid government response must apply pressure to increase the responsibility and liability of platforms to take action to combat disinformation. This added responsibility will motivate platforms to take down malicious content, but also make efforts to decrease the ability of disinformation actors to push and amplify false narratives through algorithmic manipulation. Ways to increase the liability and responsibility of companies that operate online platforms are gaining attention within the government. Senator Mark Warner, a leading congressional figure in the fight against

---

[214] Global Internet Forum to Counter Terrorism: Evolving an Institution. (n.d.). Retrieved from https://gifct.org/about/
[215] Global Internet Forum to Counter Terrorism: An update on our progress two years on. July 25, 2019. Retrieved from https://blogs.microsoft.com/on-the-issues/2019/07/24/global-internet-forum-to-counter-terrorism-an-update-on-our-progress-two-years-on/
[216] Joint Tech Innovation: Hash Sharing Consortium . (n.d.). Retrieved from https://www.gifct.org/joint-tech-innovation/
[217] Rosenberger, L. Hamilton 68: A New Tool to Track Russian Disinformation on Twitter. September 4, 2019. Retrieved from https://securingdemocracy.gmfus.org/hamilton-68-a-new-tool-to-track-russian-disinformation-on-twitter/

disinformation, argues that platforms will need to be made more liable for claims like "defamation, invasion of privacy, false light, public discourse of private facts, and doctored footage."[218] Online social media platforms must identify inauthentic accounts and actively referee the spread of disinformation with a threat of sanction, perhaps by a government body such as the Federal Trade Commission. Significant and realistic steps toward increasing platform liability and responsibility will be to follow through on existing proposals to change the Communications Delivery Act, enact common-sense advertising reform, and create a "nutrition label" for internet privacy.

Communications Delivery Act

Changes to section 230 of the Communications Delivery Act should be made. These changes would increase the obligation that platforms have to monitor disinformation. Section 230 of the Communications Delivery Act was created for two reasons[219]. First, to ensure that online platforms are not liable for content posted by users, similar to publisher standards in other industries. Second, to give platforms legal impunity to use their technical expertise to police and moderate their sites as they see fit without the fear of lawsuits. Here, the central purpose is to empower online platforms to moderate themselves.

Changes to section 230 should be centered around increasing the liability of platforms for targeted disinformation that is created and disseminated by foreign actors. An increase in responsibility could lead influential platforms to more actively referee, and potentially identify and remove disinformation before it gains momentum. A compelling voice for section 230 has been US Senator Ron Wyden. Senator Wyden has stated that section 230 is intended to be both a "sword" and a "shield."[220] These statements are contrary to a prevailing view that section 230 gives companies an excuse not to moderate their platforms[221]. Section 230 has a broad interpretation and requires a greater focus on the liability it produces for online platforms. A debate is needed over whether companies are adequately using their immunity, and the subsequent responsibility to create novel and consistent ways to moderate their technologies.

The immunity that section 230 provides ought to better align with a centralized government strategy to fight disinformation. Some have argued that taking down content with a political leaning should void section 230 immunities[222]. Perhaps, in the context of disinformation, not acting on shared information about sources of disinformation, or working to find novel ways to moderate would void section 230 protections in the form of sanctions. This argument rests on the basis that the internet is not neutral; rather, it ought to exist for society's overall benefit. The public's opportunity to make rational judgments is of paramount importance, and the presence of

---

[218] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," Atlantic Council, June 13, 2019, https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/.
[219] 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text/47/230
[220] Stewart, E. (2019, May 16). Ron Wyden wrote the law that built the internet. He still stands by it - and everything it's brought with it. Retrieved from https://www.vox.com/recode/2019/5/16/18626779/ron-wyden-section-230-facebook-regulations-neutrality
[221] Wakabayashi, D. (2019, August 6). Legal Shield for Websites Rattles Under Onslaught of Hate Speech. Retrieved from https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html
[222] Laslo, M. (2019, August 13). The Fight Over Section 230-and the Internet as We Know It. Retrieved from https://www.wired.com/story/fight-over-section-230-internet-as-we-know-it/

disinformation disrupts the public's ability to form reasonable opinions and make sound judgments.

Advertising Reform

Common sense advertising reform can combat algorithmic manipulation. Here, improvements ought to center around curbing advertisers' ability to target and track potential customers online. Foreign disinformation actors can capitalize on online platforms' use of user data to target specific audiences that are vulnerable to particular messaging. Two existing proposals do well in this area, have bipartisan support, and should be passed. First is the "Do Not Track Me Online Act," introduced in 2011. This legislation includes enforcement for an online opt-out mechanism, enforced by the Federal Trade Commission, to ensure that platforms or websites may not use personal data to target and track an individual. Under this act, unsolicited use of user data would be regarded as an unfair and deceptive act or practice affecting commerce prescribed under the Federal Trade Commission Act[223].

Second is the Honest Ads Act. This legislation was introduced by US Senators Mark Warner, Amy Klobuchar, and Lindsey Graham. The goal of this legislation is to prevent foreign interference in US elections and improve the transparency of online political advertising. The act was put forth as a response to Russia's buying and placing of ads during the 2016 election, utilizing online platforms usage of user data to target specific populations. The Honest Ads Act would deter foreign actors from influencing elections by taking steps to ensure that the same rules cover advertisements sold online as ads sold on TV, radio, and satellite[224]. Providing the disclosure of this information improves overall transparency, thus preventing foreign actors from using personal data to target vulnerable segments of the general population through advertising.

The Honest Ads Act would make companies disclose how much money specific ads cost, the number of views an ad gets, how the ad specifically targets potential consumers, and the contact information of who is buying an ad[225]. Specifically, the Honest Ads Act would improve online advertisement disclosure by amending the definition of "electioneering communication" in the Bipartisan Campaign Reform Act of 2002, to include paid internet and digital advertisements[226]. It would also require digital platforms with at least 50,000,000 monthly visitors to maintain a public file of all electioneering communications purchased by a person or group who spends a significant amount of money on online advertising[227]. These steps require that online platforms more actively ensure that foreign actors cannot purchase political advertisements to influence the American public.

---

[223] Speier, & Jackie. (2011, February 18). H.R.654 - 112th Congress (2011-2012): Do Not Track Me Online Act. Retrieved from https://www.congress.gov/bill/112th-congress/house-bill/654

[224] Klobuchar, & Amy. (2018, June 26). S.1989 - 115th Congress (2017-2018): Honest Ads Act. Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/1989.

[225] Klobuchar, & Amy. (2018, June 26). S.1989 - 115th Congress (2017-2018): Honest Ads Act. Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/1989.

[226] The Honest Ads Act Explained. (2019, August 14). Retrieved from https://www.brennancenter.org/our-work/research-reports/honest-ads-act-explained

[227] The Honest Ads Act Explained. (2019, August 14). Retrieved from https://www.brennancenter.org/our-work/research-reports/honest-ads-act-explained

Nutrition Label

A "nutrition label" for internet privacy would be a simple tool that consumers could look at to understand what the privacy impact of an online platform is before they use it. Due to the inherent revenue model of online social media platforms, advertisers and technology companies are continually finding new ways to collect and monetize data. A significant barrier to consumers understanding where and how their data is being used is the privacy policies of online platforms. These policies are usually convoluted and ever-changing.

This label would be as easy to use as a standard nutrition label, with its content managed by a government agency similar to the FDA[228]. The label would fully disclose what actions platforms take with an individual's data, and provide notifications to any change in company policies. Protecting and educating consumers in this way would help them to gain a better understanding of where their data might be going, and less likely to share data on platforms that can be utilized by foreign disinformation actors. This action would strengthen the publics' ability to make informed decisions about the data they are putting online and increase their digital literacy.

The nutrition label approach is a consumer consent strategy, rather than a harm-based one. The label would give individuals the power to make decisions based on the information they gather themselves. For this reason, a nutrition label for online privacy could be passed in a bipartisan manner. Privacy policies are typically difficult to understand, allowing companies not fully to disclose how personal data is used. Greater transparency of data usage means that consumers can be more skeptical of specific policies, more mindful of where their data go, and how they are used, with the end goal of a greater understanding of how foreign actors can utilize personal data. As the usage of sites with unclear data usage policies decreases due to this understanding, it will become more difficult for disinformation actors to use personal data to spread purposefully false and malicious content.

Building Public Resilience

A vital aspect of combating targeted disinformation campaigns is to build public resilience. Public resilience is essential for two main reasons. First, creating a climate favorable to solutions on foreign disinformation is necessary as any government solutions will require favorable public opinion[229]. Second, the brunt of the effort to combat disinformation campaigns ultimately falls on the users of online communication platforms. Without users willing to endorse and share disinformation, disinformation campaigns would be deprived of the fuel that powers them[230]. Malicious online content can infect the thought process of a population similar to a virus[231]. The antidote, in this case, is the knowledge that foreign actors are actively trying to influence public opinion through social media, and what their strategy entails.

---

[228] "What Is the Trust Project and What Does It Do?," The Trust Project, accessed September 17, 2019, https://thetrustproject.org/faq/#what_does_it_do.
[229] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," Atlantic Council, June 13, 2019, https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/.
[230] Thomas Fingar (Shorenstein APARC Fellow in the Freeman Spogli Institute for International Studies, Stanford University), quoting the Pogo comic strip from 1971 in discussion with the authors, June 28, 2019.
[231] Jon Roozenbeek and Sander van der Linden, "The Fake News Game: Actively Inoculating Against the Risk of Misinformation," accessed September 17, 2019, https://www.cam.ac.uk/sites/www.cam.ac.uk/files/fakenews_latest_jrr_aaas.pdf.

Media literacy campaigns can be an effective means of protecting users against the disease like qualities of disinformation. The U.S.-based National Association for Media Literacy Education defines media literacy as "the ability to access, analyze, evaluate, create, and act using all forms of communication…Media literacy empowers people to be critical thinkers, effective communicators, and active citizens"[232]. There are indications that the American public senses the need to become more media literate. Studies indicate that news consumers admitted difficulty distinguishing between real news and false information during the 2016 US presidential election[233]. Additionally, individuals believed that accuracy, impartiality, and transparency were the most critical factors in trusted news sources, and wished that the news industry did a more thorough job of vetting information[234].

Investing in public education and strengthening public awareness addresses the "useful idiot" problem, where unwitting members of a target population spread disinformation that has been targeted towards them. The spreading of false narratives through domestic voices is a primary means of effectively implementing a disinformation campaign. Making the general public more aware and less likely to believe information from dubious sources decreases a foreign actor's ability to influence the general public. There ought to be a wide-ranging effort to empower citizens and ensure the public is well-informed and well-equipped to use critical thinking skills when consuming information online[235]. A government-led media literacy campaign should focus on communicating how algorithmic ranking works and why disinformation spreads. Federal funding for media literacy programs will help consumers sort through information online, limiting the spread and overall impact of intentionally false and malicious content.

Recent education efforts around the world should be studied. For instance, Finland has been conducting counter-disinformation efforts centered around public education and bolstering the critical-thinking skills of the Finnish public. Simple, yet effective, slogans such as "do not repeat lies," are part of Finland's comprehensive strategy to educate the public and counter Russian disinformation[236]. These efforts become less about correcting false information, and more about creating a positive counter-narrative, promoting the idea that combatting disinformation is a fundamental civic duty.

Strong public education efforts are observable in other European countries such as Sweden and Estonia. Sweden has actively produced educational content for recent election cycles that explain what signs to look for regarding targeted disinformation[237]. Estonia has long been combatting disinformation campaigns of Russian origin and has a robust response with an active component

---

[232] "Media Literacy Defined," National Association for Media Literacy Education, accessed September 17, 2019, https://namle.net/publications/media-literacy-definitions/.
[233] Darrell M. West, "How to Combat Fake News and Disinformation," Brookings, December 18, 2017, https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.
[234] "Indicators of News Media Trust," Knight Foundation, September 11, 2018, https://www.knightfoundation.org/reports/indicators-of-news-media-trust.
[235] Senate Intel Committee's Initial Recommendations on Election Security for 2018 Election Cycle. (2018, March 20). Retrieved from https://www.warner.senate.gov/public/index.cfm/2018/3/senate-intel-committee-s-initial-recommendations-on-election-security-for-2018-election-cycle.
[236] Standish, R. (2017, March 1). Why Is Finland Able to Fend Off Putin's Information War? Retrieved from https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.
[237] Taylor, M. (2019, July 31). Combating disinformation and foreign interference in democracies: Lessons from Europe. Retrieved from https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/.

of public education[238]. Estonia actively counters the pro-Russian narrative by publically calling out false stories and directly blaming those responsible. The Estonian government regularly debunks stories emerging from Russian language media, and elected officials will carefully consider what outlets to provide comments.

Conclusion

This analysis has examined how targeted disinformation campaigns operate and why they are so useful in addition to highlighting avenues for potential time-sensitive and bi-partisan government action. An increased understanding of how information warfare is being conducted to influence democratic societies is vital. Modern targeted disinformation campaigns are currently being utilized for sowing discord within American democracy. These ongoing efforts are a cheap and effective way to create real harms that have a society-wide impact. This form of information warfare capitalizes on the inherent features of internet messaging platforms and the tenants of free democratic societies. In doing so, these tactics spread false and malicious content to promote chaos and fear, generate distrust toward government, and exacerbate existing social and political divides.

Immediate government action can be taken to combat this threat. Modern disinformation operations are not married to a particular election cycle, political candidate, or political party, and efforts to combat them need to be sustainable in the long-term and involve a cohesive government approach. An effective, government-led response has four main components. First, to allocate government responsibility and centralize efforts to combat threat actors. Second, to strengthen and promote methods of information sharing between the public and private sectors. Third, to increase the liability of online social media platforms. Lastly, to build resilience through public education.

Allocating government responsibility for the issue of targeted disinformation would establish guidelines and procedures, leading to a more transparent and cohesive response strategy. A centralized command structure would improve every other aspect of the response, especially regarding the ability to share information. Improved information sharing capabilities would strengthen the capacity to identify threat actors and the content that they produce quickly, and then communicate this vital information to those actively combating disinformation in the private sector.

Further research should continue investigating ways to establish linkages between the public and private sectors. The private sector has a significant role to play in combating targeted disinformation as their platforms are the space where information warfare is taking place. As information and communications technology advance, information sharing to address policy issues becomes more feasible. Given the importance of quickly sharing information to an adequate response, identifying factors that can influence and strengthen information sharing at intra-organizational, inter-organizational, and interpersonal levels is critical[239].

---

[238] Sarlo, A. (2017, June). Fighting Disinformation in the Baltic States. Retrieved from https://www.fpri.org/article/2017/07/fighting-disinformation-baltic-states/.

[239] Yang, T. M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, *28*(2), 164-175.

Additionally, increasing platform liability is necessary. Increasing accountability would empower online platforms, under the direction of national security experts, to take down harmful disinformation produced by foreign actors and work toward novel technological solutions. Also, limits to the use of personal data by online platforms would decrease a threat actor's ability to exploit the powerful algorithms used to generate revenue. Multiple policy solutions should be considered for this aspect of the response framework.

First, further research is needed regarding changes to section 230 of the Communications Act. This research ought to explore whether changes to section 230 of the Communication Act would be an effective response to increasing platform liability. It is necessary to understand how platforms would react to these changes, and if overall efforts to combat disinformation would increase compared to a more open model that relies on the utilization of third-party fact-checking resources. Additionally, how would a more robust enforcement policy operate? Determining whether enforcement should run on an incentivized "carrot and stick" model, or a punishment-based model with the threat of sanctions from a government body is a requirement to move forward with any changes.

Another essential question to consider is whether an increased liability to remove malicious content produced by foreign actors would reduce the overall impact of targeted disinformation, and would this progress be worth the legal battle that would stem from increasing the liability of online platforms? Here, efforts should build on and apply existing research into what the legal ramifications of these changes would be[240]. The following area of study brings up a vital limit to research in the field of disinformation. The difficulty lies in being able to pin down the real impact of targeted disinformation on the public. Determining whether an individual or collective would or would not have formulated a particular opinion based on exposure to disinformation is fruitless, due to the wide variety of alternative causal mechanisms. Rather than measures of influence such as public opinion or levels of polarization, researchers should utilize more precise tests that examine levels of activity. For instance, the amount of disinformation content created by foreign actors, how quickly and effectively this content is spread, and how many users are exposed to and interact with dishonest content.

Second, additional research into the Honest Ads Act is required. Specifically, research should address how increasing advertising transparency would decrease the ability for algorithmic manipulation. Over time, would there be a significant reduction in targeted ads places by foreign actors designed to manipulate and amplify false content? Also, ways to strengthen the relatively loose definition of "political ads" should be examined, as this policy would not reach ads that are not considered to be political. Would this be a loophole that threat actors could manipulate? An additional gap may be the particular limits on spending required for advertising transparency. Research should explore how exactly foreign actors can buy advertising on smaller scales and through disguising operations to make foreign efforts look like domestic ones. Also, further research into a "nutrition label" for internet privacy is needed. Research questions should examine how information consumers would utilize such a tool. Would this label make consumers less likely to place their information in online spaces that have an unclear policy and are ripe for manipulation?

[240] Hwang, T. (2017). Dealing with Disinformation: Evaluating the Case for CDA 230 Amendment. *Available at SSRN 3089442*.

These policy initiatives are a useful place to begin combatting targeted disinformation. However, these efforts do not reach the logic of social media sites that reward outrage and bias confirmation like organic social media posts, personalized feeds, and troll farms. Understanding ways to reach these aspects without changing the ability of social media platforms to operate freely is vital. The overall difficulty of addressing the fundamental characteristics of social media revenue generation makes the element of building public resilience critical.

A central component of a cohesive, whole-of-society approach to combat disinformation is to invest in public education. This investment would give citizens more opportunities to use their critical thinking to limit the impact of false and malicious content that is created and disseminated by foreign actors. Further research should address what specific components of successful education efforts, particularly in Baltic and Scandinavian countries, would be transferable to the United States. Research questions should examine how precisely an American social media literacy curriculum would look. Aspects of past successful public education initiatives that utilize online marketing, including the successful and federally funded anti-smoking campaign, should continue to be studied and applied[241]. Research questions should also examine the development and implementation of a critical-thinking news consumption curriculum for elementary education to instill long-lasting positive habits.

Effectively responding to the challenges that society faces require substantial cooperation. Societies' ability to cooperate is threatened when the means of gathering and analyzing information is disrupted. The chaos and discord produced by targeted disinformation campaigns are real and ongoing. However, swift and decisive government action can be impactful, primarily as the United States builds up to the 2020 presidential election, and works toward finding solutions in response to critical issues such as the Covid-19 pandemic and subsequent economic crisis, racial injustice and inequality, and climate change.

[241] Impact of first federally funded anti-smoking ad campaign remains strong after three years. (2016, March 24). Retrieved from https://www.cdc.gov/media/releases/2016/p0324-anti-smoking.html