

FREE
RUSSIA



Maria Snegovaya

Kohei Watanabe

THE KREMLIN'S SOCIAL MEDIA INFLUENCE INSIDE THE UNITED STATES: A MOVING TARGET

FREE RUSSIA FOUNDATION



THE KREMLIN'S SOCIAL MEDIA INFLUENCE INSIDE THE UNITED STATES: A MOVING TARGET

Maria Snegovaya

Postdoctoral Fellow at Virginia Tech (Virginia Polytechnic Institute and State University), Visiting Fellow at George Washington University

Kohei Watanabe

Assistant Professor, Political Science Department and Digital Science Center of the University of Innsbruck & Independent Data Science Consultant

FREE RUSSIA FOUNDATION

FEBRUARY 2021

CONTENTS

1. Introduction	5
Definitions	5
Our Contribution	6
2. Russia's Social Media Operations in the United States	7
2.1 New Information Environment	7
2.2 Disinformation Ecosystem	8
2.3 Kremlin Operatives	9
Internet Research Agency	10
Main Intelligence Directorate (GRU)	10
Federal Security Service (SVR) and Foreign Intelligence Service (FSB)	11
2.4 Main Elements	12
Platforms	12
Online Kremlin-funded News Outlets	12
Media Outlets Without Direct Attribution	14
Social Media Pages, Groups and Ads	15
Promoters	16
Trolls, Honeypots and Fake Personas	17
Individuals	18
Automated Accounts/Bots	20
3. Trends in the Russian Social Media Influence	21
3.1 What's New in 2020?	21
3.2 The Moving Target	22
Platforms	22
Promoters	24
4. Measuring Impact	25
4.1 Who Is Targeted?	25
Demographic Characteristics	25
Partisanship/Political Ideology	26
Trust in Media and Institutions	26
4.2 Is Russia Successful?	27
4.3 Methodological Issues	28

5. The Study of Twitter Users' Engagement with Russia-Aligned Accounts on Twitter	29
5.1 Identifying Russia-Aligned Handle Names	30
Data collection	31
Similarity Computation	31
5.2 Interaction with Russia-Aligned Accounts	32
Content of Posts by Russia-Aligned Accounts	33
Engagement with Russia-Aligned Accounts	32
Discussion	35
5.3 Characteristics of Twitter Users Predicting Their Engagement with Russia-Aligned Accounts	36
Basic Demographic Characteristics	38
Ideology	41
Trust in Media and Institutions	45
Impact of Engagement with Russia-Aligned Accounts on Voting Behavior	48
Discussion	57
6. Policy recommendations	58
7. Acknowledgements	61
References	62
Appendix I. Russia's Social Media Operations Databases	73
Appendix II. Descriptive Statistics	74
Appendix III. Basic Demographic Characteristics and Engagement with Russia-Aligned Content	76
Appendix IV. Ideology and Engagement with Russia-Aligned Content	79
Appendix V. Ideology and Trust in Media and Institutions (OLS model)	82

1. INTRODUCTION

In recent years, Russia has executed a series of influence operations in the United States. The main goal of these operations with regard to the United States is to sow domestic discord, disrupt and discredit democratic governance, undermine US international standing and influence, and weaken the existing international system (Kenney et al., 2019; Posard et al., 2020). To achieve these goals, Russia's information operations manipulate internal domestic vulnerabilities and seek to amplify existing societal fractures within the United States (Mueller 2019; Tucker 2020). With these strategic goals in mind, Russia's information operations on social media appear to have multiple objectives, including inducing decision-making paralysis, suppressing electoral participation, strengthening groups that share Russia's objectives or point of view, and creating alternative media narratives that advance Russia's objectives (Helmus et al., 2018: 2). In fostering divisions, Kremlin proxies focus on political hot-button topics, in particular race, nationalism, immigration, terrorism, guns, and LGBT issues (Kim, 2020: 8).

This report examines recent research on the constitutive elements of the Kremlin's social media operations, as well as the results of our own analysis conducted in the aftermath of the 2020 presidential election in the US. We find that, since 2016, the Kremlin's social media operations have significantly evolved by improving their ability to conceal the identity of Kremlin proxies, as well as using the changing and more polarizing US internet environment. We also find that the groups most likely to engage with Russia-aligned content are found on the extremes of both the right and left ends of the political spectrum in the US and tend to share lower trust in mainstream media and institutions. In terms of its impact, higher engagement with Russia-aligned content correlated with increased individual propensity to take part in the 2020 US presidential election, and with decreased individual propensity to support the presidential candidates from the opposite political camp among individuals on both sides of the political spectrum. This finding is consistent with the argument that the Kremlin attempts to exacerbate the existing political divisions within the United States.

DEFINITIONS

Information operations can be defined as a means of conveying specific information that predisposes targets to voluntarily make a decision desired by the initiator of the action (Snegovaya 2015:10). Russia deploys information operations as a soft-power tool based on disinformation campaigns, propaganda, and subversion (Snegovaya 2015; Galeotti 2016). We define disinformation as information that foreign state-linked online media promote aiming to influence the American political process. In the Communist period, the Kremlin commonly used disinformation strategies to reinforce people's existing beliefs and fears and to sow divisions among targeted social groups. In the post-Communist period, a decline in traditional forms of ideological contestation made the promotion of disinformation an even more useful tool than traditional propaganda campaigns (Nye 1990; Sakwa 2012: 581). The Kremlin's long-standing disinformation tactics have been updated to account for the new context with sharing hacked information and spreading sensationalized stories

through actors who serve to repeat, promote, and amplify Russian themes and messages in an effort to reach out to American audiences (Kelly and Samuels, 2019).

The Kremlin's approach to information operations is holistic and based on development of the informational ecosystem. It taps into the government's widespread intelligence and espionage capabilities through numerous intelligence agencies, traditional media, covert websites and social networks, online bots, trolls, and unwitting individuals unknowingly amplifying pro-Kremlin narratives (Kenney et al., 2019). The new information environment is conducive for advancing the Kremlin goals, as it allows it to spread its narratives faster and to conceal its identity more successfully.

OUR CONTRIBUTION

While there is hardly a lack of analysis of the Kremlin's information operations, this report pays particular attention to the evolution of its social media approach. By reviewing existing studies on this issue, we analyze how Kremlin proxies modified their approach between 2016 and 2020 in response to the adoption of counter-measures by the US intelligence and policy communities.

We conclude that in recent years US counter-measures have achieved significant progress in combatting Russia's influence operations. In particular, these efforts decreased the size of the audiences reached by the Kremlin and susceptible to its message. To conceal their identity, Kremlin proxies now have to rely on promoters with fewer followers and smaller platforms. However, in response to this counter-effort, Kremlin influence operations have also evolved and became harder to detect. To conceal their identity more effectively, Kremlin proxies adopted more sophisticated approaches by co-opting authentic domestic voices and institutions to promote their narratives, by more actively "laundering" narratives, and by adjusting the behavior of bots and trolls to make them appear more authentic. Most importantly, the domestic information environment in the US as well as deepening polarization in recent years have provided the Kremlin more opportunities to exacerbate existing divides by amplifying narratives produced by legitimate US sources, rather than creating their own. Our key conclusion in this report is that the battle against the Kremlin's information operations is far from over.

Because Russia's disinformation is so commonly tailored to specific audiences, generic counter-approaches are unlikely to be sufficiently effective without knowing who is at risk (Partin 2020). Many analysts have identified the lack of attention to the targeted audiences as a particularly worrisome gap in policy analysis (Lucas and Pomerantsev 2016; Kalenský 2019). Therefore, we devote part of this report to quantitative analysis of US Twitter users' engagement with Russia-linked content to analyze the characteristics that make Americans more likely to engage with it. This study took place during the 2020 US presidential election.

Our project included a two-stage approach that combined improved data sampling methods for Twitter with survey methodology.

First, we recruited 2,000 US respondents who are active on Twitter for personal purposes through the Lucid Market Research Ltd. online panel. Subsequently, these respondents were surveyed with the purpose of identifying their demographic and attitudinal characteristics. Next, we collected messages posted to Twitter by our survey respondents as well as by users with whom our respondents engaged in

the last year. Using quantitative text analysis techniques and the large collection of Twitter posts, we measured how often our survey respondents engaged with narratives spread by Russia. Based on this analysis, we created an index of exposure to Russia-aligned content. Finally, we correlated the resulting index with the identified characteristics of our respondents. We found that US Twitter users more likely to engage with Russia-aligned content tend to have lower socioeconomic status, belong to racial minorities, be male, share extreme ideological positions (both left and right), and have lower levels of trust in mainstream media and institutions. Our analysis has discovered a higher propensity to participate in the 2020 presidential election among the respondents more actively engaged with Russia-aligned content. We also found that engagement with Russia-aligned content tended to negatively correlate with propensity to support the presidential candidates from the opposite political camp among individuals on both sides of the political spectrum. This finding is consistent with an argument that the Kremlin attempts to exacerbate the existing political divisions within the United States.

Our policy recommendations build on these findings.

2. RUSSIA'S SOCIAL MEDIA OPERATIONS IN THE UNITED STATES

2.1 NEW INFORMATION ENVIRONMENT

While there is a great deal of continuity between the information operations implemented by the Soviets and today's Kremlin operatives (Snegovaya 2015; Giles et al., 2015), recent technological innovations and development of the new media have fundamentally altered the information environment and information-related capabilities against which these campaigns are implemented, providing Russia a "cheap, efficient, and highly effective access to foreign audiences with plausible deniability of their influence" (Watts, 2017). These changes allowed for fast and efficient coordination across different elements of the information operations (actors and platforms) providing the Kremlin with more leverage (Snegovaya 2015: 14).

Below we summarize the key elements of the new information environment that have facilitated the Kremlin's influence operations in the United States.

First, the spread of the internet and expanding number of platforms dramatically increased content choices available to American audiences. The expansion of entertainment options, particularly for people with low interest in politics, deepened the gap in political knowledge between those who are interested in politics and those who are not (Graber and Dunaway, 2017: 106).

Second, the abundance of choices created incentives for media organizations and audiences to self-select into partisan and ideologically oriented sources of information. While the aggregate levels of knowledge increased, both Democrats and Republicans learned at different rates depending on whether the information they encountered aligned with their partisan predilections (Jerit and Barabas, 2012: 672). As a result, people online increasingly self-selected into "echo chambers" (communities of people with similar opinions), which limited their exposure to alter-

native viewpoints (Pariser 2011; del Vicario et al. 2016). This further deepened the partisanship and polarization in American society, providing ample opportunities for the Kremlin's effort to amplify US domestic divisions.

Third, while the spread of social media allowed for faster, cheaper, and easier ways of capturing and sharing news and information, it has also created additional channels through which the audiences may be misled with false information. Due to a low threshold of information access and lack of filtering, online media with questionable reputations received an opportunity to reach wide audiences, which contributed to a rapid spread of unsubstantiated or false information (Baum and Groeling 2008; Ribeiro et al. 2017). This allowed Kremlin-linked actors to bypass assistance from intermediaries, such as established broadcasters and publishers, which in the past would have limited the spread of disinformation, and directly reach out to targeted audiences, rapidly gain momentum, and thereby advance their objectives.

Fourth, the new information environment has also provided the Kremlin with new instruments, such as hackers, bots and trolls. Russian trolls are individuals in online discussion forums who attempt to derail conversations, spam them with indecent comments, spread disinformation, and steer online conversations with pro-Kremlin rhetoric. By contrast, Russian bots are programs that automatically send mass spamming with short, often identical, messages. The use of these new internet technologies gave Russia an additional tool to amplify its messages among targeted audiences.

These characteristics of the new information environment facilitated access to US audiences by the Kremlin, which is important given that it predominantly implements its operations from outside of the United States (Kenney et al., 2019). Speed is another valuable advantage provided by the new information environment as it limits the ability of counter-actors, such as NATO, to quickly respond and adjust to constantly evolving Russian information operations (116th Congress, 1st Session Senate, 2019: 18; Rid 2020).

2.2 DISINFORMATION ECOSYSTEM

Russia's approach to information operations is based on developing a disinformation ecosystem that allows for varied and overlapping approaches and narratives on social media to reinforce each other. This ecosystem combines various sources of disinformation and propaganda pushed on platforms such as state-funded media outlets, proxy websites, social media pages by promoters—including bots, trolls, false social media personalities, and (witting or unwitting) individuals (GEC, 2020: 5; Martin and Shapiro, 2019; Hanlon, 2018). Simultaneous engagement of these multiple channels creates the effect of the "firehose of falsehood," due to high numbers of platforms and messages and a fast, continuous, repetitive pace of activity (Paul and Matthews, 2016). For example, the information operation leading up to the 2016 US presidential and congressional elections was part of a three-pronged strategy, which also included the attempted hacking of the voting system; the cyber-attack on the Democratic National Committee email server and subsequent release of confidential emails to the data dump WikiLeaks website; and a sustained social media operation designed to exert political influence and exacerbate social divisions in the US (DiResta et al. 2018: 9; Cosentino, 2020).

A recent report by the Global Engagement Center identifies three reasons

why the disinformation ecosystem is particularly well-suited to serve the Kremlin's goals.

First, it allows the different elements of the ecosystem to adjust their narratives to fit different audiences. Since various channels the Kremlin has at its disposal do not require consistency (unlike traditional media), its message can be crafted to fit preferences of specific groups. This ability is important given the tendency of internet users to self-select into echo-chambers, and hence messages need to be tailored toward the specific preferences of target groups, which is consistent with the Kremlin's reflexive control approach (Snegovaya, 2015). This allows Kremlin proxies to reach out to groups of different, even opposite, ideological leanings. For example, Golovchenko et al. (2020) show that in the 2016 US presidential election, Russian trolls on social media engaged with ideologically diverse sources and promoted links to both sides of the US ideological spectrum. Other studies have demonstrated that the Kremlin commonly "recycles" bots – meaning that it uses the same bots to achieve different goals in different contexts (Starbird et al. 2014; Nied et al. 2017). For example, a series of bots that were producing alt-right narratives during the 2016 US presidential election disappeared after November 8, 2016 and reappeared in the run-up to the 2017 French election, tweeting anti-Macron content (Ferrara 2017).

Second, different elements of the ecosystem are not openly linked to Russia, allowing the Kremlin plausible deniability when their proxy platforms and promoters peddle misleading and false narratives, and providing it the ability to shield itself from criticism (Snegovaya 2015: 15-17). Russian information operations are "designed to be deniable because they use a mix of agents of influence, cutouts, front organizations, and false-flag operations" (Office of the Director of National Intelligence, 2017: 2).

Third, the disinformation ecosystem creates a media multiplier and amplifier effect among its different elements, increasing their outreach and resonance (GEC, 2020: 5). Social media appear to be the key tool of amplification of the messages the Kremlin spreads.

Coordination across these moving pieces of the disinformation ecosystem is important, although not always achieved. The most successful Kremlin operations tend to combine covert hacking and dissemination operations and social media operations with more overt channels, such as Kremlin-funded media (116th Congress, 1st Session Senate, 2019: 16).

2.3 KREMLIN OPERATIVES

Moscow commonly adopts a decentralized approach in its influence operations. Diffuse organizations on the initiative of individuals are "guided by their sense of the Kremlin's desires rather than any detailed master plan" (Galeotti, 2017a), while others are directly linked to the Kremlin and report to Russia's president. The competition among these many rival agencies is often intense (Galeotti, 2017b; Soldatov and Rochlitz, 2018), and it is not uncommon for them to go after the same target (Galeotti, 2016b).

The assessment of US intelligence reveals a sprawling campaign of influence involving several of Russia's intelligence agencies: the Federal Security Ser-

vice (FSB), the Foreign Intelligence Service (SVR), the Main Intelligence Directorate (GRU), as well as pro-Kremlin oligarch-led private company the Internet Research Agency (IRA) (Office of the Director of National Intelligence, 2017). Of the intelligence agencies, the GRU is the most active group as it has access to large amounts of resources to support its cyber operations (Cunningham, 2020).

The convergence of all these groups on one common goal of interference in the US political process is one of the most obvious indicators that the interference has been directly ordered by President Vladimir Putin.

INTERNET RESEARCH AGENCY

The activities of the IRA have received particular attention in the literature. The St. Petersburg-based company received guidance and funding from the oligarch Yevgeniy Prigozhin, who has close ties to Vladimir Putin and Russia's intelligence. As early as April 2014, the IRA formed a new department (known internally as the "Translator" (Переводчик) department) that focused solely on social media operations in the US (116th Congress, 1st Session Senate, 2019: 30; Mueller 2019: 20).

The IRA has implemented multiple social media operations in the United States, including the earliest known to date, reaching out to millions of Americans. In the 2016 US election operation, the IRA developed sustained relationships with targeted groups by infiltrating communities on social media, masquerading as members of those groups and gradually increasing the number of followers of its accounts. The IRA targeted audiences through segmentation and interest-based techniques using concise messaging, visuals with high virality potential, and provocative, edgy humor (DiResta and Grossman, 2019: 91). Twitter and Facebook proved to be particularly effective platforms for IRA purposes due to the speed and the outreach to the US audiences that they provided (DiResta et al., 2018).

In recent years successful counter-efforts aimed at exposing IRA-linked accounts made it modify its strategy. The IRA has focused less on cultivating large numbers of followers online (which requires a lot of effort and is easy to lose when an account gets blocked) and shifted more towards working with local native freelancers and outlets to promote pro-Kremlin narratives.

MAIN INTELLIGENCE DIRECTORATE (GRU)

Another actor actively involved in information operations in the United States is the GRU, the intelligence service of the Russian armed forces.

While the GRU's information operations capabilities overlap with those of the IRA (promotion of the same divisive narratives through similar means – creating fake media entities, fake personas, and fake amplification patterns), its operations are somewhat different. For example, in 2016, instead of cultivating relationships with its audience, the GRU tended to run these operations within a very short time-frame, often with frenetic posting patterns (DiResta and Grossman, 2019: 91). The GRU operations also actively relied on the strategy of "narrative laundering," which included planting a pro-Kremlin message or a story and attempting to have it picked up and distributed by larger and larger media outlets while concealing its origin. These stories were then promoted and legitimized through repetition or a citation

chain across the IRA-attributed social media accounts, other fake personas on social media, made-up think tanks, alternative news outlets, and the media outlets created by the GRU operatives (DiResta and Grossman, 2019: 9; Kelly and Samuels, 2019).

The GRU also used the “hack and leak” strategy, hacking US organizations and leaking the information to data-dump websites and journalists. For example, Fancy Bear (also known as Sofacy or APT 28), one of the groups that hacked the Democratic National Committee (DNC) in 2015-2016, was identified as GRU-linked. In 2016, Fancy Bear leaked the hacked emails to the data-dump website WikiLeaks, successfully disrupting the Democrats’ national convention in the midst of the presidential campaign. The contents of these leaks, which were widely reported on, became one of the major national narratives of the 2016 election (Kelly and Samuels, 2019; Jamieson 2020).

FEDERAL SECURITY SERVICE (SVR) AND FOREIGN INTELLIGENCE SERVICE (FSB)

The primary focus of the SVR and the FSB seems to be on cyber operations. Russian hackers, known by their nicknames APT29 or Cozy Bear, are connected to the SVR (Alperovitch, 2016). In 2014 and 2015, this group ran a wide-ranging cyber-espionage campaign targeting thousands of organizations, including government agencies, foreign embassies, energy companies, telecommunications firms, and universities. The unclassified email systems of the White House, the Pentagon’s Joint Chiefs of Staff, the State Department and the DNC were hacked as part of that operation (Nakashima and Timberg, 2020). Unlike the GRU-linked Fancy Bear, Cozy Bear did not leak the stolen emails. This is likely because contrary to the GRU, the SVR tends to steal the information for traditional espionage purposes, seeking secrets that might help the Kremlin understand plans and motives of US politicians and policymakers (Nakashima and Timberg, 2020). In 2020 Cozy Bear was yet again involved in a very successful wide-ranging hacking operation that which targeted multiple US federal and local agencies as well as private businesses (see also Chapter 3.1).

For its influence operations to be effective, the Kremlin needs to develop a deep understanding of American society. John Sipher, a retired 28-year veteran of the CIA’s National Clandestine Service, suggests that it is possible that the SVR plays a role in this area as well. Their agents, assets, agents of influence, and confidential contacts all help them determine US weak spots, and help them craft their attacks. Further, they likely assist in helping the social media operations evolve and better cover their actions.

While the FSB’s functions primarily focus on domestic operations on Russia’s territory, in recent years it has become increasingly involved in foreign cyber operations. Cyber hacking groups such as Palmetto Fusion, Turla, and Gamaredon Group are believed to be affiliated with the FSB. These organizations target different entities in different countries including the United States (Cunningham, 2020).

2.4 MAIN ELEMENTS

By drawing parallels with the former Soviets' methodology in active measures, one can classify the tools at Moscow's disposal based on their degree of public association with the Kremlin – overt ("white") and covert ("gray" and "black") (Weisburd et al. 2016). In recent years, as having a known association with Russia has increasingly become more toxic, the Kremlin has relied more on covert operations to achieve its geopolitical aims (Carpenter, 2019: 3). Covert measures are more efficient, as they allow Russia proxies to expand audiences for a certain message or narrative without exposing their direct association with the Kremlin. This approach also permits integration into pro-Kremlin groups of promoters whose interests only temporarily align with Russia's ("fellow travelers" and "useful idiots," who can broadly be referred to as Russia-aligned users) and who otherwise would have distanced themselves from the Kremlin. This allows for increased outreach of the information operations.

This marked shift "toward harder to detect, more targeted information operations that cover greater swaths of the information ecosystem" (Brandt and Frankland, 2020) constitutes an important recent development in the way Russia implements its information operations (discussed in more detail in Ch.4). In an effort to create "a fog of ambiguity between the Kremlin's actions and the Kremlin itself" (Meleshevich and Schafer, 2018), Russian proxies have engaged in more and more sophisticated approaches, by recruiting local authentic actors such as American freelance journalists and columnists to write articles (instead of their former method of having Kremlin proxies write them), modify trolls' and bots' behavior to make them seem more authentic, and more actively laundering narratives across the information ecosystem (Brandt and Frankland, 2020).

Below we categorize the elements of the Kremlin disinformation ecosystem as *platforms* that are used to create pro-Kremlin messages and narratives, and *promoters* that push and amplify those communications.

PLATFORMS

In this section we describe Kremlin-linked platforms that create and/or promote narratives that are favorable to the Kremlin. These include websites and social media platforms overtly or covertly funded by the Kremlin.

ONLINE KREMLIN-FUNDED NEWS OUTLETS

Russia's social media campaigns are part of its information operations involving traditional media channels openly funded by the Kremlin. These "white" channels include overt Russian state news outlets, such as the state-funded broadcast network RT (formerly Russia Today), its subsidiary Ruptly, the news agency Sputnik, websites of pro-Russian think tanks and foreign-based Russia-funded media that craft and promote pro-Kremlin narratives on TV, radio, and the internet. By mixing true information with manipulated or fake stories, these channels create messages that are

favorable to the Kremlin and then disseminate them online.

After successfully deploying its information operations in the Ukrainian crisis in 2014 (Snegovaya 2015), the Kremlin has significantly intensified its information operations in the West, employing primarily the RT and Sputnik News. RT, formerly Russia Today, (and its multiple branches, such as RT America and Going Underground RT) is a satellite broadcaster founded originally for public diplomacy in 2005 and which has subsequently become an outlet for active disinformation against the West. The Kremlin is involved in RT operations in different ways such as supervising hiring of managers, imposing story angles, and occasionally disapproving of stories (Elsawah and Howard, 2020: 21). RT, whose annual budget exceeds \$300 million, claims to be the most-watched news channel on YouTube (McFaul, 2020). RT's editor-in-chief, Margarita Simonyan, has recently reported that based on Tubular Audience Rating in November 2020, RT ranked third among the world's news broadcasters in terms of the number of unique users on social networks above 18 years old, bypassing the BBC and CNN. RT also ranked fourth in terms of the number of unique users on social networks, ahead of CNN. However, these numbers need to be treated carefully, given that RT is known for fudging its ratings (it often reports numbers that refer to the theoretical geographical scope of the audience) (Erickson, 2017).

Part of RT's popularity is explained by its ability to mix the entertaining content with pro-Kremlin narratives. RT provides rather critical coverage of the United States. For example, in the run-up to the 2020 election RT consistently portrayed the United States as rife with political violence, chaotic, anarchic, and on the edge of collapse (Dubow et al., 2020). RT flagship shows suggested that the 9/11 attacks were implemented by Americans themselves (Yablokov, 2015: 306). RT content seems to be directed at both extreme left and right audiences in Europe and the US (Yablokov, 2015: 306).

Sputnik News was founded in 2014 to spread pro-Russian narratives on the internet in more than 30 languages.

Disinformation operations through traditional media channels remain important for the Kremlin. Over the years, the Kremlin committed significant resources to these efforts, especially their social media footprint, and continuously expanded their funding (for example, by the draft law prepared by Russia's Finance Ministry, subsidies to RT can be increased to 27.3 billion rubles or USD 363.8 million in 2021) and their outreach (for example, RT plans to open its German-language version in 2021) (TASS, 2020).¹

Besides traditional media channels, other online "white" measures include websites directly linked to Russia. Overtly Kremlin-backed English-language sites, such as Redfish and Ruptly, have a significant presence on social media, with millions of views and engagements. Ruptly TV is an openly acknowledged RT subsidiary based in Berlin with 113,000 Twitter followers and 1.63 million YouTube subscribers. Its most popular videos exceed 3 million views. Just as RT, Ruptly content mixes "light news" videos designed to attract clicks mixed with content that is favorable to the Kremlin, such as Russia's President Putin urging the lifting of sanctions during his UN

¹ For comparison: Healthcare spending in 2021 in Russia is expected to decrease by 3% compared to 2020, and by 4% by 2023. These cuts are primarily due to the federal budget decrease, where expenses in prices adjusted for inflation in 2021 will decrease by 14% compared to 2020, and by 23% by 2023 (Бюджет – 2021, 2020).

speech (Dilanian and Ramgopal, 2020).

As examples of other websites openly affiliated with the Kremlin, the US Global Engagement Center has recently identified the “Strategic Culture Foundation,” an online journal registered in Russia that is directed by SVR and closely affiliated with the Russian Ministry of Foreign Affairs; “New Eastern Outlook,” a pseudo-academic publication of the Russian Academy of Science’s Institute of Oriental Studies that promotes disinformation and propaganda focused primarily on the Middle East, Asia, and Africa and that combines pro-Kremlin views of Russian academics with anti-US views of Western fringe voices and conspiracy theorists; “Katehon,” a Moscow-based quasi-think-tank led by Russian-intelligence-linked individuals and that is a proliferator of virulent anti-Western disinformation and propaganda via its website, which is active in five languages (GEC, 2020: 13).

MEDIA OUTLETS WITHOUT DIRECT ATTRIBUTION

This group includes media outlets that frequently echo the Kremlin line but are not openly affiliated with Russia, such as conspiracy websites, far-right or far-left websites, data dump websites as well as various news aggregators with unclear funding and motivations that amplify narratives the Kremlin spreads (Weisburd et al. 2016). While in 2016 Kremlin operatives such as GRU periodically tried creating their own content, in recent years they increasingly recruit Americans on both sides of the political spectrum to write articles and posts for these websites that indirectly align with Moscow’s agenda.

For example, *Maffick Media* is a Berlin-based company registered in March 2018 that runs a network of media productions with a significant social media presence and content targeted towards young, English speakers (Hanlon and Morley, 2019). Soapbox and “In the Now” media productions of Maffick Media take strong, often-fringe political stances on contemporary social and political issues and curate content, “packaged as meme-able satire and no-nonsense takes on history, environmental issues, and sensitive global politics” (Hanlon and Morley, 2019). Many are oriented toward younger Americans and the political left, and are meant to dealign these individuals from the Democratic party as well as to exacerbate American political tensions the same way the IRA tried to do in 2016 (Dilanian and Ramgopal, 2020; Collier and Dilanian, 2020). Although none of Maffick Media’s accounts openly admit their connection to the Kremlin, the majority shareholder of the company is Ruptly TV, an overt Berlin-based RT subsidiary. Moreover, the company’s history and financial filings reveal close ties to Kremlin-controlled media (Hanlon and Morley, 2019).

Another Russia-linked network targeting progressive and left-wing audiences in the US and the UK, Peace Data, launched in 2020 with coverage focused largely on the environment and corporate and political corruption. The network-linked personas masqueraded as left-wing journalists and editors. While some of Peace Data’s freelance journalists were real reporters, others were personas whose profile pictures were deep fakes, or AI-generated (Collier and Dilanian, 2020; Nimmo et al, 2020). They published and shared articles about the race protests in the United States, accusations of foreign interference and war crimes committed by the US, corruption, and capitalism-induced suffering, and they criticized both right-wing and center-left pol-

iticians while endorsing progressive and left-wing policies (Nimmo et al., 2020: 3).

Another such organization, the Newsroom for American and European Based Citizens (NAEBC), run by IRA-linked people, focused on the right side of the U.S. political spectrum. In an effort to influence US voters ahead of the 2020 election, the website focused primarily on US politics and current events, republishing articles from conservative media and paying Americans to write about various politically sensitive issues. A network of accounts posing as editors and journalists then promoted the articles on social media sites favored by right-wing users (Stubbs, 2020).

SOCIAL MEDIA PAGES, GROUPS AND ADS

A significant part of the Kremlin operation focuses on directly planting pro-Kremlin narratives on the social platforms through pages, groups, and ads.

The scale that such operations have reached in the US is mind-boggling. Throughout the 2016 election, at least 470 pages and accounts, followed by some 3.3 million Facebook users, were identified as IRA-created. These pages were associated with about 76.5 million user interactions, including 30.4 million shares, 37.6 million likes, 3.3 million comments, and 5.2 million reactions. According to Facebook's estimates between January 2015 and August 2017, up to 126 million Americans came into contact with content manufactured and disseminated by the IRA via its Facebook pages (116th Congress, 1st Session Senate, 2019: 40).

Rather than directly expressing clear support for one presidential candidate over another, most of the content disseminated by the IRA discreetly messages narratives of disunity, discontent, hopelessness, and contempt of others, all aimed at sowing societal division (116th Congress, 1st Session Senate, 2019: 32). The IRA-linked Facebook groups cover a range of politically sensitive issues in an effort to deepen the existing partisan division in US politics. In the 2016 election they included conservative and anti-immigration groups ("Being Patriotic," "Stop All Immigrants," "Secured Borders," and "Tea Party News"), purported Black social justice groups ("Black Matters," "Blacktivist," and "Don't Shoot Us"), LGBTQ groups ("LGBT United"), and religious groups ("United Muslims of America") (Mueller, 2019: 24-25).

However, recent analysis shades some skepticism on the scale of these operations. For example, according to Rid (2020; Howell 2020) the effect of the IRA activities was substantively overstated. First, referring to the 126 million impressions (the number of Americans who touched or saw the IRA content in 2015-17) on Facebook, many of those numbers refer to impressions (rather than views, or direct engagements). Second, according to his estimates, many of those took place after the 2016 US elections. By Rid's estimates, approximately 37% of impressions took place before the 2016 elections and the majority – almost two-thirds – took place after the elections. Hence, they were unlikely to influence the outcome of the 2016 elections. Before the 2016 elections many of the IRA accounts had significantly fewer followers, sometimes as low as one-fifth of the overall number of followers estimated by Facebook (Rid 2020; Howell, 2020). The question remains as to what extent one can make such far-reaching conclusions based on isolated elements of Russia's social media operations. Jakub Kalenský, a Senior Fellow at the Atlantic Council's Digital Forensic Research Lab, for example, suggests that "taking just social media

posts, as well as just a few news articles, or just a few statements, and analyzing them as isolated phenomena does not give us a reliable information about the impact of Kremlin's campaign. It is not one measure that matters, but rather the sum and accumulation of them, and the synergy between them." (see also McCauley, 2013) Moreover, as we demonstrate in this report, since the Kremlin's social media operations continued into 2020, the evidence of a rise in impressions continuing after the 2016 elections looks more meaningful. The election of Donald Trump and subsequent deepening polarization of US society has also potentially augmented the possibilities for IRA's work.

The paid advertisements purchased by the IRA throughout 2015-17 received a lot of media attention. However, the ads are only a minor element of the IRA's 2016 election interference, as compared to the more prevalent use of free content via multiple social media platforms. Between June 2015 and August 2017, the IRA purchased about 3,400 ads on Facebook and Instagram, which constituted only a minor share of approximately 61,500 IRA-created Facebook posts, 116,000 Instagram posts, and 10.4 million tweets. The IRA spent only a tiny share (less one tenth) of its overall operational costs of approximately USD 1.25 million per month on advertainments (116th Congress, 1st Session Senate, 2019: 40).

The IRA mainly used interest-based targeting (Kim, 2018). The ad content was distributed to target audiences through social media algorithms designed to shape content to correspond to their needs and interests. These were identified based on the users' record of following similar pages or viewing related content, as well as the information they provided in their profiles, including their interests, activities, favorite music, movies, and TV shows.

For example, the IRA used Facebook's geographic targeting feature to deliver ads to targeted audiences in specific US locations, down to the state, city, or even university level (Stretch, 2017; 116th Congress, 1st Session Senate, 2019: 44). These ads were then catered to specific interests of targeted groups, be it supporters of Second Amendment, Muslims, or supporters of Donald Trump or Hillary Clinton, based on specific issues which were at the forefront of political debates in the 2016 elections (Timberg et al., 2017; Kim, 2018: 7). The ability to use Facebook algorithms magnified the IRA's effectiveness. The most effective ads tended to have less positive sentiment, focus on past events, and were more specific and personalized in nature (Dutt et al., 2018). The IRA-funded political ads spread their narratives to an estimated 23-70 million Facebook users (Hanlon, 2018).

While disinformation operations targeting users outside the US continued in subsequent years, their scale has significantly dropped due to the tech companies' effort to block content linked to Kremlin influence operations.

PROMOTERS

This section explores actors who serve to repeat, promote, and amplify Russian themes and messages. These include trolls/fake personas and individuals who are knowingly or unknowingly used by the Kremlin to amplify its narratives, as well as non-human actors – automated accounts or bots. Studies have found that human actors play a key role in spreading false information on Twitter (Starbird, 2017).

TROLLS, HONEYPOTS AND FAKE PERSONAS

To conduct its influence campaigns in the United States the IRA in 2014-16 created thousands of *troll accounts* on social networks, such as Facebook, Twitter, and Instagram. Trolls are real people using Internet proxy services to hide their IP addresses and to post inflammatory, harassing, or misleading messages online in an attempt to provoke a response from other users. These accounts seek to connect with Americans on social networks and potentially push them to take actions in the real world that are favorable to the Kremlin (116th Congress, 1st Session Senate, 2019: 20). Russian trolls engage in a variety of influence techniques including aggressively using offensive slurs and attacks; utilizing irony and sarcasm; peddling conspiracy theories; diverting discourse to other problems; posting misleading information on popular websites; and presenting indigestible amounts of data without sources or verification (Svetoka et al., 2016; 116th Congress, 1st Session Senate, 2019: 19).

A particular subgroup in this category includes “honeypots”: fake social media profiles that are designed to engage in conversation with real people online. They may include a “component of sexual appeal or attraction, but they just as often appear to be people who share specific political views, obscure personal hobbies, or issues related to family history” (Weisburd et al. 2016). The honeypots are designed to earn the trust of unsuspecting users to disseminate content from white and gray propaganda channels, or to persuade targets to click on malicious links or deceive people into downloading viruses. Successful honey pots manage to expose to such malware specific individuals of interest (politicians, public figures), allowing Kremlin operatives to access and publish their personal information. Subsequently such information becomes instrumental in constructing narratives beneficial for the Kremlin and gets promoted through traditional white channels (Weisburd et al. 2016).

The GRU-linked accounts shared some similarities, which allowed them to be identified as suspicious. First, their author bios often claimed that they were independent freelance journalists or graduate students of a relevant academic discipline in order to justify their publication patterns of placing a single article across multiple publications. Second, they had an underdeveloped background; they often talked about only one topic, had only one photo, lacked social presence on other media; some had followers who also looked inauthentic (DiResta and Grossman, 2019: 28)

Kremlin-linked trolls engage with a wide variety of channels and means, having infiltrated and utilized nearly every social media and online information platform, including Twitter, Facebook, Instagram, Reddit, YouTube, Tumblr, 4chan, 9GAG, and Pinterest (Rosenberger, 2018). There were even attempts to infiltrate internet games, browser extensions, and music apps, for example by encouraging users of the game Pokémon Go, which was very popular at the time of the 2016 presidential election, to use politically divisive usernames (DiResta et al., 2020). Between 2015 and 2017, Russian trolls posing as American activists created Facebook events seen by more than 300,000 Facebook users (O’Sullivan, 2018).

Studies have identified several behavioral patterns of pro-Russian trolls in the United States (Zannettou, 2019a). First, their pattern of behavior in sharing of images is tightly coupled with real-world events. For instance, scholars have found a peak in activity coinciding with the Unite the Right rally in Charlottesville that took place in August 2017, suggesting their effort to sow discord during divisive events (Zannettou

et al., 2020). Second, in terms of their content, Russian trolls were mainly posting about Russia, Ukraine, and the USA. However, specific targets varied over time. For instance, Russian trolls were posting images related to Ukraine almost exclusively in 2014, and those related to Donald Trump mainly after 2016 (Zannettou et al., 2020).

In terms of their political leanings and preferences, trolls tend to promote links to both sides of the ideological spectrum by infiltrating right- and left-leaning political communities and participating in their discussions (Zannettou et al., 2019c). In the 2016 election the “conservative” trolls tended to be more active than the “liberal” ones, which was consistent with the IRA’s support for Donald Trump’s campaign (Golovchenko et al., 2020). Trolls are quite sophisticated in their messaging, i.e., they target right- and left-leaning communities differently with approaches tailored to each groups’ interests to maximize hostility across the political spectrum in the US (Boyd et al., 2016).

In recent years social media platforms became quite successful in identifying and blocking Russian trolls (see, e.g., Im et al., 2020; Ghanem et al., 2019). In response, Kremlin proxies seem to have adjusted their approach. First, in the past, Russian trolls tended to publish posts with many language errors, which made them suspicious and easily identifiable. However, they have recently adopted a new approach by copying and pasting chunks of texts written by native English speakers to avoid errors; using less text and fewer hashtags and reposting screenshots; using accounts with fewer followers; and removing or blurring watermarks (Alba, 2020). Second, instead of disseminating messages as widely as possible, as in 2016, in 2020 Russian actors have been shifting to platforms with a more limited outreach (such as blogs, 4chan and Reddit) that are harder to monitor (Barnes and Goldman, 2020). Third, the Kremlin has also relied on more targeted information operations that engage trolls and fake personas less and instead seek to co-opt authentic domestic voices and real US-based individuals. These approaches, which allow it to co-locate trolls within the targeted population, have been successfully tried by the Kremlin in several African countries and in the United States (Brandt and Frankland, 2020).

INDIVIDUALS

Since 2016, the Kremlin and its proxies have moved towards harder-to-detect approaches attempting to co-opt real-world domestic voices within target societies, especially journalists and activists, and renting social media accounts of genuine users to share content that looks authentic. This allows them to disguise their information operations as authentic advocacy (Brandt and Frankland, 2020).

Real-life individuals, publicly promoting pro-Kremlin narratives, might be subcategorized into three classes.

The first group, the “*useful idiots*,” consists of unwitting Americans who are exploited by the Kremlin to further amplify Russian propaganda (Weisburd et al. 2016). These individuals are usually sympathetic to the pro-Kremlin actor’s cause but do not fully comprehend the objectives of their campaign, and ultimately end up spreading disinformation without knowing they are actively participating in the Kremlin’s information operations (Guge, 2020: 16). The IRA set the goal of targeting US persons who could be used to advance its operational goals at least in 2014

(Mueller, 2019: 31). Since then, multiple US social media influencers (very well-networked accounts that spread messages effectively and quickly) often picked up and promoted a pro-Kremlin agenda. Since 2018, in an effort to conceal their origin, Kremlin operations appear to prioritize legitimate US-based journalists and activists over large troll farms (Brandt and Frankland, 2020). For instance, the Peace Data website launched by Kremlin-linked proxies in 2020 has hired US journalists to publish op-eds and push news that aligned with the Kremlin's agenda.

The second group, the *"fellow travelers,"* are the individuals who are ideologically sympathetic to anti-western viewpoints and whose beliefs therefore temporarily align with the Kremlin's agenda. These are commonly found among radical movements and fringe party sympathizers that are dissatisfied with the establishment and the existing political status quo. Reactionary impulses among these social groups make them embrace the themes intensely promoted by the Kremlin information operations (Snegovaya, 2020). Successful IRA efforts sometimes attracted high-profile individuals to promote their narratives. For example, several high-profile individuals in the US, such as Roger Stone, Sean Hannity, Donald Trump Jr., a number of black social justice activists, were spreading content—presumably unwittingly—created by the IRA leading up to the 2016 election (116th Congress, 1st Session Senate, 2019: 40; Guge, 2020: 21). Throughout the 2016 election, members of the Trump campaign repeatedly promoted (by linking, retweeting etc.) pro-Trump or anti-Clinton content published by the IRA through IRA-controlled social media accounts (Mueller, 2019: 33). Since 2016 Russians no longer need to spend much time creating "fake news." Instead, they increasingly make a stronger emphasis on amplifying the "fake news" being created in the US.

This group also includes Americans such as Larry King and Jesse Ventura, who have held programs on RT and other media outlets (Bodine-Baron et al., 2018: 27). For example, the American journalist Max Blumenthal, a frequent contributor to Russia Today and Sputnik, often embraces pro-Kremlin narratives in his coverage of the war in Syria. In his article, Blumenthal, who visited Moscow in December 2015 to attend the 10th anniversary of the RT network, embraces common Kremlin frames regarding the war in Syria. For example, he condemns the aggressive terrorist and economic war (a reference to US sanctions) launched against Syria by "international imperialism," calls for a media campaign to galvanize world public opinion in support of the Syrian government and accuses US policy of besieging independent and free countries (Johnson, 2019).

Third, *"agent provocateurs"* are individuals knowingly committing illegal or clandestine acts on behalf of the Russian government (Watts, 2017). For instance, in its 2016 operation, the IRA operatives posing as grassroots activists on social media convinced many unwitting Americans to engage in offline activities such as political rallies. This activity resulted in at least 130 events promoted and organized online, and over 300,000 Facebook users engaged with content promoting these physical events (Stretch, 2017; Guge, 2020: 25).

In recent years, Russia's tactics have been shifting towards amplifying and using America's polarized internet culture against itself—and the personas and conspiracy theories that inhabit it (such as QAnon). Therefore, in subsequent parts of this report we rely less on the terminology of "useful idiots" and "fellow travelers" and instead use terms such as Russia-aligned users.

AUTOMATED ACCOUNTS/BOTS

Bots or automated accounts on social media are computer algorithms designed to execute specific online tasks autonomously and repetitively. Bots simulate human behavior on social media, which allows them to believably and strategically interact with users and promote relevant content (Guge, 2020: 15). They help Kremlin operatives artificially amplify and increase the spread of the online content to attract the attention of target audiences and mainstream media (116th Congress, 1st Session Senate, 2019: 18) and to proliferate on social media platform with Application Program Interfaces (APIs).

Twitter networks are almost completely bounded by highly automated accounts. About 45 percent of Russia's activity on Twitter occurs through mostly automated accounts (Woolley and Howard, 2017). Bots tend to become more active around the time of important political events (such as elections or national conventions of the US Democratic and Republican parties) (Ferrara et al., 2020). For example, nearly 19 percent of all tweets related to the US presidential election in 2016 were generated by bots (Bessi and Ferrara, 2016); and over 50,000 Kremlin-linked automated accounts were tweeting election-related content (Twitter Public Policy Blog, 2018).

Just like other Kremlin-linked promoters, Russian bots tend to target both right-leaning and left-leaning users (Ferrara et al., 2020). However, in 2020 a large amount of bot activity on Twitter was found to be associated with rightwing conspiracy theories such as QAnon or depicting COVID-19 as a liberal scam. According to the findings, bots constituted approximately one in four accounts that used QAnon hashtags and retweeted the far-right outlets, such as Infowars and One America News Network (Ferrara et al., 2020).

Studies of available datasets of Russian bots on Twitter have revealed that they tend to be more formal and structured in their language in comparison to human accounts (trolls/fake personas), which can be identified through the use of slurs, slang, X-rated words, incorrect English, etc. (Alsmadi and O'Brien, 2020). Behavior of the automated accounts is easier to predict, and US tech companies have become much better at fighting them. As a result, in the 2020 election, bots had smaller impact on the US online conversation, as compared to 2016 (Samuels and Akhtar, 2019).

However, in response, Kremlin proxies have adjusted bot activity to make them more sophisticated and harder to detect. Compared to the earlier (fairly primitive) 2016 automation (Guglielmi, 2020), recent bots have adopted more believable online profiles, more advanced conversational skills, and stronger resemblance to real-life users embedded in human networks. In addition, some accounts are now partially managed by humans to make them appear more authentic (the so-called "cyborgs" or "sock puppets") (Samuels and Akhtar, 2019). Another novelty is the emergence of "inorganic coordinated activity," where a group of bots, humans, or a combination thereof tries to influence online conversation by strategically releasing premeditated messaging at a specific time. This makes a fairly small number of these accounts appear larger in size. A recent analysis has discovered that such networks of coordinated users tried to promote unrelated causes and disinformation (such as anti-vaccine content) using the viral hashtag the #DemDebates during the Democratic debate held on October 15, 2019 (the so-called "hashtag hijacking" or "hashtag surfing" (Samuels and Akhtar, 2019).

3. TRENDS IN THE RUSSIAN SOCIAL MEDIA INFLUENCE

3.1 WHAT'S NEW IN 2020?

Despite the counter-measures adopted by the US policy and intelligence communities, the Kremlin's attempts to interfere in the US political process continued during the 2020 US presidential election.

Some tactics for 2020 election interference remained the same as in 2016. For example, the IRA-backed trolls pretended to be locals, targeted Americans on both the left and right with posts designed to foment outrage, fear, and hostility and to discourage specific demographics from voting with a particular focus on swing states (Kim, 2020). Among other goals, Kremlin proxies allegedly tried to promote the presidential nomination of Senator Bernie Sanders and assist the reelection of President Donald Trump, whose statements they often amplified (Sanger and Kanno-Youngs, 2020).

However, Kremlin proxies also learned from past mistakes. For example, the IRA-linked trolls became more sophisticated in their attempts to conceal their identities, making it harder to identify and track them. In particular, the IRA trolls became better at impersonating candidates and parties, and instead of creating their own fake advocacy groups (as they did in the past) got better at mimicking and appropriating names and logos of actual official campaigns and groups (Kim, 2020). Some of these efforts have been taken outside of Russia. In contrast to 2016, when much of the trolling was operated from the IRA office in St. Petersburg, in 2020 part of the influence operation was outsourced to troll farms in Ghana and Nigeria (Ward et al., 2020).

In 2020, Kremlin proxies also improved their techniques for concealing the origin of information, a tactic known as "information laundering." Under such an approach, pro-Kremlin narratives are spread on Russia-affiliated websites and then picked up and promoted by more legitimate news outlets (Brandt and Frankland, 2020). For example, Kremlin proxies create an account and post a false story on it; then they deploy a second set of fake accounts or websites to post expanded versions of the story referencing the original post as their source; and eventually they engage a third set of accounts or websites to attract the attention of traditional media outlets (Aleksejeva et al., 2019). In 2020, at least two new websites were identified (and subsequently blocked by Twitter and Facebook) as being part of such an operation, the left-leaning PeaceData and the right-leaning NAEBC (see also Chapter 2.4).

Kremlin proxies also increased the use of seemingly nonpolitical content and commercial accounts, which allowed them to conceal their attempts at building networks of influence (Alba 2020; Kim, 2020).

In 2020 the Kremlin also succeeded in implementing one of the most serious cyberattacks ever suffered by the United States, targeting multiple US government entities, including federal, local, and territorial networks, as well as many business organizations. The attack, which had gone undetected for months, began no later

than March 2020. It was allegedly implemented by the SVR-linked hacking group Cozy Bear (APT29), which exploited software from at least three US firms: Microsoft, SolarWinds, and VMware.

While attempts to estimate the damage are still ongoing, by some accounts the stolen information has multiple uses and might provide the Kremlin significant leverage in the next years (Tidy, 2020). Another reason for concern is that the attackers used unusual and creative ways to carry out their operation by disguising the initial attack within legitimate software updates (Fung, 2020). While this alleged hack illustrates the capabilities of Russia's foreign intelligence services, it is not a trend or a new development in 2020; it represents more of a traditional espionage operation rather than a social media operation (unless some of the stolen information is to be gradually published through mass media).

3.2 THE MOVING TARGET

Looking at Kremlin operations on social media over recent years, one clear conclusion is that the Kremlin's influence effort isn't going away. Despite the sanctions levied on Russia and multiple counter-measures developed by the US policy community and social media companies, the Kremlin's influence operations did not stop. Instead, they slowed and evolved to avoid detection (Kelly and Samuels, 2019). The Kremlin adjusted the use of platforms and promoters to better conceal their identities and links to Russia.

While failing to fully block the Kremlin interference effort, US countermeasures seem to have succeeded in diminishing the outreach of the Kremlin proxies, which now are forced to rely on accounts with fewer followers and smaller platforms with less monitoring and regulation to avoid detection. That, however, does not mean that the war against Kremlin disinformation is won. Among other things, in recent years, the spread of domestic online disinformation has significantly facilitated the task of Kremlin proxies, which now can resort to amplifying misleading and biased narratives already present in the US information environment (instead of creating their own original content and trying to make it seem true).

Below we summarize the key elements of the evolving Russian influence strategy.

PLATFORMS

- 1) *More efforts to polarize online discussions by drawing on existing narratives.* Given domestic political divisions in the US in recent years more of the disinformation started to be produced by legitimate US sources. Accordingly, Russian proxies shifted to primarily amplifying them rather than creating them. Instead of creating their own false content, Russian proxies tend to increasingly rely on existing narratives to further polarize online conversations. To do so they often use false-flag operations or amplify homegrown conspiracy theories (Brandt and Frankland, 2020) and content (CNBC, 2020). This approach also makes it harder to detect Kremlin-linked accounts.

- 2) *Growing identities hijacking.* Kremlin proxies have also become more likely to take over authentic hashtags, and mimic or appropriate names and logos of official campaigns and local groups. Many IRA posts increasingly adopt the identity of legitimate, relatively popular nonprofits, political action committees, or grassroots organizations by using posts from those groups or creating their own content (Kim, 2020). In the past, Kremlin proxies tried creating their own think tanks and “alternative news” sites to serve as initial content drops (DiResta and Grossman, 2019). By 2020, they seem to prefer hijacking the existing ones from the authentic actors. For example, networks of coordinated users (trolls and bots) were found in 2019 attempting to promote unrelated causes and disinformation using the hashtag the #DemDebates during the Democratic debate (Samuels and Akhtar, 2019).
- 3) *Moving to smaller platforms.* Instead of increasing its outreach as widely as possible, as in 2016, in 2020 Russian operatives have been using platforms with a more limited outreach (Barnes and Goldman, 2020). The total number of influence efforts declined in news outlets, on Twitter, and on Facebook after 2017. There were also fewer operations on Instagram, YouTube, and other platforms. Instead, Kremlin proxies often moved to smaller platforms such as blogs, 4chan and Reddit, or used closed chat rooms, private Facebook groups with less regulation and monitoring (Martin and Shapiro, 2019; Kelly and Samuels, 2019).
- 4) *Narratives laundering.* While used by Kremlin proxies in the past, narrative laundering seems to have grown in popularity in recent years (Brandt and Frankland, 2020). “This approach is suggestive of intelligence operators whose mission is to carry out their work undetected, without creating a discernible community” (Aleksejeva et al., 2019: 8).
- 5) *More efforts to polarize online discussions by drawing on existing narratives.* Because in recent years more of the disinformation started to be produced by legitimate US sources, Russian proxies shifted to primarily amplifying them rather than creating their messages. Instead of creating their own false content, Russian proxies tend to increasingly rely on existing narratives to further polarize online conversations. To do so they often use false- flag operations or amplify homegrown conspiracy theories (Brandt and Frankland, 2020) and content (CNBC, 2020). This approach also makes it harder to detect Kremlin-linked accounts.

PROMOTERS

- 6) *Declining number of bots, trolls, and fake accounts, and declining number of followers.* Because themed accounts with politically divisive content and multiple followers have become more suspicious and attracted attention of regulatory and investigative bodies, Kremlin proxies appear to be working harder at hiding their origin and tend to rely more on accounts with fewer followers (Alba, 2020).
- 7) *Trolls and bots adjusting their behavior.* The IRA trolls have been adjusting their image to make detecting them harder. For example, while in the past Russian trolls often published posts with many English errors, in recent years they started copying and pasting chunks of texts written by English natives to make fewer errors. They also use less text and fewer hashtags, by reposting pictures and screenshots instead, removing or blurring watermarks (Alba, 2020), as well as using AI-generated profile pictures (Nimmo et al, 2020).

Bots have evolved as well, adopting more believable online profiles, more sophisticated conversational skills, and stronger resemblance to real-life users embedded in human networks. Some accounts are now partially managed by humans (the so-called “cyborgs” or “sock puppets,”) which makes them appear more authentic (Samuels and Akhtar, 2019). The “inorganic coordinated activity” is another new technique: a group of bots, humans, or a combination thereof strategically releases premeditated messages at a specific time in order to influence the online conversation. This approach allows these accounts to appear larger in size (Samuels and Akhtar, 2019).

The above evidence is consistent with a broader argument about the flexibility and adaptability of the Kremlin’s information warfare tactics to the changing geo-strategic environment (Mölder and Sazonov, 2018). The Kremlin’s continuous focus on the information environment is evidenced by its ongoing expansion of Russia’s information influence globally (Bugayova, 2020), as well as by the growing budgets of the Kremlin-funded news outlets such as RT (see Chapter 2.3). This suggests that Kremlin information operations will remain a challenge for the United States in years to come.

4. MEASURING IMPACT

4.1 WHO IS TARGETED?

The above analysis has demonstrated that the proxies often carefully tailor their messages to specific interests of target US audiences. This approach is linked to the concept of *reflexive control* which Russia has used in its influence operations since the Soviet times. *Reflexive control* allows a controlling party to influence the target into unknowingly making bad decisions by interfering with its perceptions (Thomas, 1996; 2004; 2009; Snegovaya 2015). For reflexive control to be effective, a controlling party (the Kremlin) needs to understand its target's filter. *Filter* refers to concepts, knowledge, ideas, and experience of the target that are the basis of their decision-making (Thomas, 2004: 2). The goal of reflexive control is to find, emphasize, and exploit a weak link in the enemy's filter by imitating the target's reasoning and causing them to make a decision unfavorable to themselves (Leonenko, 1995: 28).

The use of interest targeting while designing Facebook ads, for example, is an example of how a target's filter can be identified (see Ch.2.4). The IRA designed ads based on the information about users' following similar pages or viewing related content, as well as their profile information (such as their geographic location, interests, activities, favorite music, movies and TV shows) (Stretch, 2017; Timberg et al., 2017; 116th Congress, 1st Session Senate, 2019: 44).

What are the specific filters commonly exploited by Kremlin proxies in their US social media operations? Below we explore the characteristics of social groups that may make them more likely to engage with Russia's disinformation.

DEMOGRAPHIC CHARACTERISTICS

Lower education and lower socioeconomic status may be associated with higher propensity to engage with disinformation. Respondents with lower education and socioeconomic circumstances are less likely to check information they come across online (Carmi et al., 2020: 13), which makes them more likely to engage with such content (Bargaoanu and Radu, 2018; Glenski et al. 2018). Groups more prone to engage with disinformation are found among the representatives of the lower middle class or working class with only a basic education (Kandrik and Jevčák 2018: 3).

Race is another important variable that in the US context may predict higher levels of engagement with Russia-aligned content. Studies have identified the African American community as being targeted particularly actively by Kremlin proxies. Given the salience of racial issues in the US context, IRA operations were purposefully designed to inflame racial tensions and influence presidential elections in both 2016 and 2020. For example, throughout the 2016 campaign, the IRA Facebook ads (over 66% containing a race-related term), its social media pages (the "Blacktivist" page on Facebook generating 11.2 million engagements with Facebook users) and Twitter and Instagram accounts (five of the top 10 IRA Instagram accounts focused on African-American issues and audiences, the most popular @blackstagram account collected 303,663 followers) all consistently pushed racially divisive narratives (116th Congress, 1st Session Senate, 2019: 7; DiResta et al., 2018). After 2016,

fueling the racial divide remained a running theme of the IRA social media operations. In 2020 they kept pushing the narrative related to police brutality and racism against African Americans, as well as attempting to mobilize hate and supremacist groups. In addition to social media accounts, more traditional channels, such as RT and even Russian government Twitter feeds, promoted related themes (Barnes and Goldman, 2020).

PARTISANSHIP/POLITICAL IDEOLOGY

Many studies in the US show that partisanship consistently predicts people's engagement with disinformation (Kahan, 2017; Van Bavel and Pereira, 2018). Kremlin proxies spread negatively framed information that is tailored to these groups' political views, i.e. each group receives information about their political opponents that is deemed politically damaging. For example, conservatives are often given information about outrages committed by liberals, immigrants, George Soros, and others; liberals are shown the information about misdeeds of Republicans, Trump administration, or evangelical Christians (Linville and Warren, 2019; Freelon et al., 2020).

However, political partisanship alone is unlikely to fully account for people's susceptibility to disinformation. First, people on both sides of the political spectrum are more likely to engage with disinformation. This suggests that partisans on both sides of the political spectrum may have similar characteristics that explain parallels in their behavior. Second, some studies find that partisan bias of presented information and individual political affiliation play little role in perceptions of information accuracy (Pennycook and Rand 2019). Hence factors other than partisanship may also play a role in individual susceptibility to disinformation. For example, the effect of stronger partisanship might be mediated by variables, such as lower trust in media and the establishment.

TRUST IN MEDIA AND INSTITUTIONS

Studies find that lower trust in traditional media might (somewhat ironically) make people more likely to engage with disinformation (Zimmermann and Kohring 2020). In the US context the effects of lower media trust may be particularly pronounced given the frustration with the traditional media that has spread among Americans in recent years (Brennan, 2019). According to the data from Edelman's annual trust barometer, by the end of 2020 trust in traditional media in the U.S. has declined to an all-time low with fewer than half of all Americans having trust in traditional media (Salmon, 2021). This finds its confirmation in popularity of the term "mainstream media." Often used with a negative or pejorative connotation, this term refers to various large traditional media conglomerates that influence and shape prevailing ideological positions of the largest audiences (Chomsky, 1997; LaMarco, 2018). The "mainstream media" are then contrasted to "alternative media" on the internet, which allegedly allow for the expression of more alternative viewpoints (Tkacheva et al., 2013). In the US context, the mistrust in media is particularly pronounced among self-identified conservatives who often accuse "mainstream media" of having a "liberal bias" (Lee 2005; Gauchat, 2012; Kraft et al., 2014). However,

both liberals and conservatives freely associate traditionally rightwing and leftwing media sources respectively with the term fake news (van der Linden et al., 2020). The amalgamation of terms now also includes the “lame-stream” media often used by conservatives to describe how out of touch traditional (primarily left-leaning) outlets have become. Therefore, mistrust in “mainstream media” may make Americans on both sides of the political spectrum more likely to engage with Russia’s disinformation.

Similar reasoning may be applicable to institutional trust more broadly (be it traditional media, big corporations, international institutions, the political establishment, and so on) (Freeman et al. 2020; Kim and Cao, 2016; Einstein and Glick, 2015). Recent studies suggest that the lack of trust in political institutions may be among the key factors that make people on both sides of the political spectrum susceptible to disinformation (Gunther and Storey 2003; Zimmermann and Kohring 2020; van der Linden et al., 2020) especially given that Russia’s online disinformation campaigns are directly targeted at fomenting mistrust in the establishment and political institutions (Watanabe 2018).

If trust in established institutions is low, media literacy programs that are (in view of mistrustful social groups) promoted by the establishment itself will not be effective in changing their views and information consumption patterns. Groups with low levels of media and institutional trust require more sophisticated approaches designed to restore their confidence in actors promoting those programs in the first place (Silverblatt 2015; Humprecht et al. 2020).

4.2 IS RUSSIA SUCCESSFUL?

To what extent have Russia’s disinformation operations succeeded in achieving Russia’s goals?

The answer largely depends on how one understands the goals of Kremlin operatives. For example, while in its 2016 election interference the IRA expended significant effort building up a presence on social media platforms and was able to amplify its messages across wide audiences, the GRU largely failed to achieve virality on social media (DiResta and Grossman, 2019: 9-10). However, when viewed as traditional media operations, the GRU campaigns were fairly successful throughout the same period. The GRU placed articles from multiple fake personas in over 140 media outlets and those were periodically amplified by large state media entities (DiResta and Grossman, 2019: 9-10). Given the success of the US counter-measures in blocking Kremlin-linked accounts with a large number of followers, in recent years the IRA approach shifted to more closely resemble the GRU operations, planting pro-Kremlin narratives in local outlets run by partisan American groups (see Chapter 4).

Quantitative studies of the impact of Russia’s influence operations return mixed results. On the one hand, some successes are undeniable. Throughout 2016 IRA-linked Facebook groups succeeded in organizing multiple opposing rallies, drawing American citizens into the streets in direct opposition to one another (116th Congress, 1st Session Senate, 2019: 37, 40, 42, 46; Mueller, 2019). A recent RAND study demonstrates that Russian disinformation may be able to deepen polarization within American society. By targeting users with extreme partisan views on both sides

of the political divide, the Kremlin's disinformation narratives are able to successfully elicit strong partisan responses that may help exacerbate divisions in American society (Helmus et al., 2020).

Jamieson (2020) argues that the DNC leaks by Russian hackers were able to successfully shift the media agenda in the final presidential debates and the final month of the 2016 election, which benefited Donald Trump and ultimately likely brought him victory. As result, according to Jamieson, Russian trolls and hackers probably affected the outcome of the 2016 election by mobilizing potential Trump voters and discouraging liberal voters who weren't keen on Clinton. However, she points out that quantifying the impact of the Russian activity is impossible in the absence of "real-time, rolling cross-sectional polling data tied to media messaging and exposure in each of the three decisive states," Michigan, Pennsylvania and Wisconsin. And even if one had such a panel, the effect of specific Russian propaganda efforts would be hard to isolate from confounding factors, because of the difficulty of finding a control group not exposed to them (Jamieson, 2020; Bershidsky, 2019).

On the other hand, a number of studies find that the impact of disinformation on US users' opinions is minimal. For example, the longitudinal analysis of data on Republicans and Democrats from late 2017 and Twitter accounts operated by the IRA found no evidence that interacting with these accounts substantially impacted US respondents' political attitudes and behaviors (PNAS, Bail et al. 2020). Similarly, scholars who investigated Russian trolls' ability to spread news stories found that their effect was marginal, with the significant exception being the news published by the state-funded RT outlet (Zannettou et al. 2019c). Eventually, a high number of complicating factors make it hard to estimate the real impact of these operations (see also Rid 2020).

4.3 METHODOLOGICAL ISSUES

While most studies exploring the impact of Russia's social media operations are conducted on Twitter for data availability reasons (e.g., Gatewood and O'Connor, 2020; Golovchenko et al., 2020; Helmus et al., 2018; Marcellino et al., 2020), this impact cannot be measured accurately without careful sampling of users and messages on the platform.

Keyword-based sampling of messages tends to overemphasize the influence of Russia's disinformation, because such a sample usually contains messages about divisive topics (e.g., election and racial inequality). While keyword-based sampling can be justified as it grants researchers efficiency in revealing Russia's disinformation strategies, the analytical result does not carry implications for Twitter users who are not interested in these topics.

Random sampling of messages is also unsuitable for measuring accurately the influence of agents/trolls on average users, because such a sample will be dominated by a small number of highly active users.² Although random sampling is a better approach to measuring impact than keyword-based sampling as it offers a

² Earlier study shows that average Twitter users post messages only twice a month. 80% of posts are produced by 10% of active users (Wojcik & Hughes, 2019).

wider picture, the results cannot be generalized beyond the Twitter user community.

Random sampling of users leads to a biased estimation of the impact, because only a small number of Americans use Twitter, and their demography is very different from the American population: only 22% of Americans answered they ever used Twitter, and these are more liberal and concentrated among younger generations (Perrin and Anderson, 2019).

To study the impact of Russia's social media operations on Twitter and other platforms (Facebook, Instagram, Reddit etc.), researchers must combine the information about users' individual-level characteristics and their engagement with the analysis of the content promoted by the Russian agents/trolls. Combining these pieces of information allows one to capture how individual-level characteristics (such as age, gender, socio-economic status, and political orientations) correlate with exposure to disinformation. Since Twitter does not collect information on users' personal characteristics, researchers must combine surveys of users along with content analysis of social media posts. The below study presents the results of such an analysis.

5. THE STUDY OF TWITTER USERS' ENGAGEMENT WITH RUSSIA-ALIGNED ACCOUNTS ON TWITTER

Social media analysis provides a window into the perspectives, thoughts, and online behavior of a wide range of relevant audiences against which information operations are implemented. Social media platforms allow researchers to study users' susceptibility to particular narratives among social groups targeted by the Kremlin's information operations if combined with information on their demographics that is obtained through a questionnaire survey. This knowledge could help inform policymakers and help them develop countermeasures crafted to the needs of particular audiences and groups (Marcellino et al.2020).

We conducted an analysis of Twitter users' demographic information, attitudes, and political ideology along with their online behavior prior to the 2020 presidential election. We expected that the Kremlin would intensify its information operation during this politically important period, allowing us to reveal its overarching strategy, but its tactics could be specific to the political and social circumstances of the time as our analysis of hashtags indicates.

The result of this analysis shows that the direct impact of the Kremlin's information operation through in the Unites States is limited, but there are highly active and strongly ideological Twitter users who promote the same narratives as the Kremlins proxies do. American social media users with low socioeconomic status tend to be susceptible to their ideological messages. This ecosystem on the social media platform allows the Kremlin to penetrate the public discussion on political and social issues in the United States more deeply.

5.1 IDENTIFYING RUSSIA-ALIGNED HANDLE NAMES

Studies existing to date have predominantly relied on external datasets to identify Twitter handle names associated with the activities of Kremlin proxies (IRA or GRU). However, no existing lists are suitable for our study, as they quickly become obsolete after publication.³ Instead, in this study we relied on a novel approach, applying a home-grown list of accounts to analyze online behavior of our survey respondents. First, we surveyed 2,000 Twitter users in the United States, asking them questions on their demographic and attitudinal characteristics. Next, we generated a list of “Russia-aligned accounts” who resemble pro-Russian media, using the word-embedding technique as described below.

The identified Russia-aligned accounts are not necessarily affiliated with IRA or GRU (establishing that link is beyond our capacity in this study), but they promote narratives that are also actively pushed by Kremlin proxies. This is sufficient for our purposes, since we assume that our survey respondents who frequently engage with Russia-aligned accounts should have similar personal characteristics as social media users who frequently engage with *actual* Russian-aligned accounts given that content of posts made by both types of accounts is very similar.⁴

We use the list of identified Russia-aligned accounts to measure how often our survey respondents were exposed to narratives that the Kremlin promotes. By combining the information about their engagement with Russia-aligned accounts we revealed the individual-level characteristics that distinguished those Americans in our sample who were more prone to engage with Russia’s narratives.

Such an analysis allows us not only to identify how widely Russia’s narratives spread on social media but also to discover specific individual characteristics of social media users who are more prone to engage with pro-Russian narratives. Given our attempt to ensure representativeness of the survey sample in two different ways (see chapter 5.3 below), the frequency of engagement with Russia-aligned accounts among our users may be hypothesized to reflect how often Americans on Twitter encounter pro-Russian narratives.

To identify Russia-aligned users we collected Twitter posts and computed the similarity between handle names using only publicly available tools and resources. We used Twitter Timeline API to collect users’ most recent posts retrospectively up to 3,200 in data collection, and R packages (*quanteda* and *LSX*) for the similarity com-

3 A list of Twitter handle names identified as under the control of the IRA was published by the US Congress soon after the 2016 Presidential Election (<https://intelligence.house.gov/social-media-content/>), but these lists become obsolete as soon as they are published because they will be deleted or suspended by platforms and new accounts will be created by the disinformation agents. Twitter also released a dataset of anonymized posts by users affiliated with foreign states including Russia (<https://transparency.twitter.com/en/reports/information-operations.html>) but it only covers from May 2009 to December 2019.

4 In other words, it does not matter if social media users who promote Russia’s narratives are actually affiliated with the Russian state or not from the respondents’ perspective. This approach is analogous to survey experiments, in which mockup texts are used as a device to analyze participants’ responses.

putation. Quanteda is a highly efficient preprocessing tool for textual data analysis (Benoit et al., 2018); LSX implements the Latent Semantic Scaling (LSS) technique to compute similarity between words accurately (Watanabe 2020).

The advantage of this proxy approach is that it allows us to generate a long list of Russia-aligned accounts while only collecting pro-Russian media posts and handle names on Twitter. This method also permits us to identify handle names of those users whose accounts have been deleted or suspended by the time of our data collection, because it only relies on whether Russia-aligned accounts are mentioned in other users' posts. However, this approach has its limitations. For example, it does not allow us to automatically determine whether the identified Russia-aligned accounts are de facto affiliated with the Kremlin. This approach also does not allow us to discover those accounts that promote narratives that are different from the ones pushed by pro-Russian media.

DATA COLLECTION

To identify Russia-aligned accounts, we collected 880,000 publicly available Twitter posts by our survey respondents since January 2020 through the Timeline API in November ("main collection") and extracted 14,139 handle names of users they mentioned in their posts at least 10 times since the beginning of the same year. Next, we downloaded 7 million Twitter posts by the users in October 2020 ("expanded collection") when the social media users were active on political and social issues prior to the election.

SIMILARITY COMPUTATION

First, we selected widely recognized pro-Russian and international/foreign media as "seed accounts" (see the list of the identified media in Table 1). Second, we fitted the LSS on the expanded collection to compute the similarity between all the handle names ($n = 98,348$) based on their surrounding words and hashtags in the posts.⁵ Third, we selected 5% of the handle names with highest and lowest proximity to the handle names of the seed accounts, and treated handle names with high proximity as Russia-aligned accounts and those with low proximity as "benchmark" accounts ($n=2,459$ each).

⁵ Word embedding techniques are utilized in the state-of-art natural language processing tools. We used SVD as the underlying algorithm for dimension reduction with $k = 300$. This technique is analogue to factor analysis of a document feature matrix to identify a smaller number of common contexts. We can generate a list of users who post similar content as pro-Russian media because they are mentioned in similar contexts by users in the expanded collection.

PRO-RUSSIAN MEDIA ACCOUNTS	BENCHMARK MEDIA ACCOUNTS
@sputnikint	@telegraph
@sputniknewsuk	@ajenglish
@sputniknewsus	@bbcworld
@rt_america	@dwnews
@rt_com	@skynews
@rt_doc	@financialtimes
@rtuknews	@cnni
@tassagency_en	@cnn
@russiainsider	
@ruptly	
@redfishstream	

Table 1. List of handle names of the seed accounts. Benchmark media are used to control users' general interest in non-US news stories.

5.2 INTERACTION WITH RUSSIA-ALIGNED ACCOUNTS

We measured how often our survey respondents interacted with the Russia-aligned users in 2020 by searching their Twitter posts in the main collection for the handle names. We do not provide specific handle names of users that we identified as being aligned with pro-Russian media in this report to comply with Twitter's policy on privacy protection. We manually inspected posts and profiles of the accounts most strongly aligned with the pro-Russian media to find that they are highly active and ideological personas, who often express American patriotism, support for Republican candidates, religious views, or conspiracy beliefs in their posts and profiles. However, many accounts were inaccessible because they were suspended or deleted, presumably due to violation of Twitter's rules on hate speech and disinformation.⁶

CONTENT OF POSTS BY RUSSIA-ALIGNED ACCOUNTS

We collected messages posted in October by the accounts identified as Russia-aligned and benchmark and compared the frequency of hashtags they used in order to summarize narratives promoted by Russia-aligned accounts (Table 2). Based on the associated hashtags, we argue that posts by Russia-aligned accounts were thematically related to the November 2020 presidential election but were not necessarily supportive of Donald Trump, while the posts by benchmark accounts were often devoted to broader social issues (e.g., police reforms and the COVID-19 pandemic).

⁶ <https://help.twitter.com/en/rules-and-policies/twitter-rules>

	RUSSIA-ALIGNED ACCOUNTS	BENCHMARK ACCOUNTS
1	#maga	#endsars
2	#fbr	#sarsmustend
3	#trump2020	#endswat
4	#resist	#endsarsnow
5	#fbrparty	#endpolicebrutality
6	#bidencrimefamily	#lekkimassacre
7	#vote	#endpolicebrutalityinnigeria
8	#kag	#endsarsprotests
9	#patriots	#nigeria
10	#45	#belarus
11	#trump	#breaking
12	#veterans	#endsarsprotest
13	#np	#iran
14	#trump2020landslide	#sarsmustendnow
15	#writingcommunity	#madeinlagos
16	#joebiden	#sarsmustgonow
17	#demvoice1	#sarsmustgo
18	#biden	#endpolicebrutalityinnigera
19	#follow	#endsarsimmediately
20	#obamagate	#sars

Table 2. Hashtags frequently used by Russia-aligned and benchmark accounts. #trump2020, #trump, #trump2020landslide, #45 (the 45th president) signal support for Donald Trump in the election; #maga (make America great again) and #kag (keep America great) also related to his campaign slogan. #bidencrimefamily and #obamagate are used to express distrust in the Democratic candidate. #fbr (follow back resist), #fbrparty and #resist are used to show disapproval of Donald Trump. #sars, #endsars, #sarsmustend, #endsarsnow, #sarsmustgonow, #sarsmustgo and #endsarsimmediately are related to the ongoing COVID19 pandemic; #endswat and #endpolicebrutality are used to criticize violence by the police.

ENGAGEMENT WITH RUSSIA-ALIGNED ACCOUNTS

We found that between January and November 2020 our survey respondents referenced pro-Russian and benchmark media that we used as seed accounts (see their list in Table 1) only 37 and 1,846 times, respectively. However, the numbers were much greater with the identified Russia-aligned and the benchmark accounts: 12,259 and 37,148 times, respectively. The absolute frequency of mentions increased towards September mainly because of the retrospective data collection; the frequency increased sharply in October and fell after the election (Figure 1). The ratio of the frequency between mentions of Russia-aligned and benchmark accounts surged in February, but gradually increased until the end of September; the ratio

increased again at the end of October (Figure 2).⁷

The total number of mentions of Russia-aligned accounts during the 11 months was high, despite the fact that these accounts did not belong to celebrities (such as political leaders or pop stars): even the share of top-10 most frequently mentioned accounts was only 1-5% of total mentions. The level of partisanship expressed in the posts on political and social issues by most frequently mentioned accounts was moderate. The number of our survey respondents who engaged with the top-500 most extreme accounts was 16, which is only 1% of the sample (Figure 3).

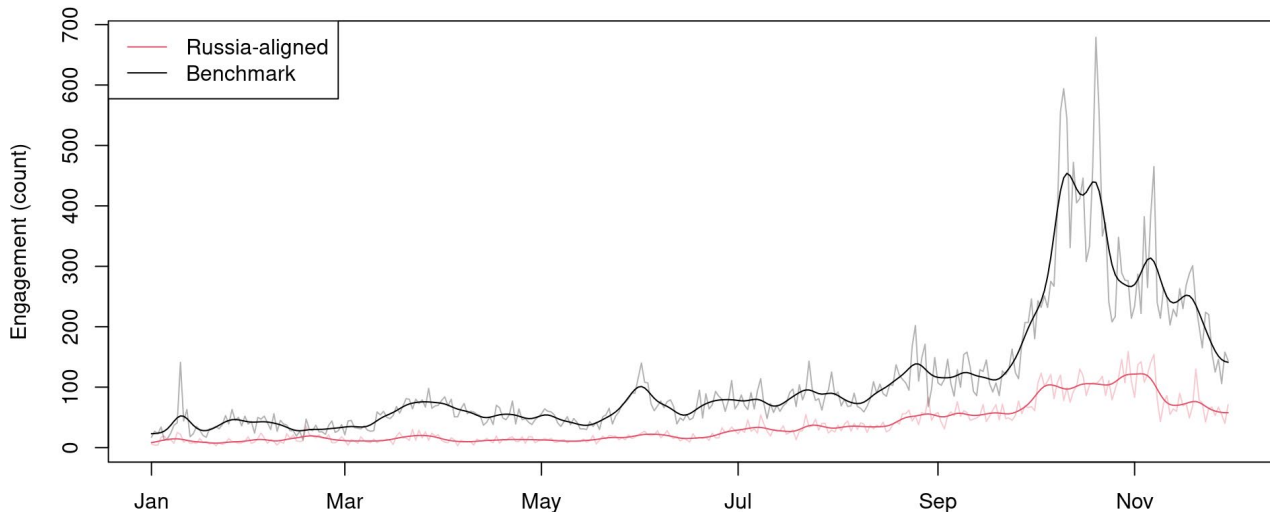


Figure 1. Engagement with Russia-aligned and benchmark accounts. Engagement with Russia-aligned accounts increased in October but fell after the November presidential election.

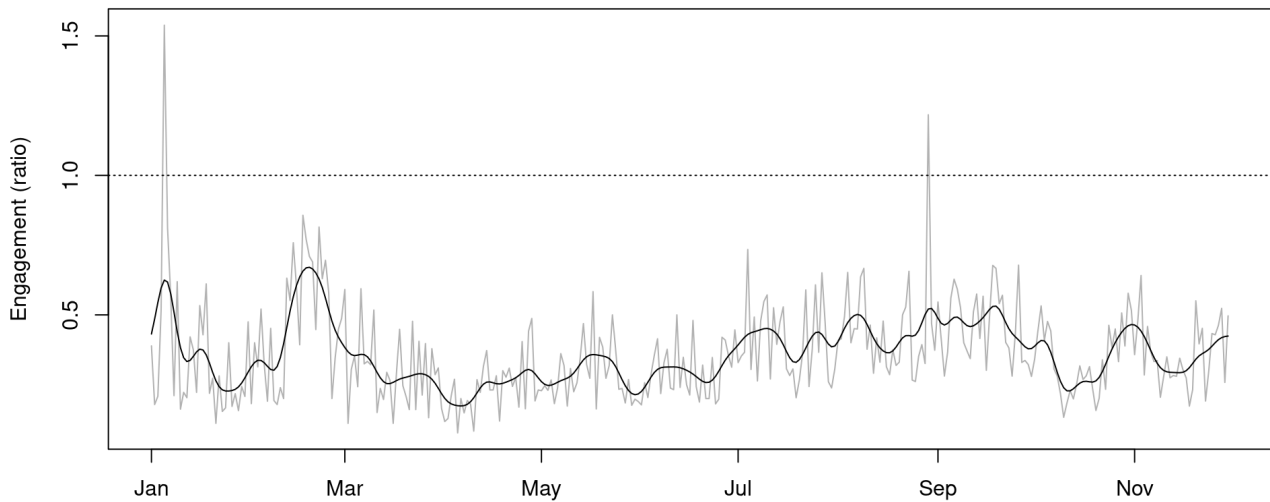


Figure 2. Ratios between engagement with Russia-aligned and benchmark accounts on Twitter. The ratio gradually increased from April to September but fell in October

7 Twitter started labeling state-affiliated accounts and excluding them from automated recommendation in users' pages in August and reportedly deleted automated accounts in October. // www.cnet.com/news/twitter-deletes-over-10k-accounts-discouraging-voting-in-midterm-elections-report-says

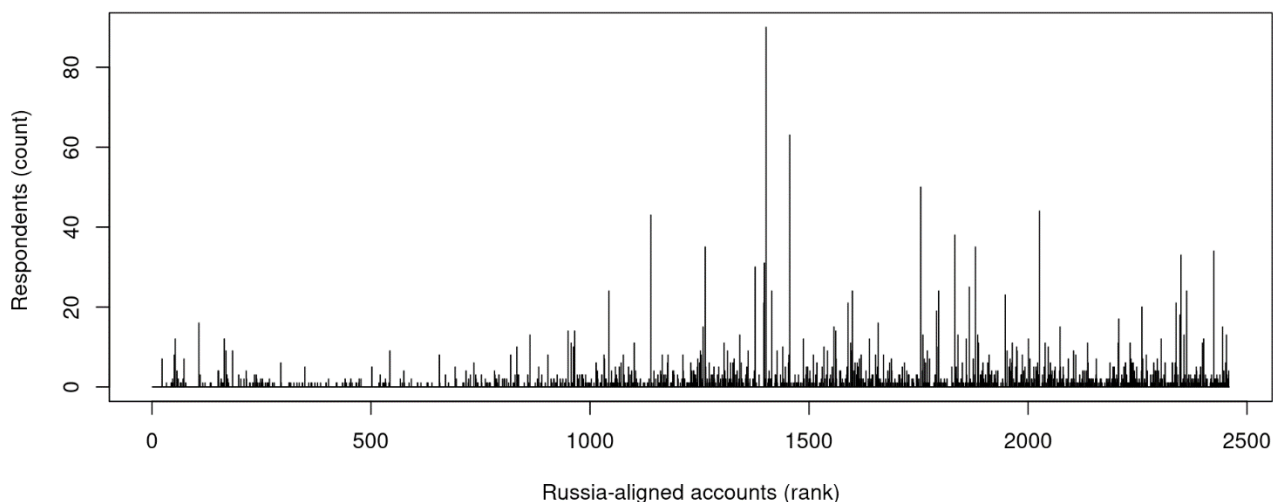


Figure 3. Frequency of mentions of Russia-aligned accounts. The accounts are sorted by their proximity to the pro-Russian seed accounts. Less than 1% of our respondents engaged with the most extreme users (left-hand side).

DISCUSSION

The results of the analysis show that, although pro-Russian media have very limited direct reach on social media, there are multiple users on Twitter who actively post partisan messages that resemble the narratives promoted by Kremlin proxies. Social media users interact with Russia-aligned accounts that frequently post divisive partisan tweets on social and political issues. These users can then be exploited by the Kremlin operations as “useful idiots” or “fellow travelers” and (unwittingly or not) help amplify narratives that benefit Russia. Although based on our analysis most of the Russia-aligned accounts our respondents interacted with were ideologically moderate, the sheer number of such Russia-aligned accounts and the frequency of engagement with them is likely to impact beliefs of those Americans who are active on social media (by, for example, making them more partisan).

While we have identified Russia-aligned accounts that were expressly supportive of Republican/Conservative politicians or skeptical about established political institutions, their influence seemed limited because they interacted with only 1% of social media users in our sample. Our data does not allow us to determine whether these accounts were actually affiliated with the Russian state agencies, but we believe many of them were not (as Twitter earlier blocked many of the accounts explicitly identified as being Kremlin-linked).

The increase in frequency of interaction with Russia-aligned accounts before the November election despite Twitter’s new actions may suggest that Russia’s collocation strategy that blurs distinctions between Kremlin proxies and ideological American citizens is successful. However, this strategy makes controlling the flow of information difficult not only for social media platforms but for pro-Kremlin actors themselves. Therefore, the extent to which they succeed in spreading disinformation on social media by having a measurable impact on electoral outcomes is questionable.

5.3 CHARACTERISTICS OF TWITTER USERS PREDICTING THEIR ENGAGEMENT WITH RUSSIA-ALIGNED ACCOUNTS

Having identified Russia-aligned accounts and frequency of our respondents' engagement with them, we correlated the resulting index of exposure to Russia-aligned content with respondents' sociodemographic and attitudinal characteristics. Those were obtained through a survey run by the Lucid Market Research Ltd. online panel (a reputable US-based online panel) between October 22nd and November 12th, 2020, around the time of the 2020 US presidential election. Participants were recruited through banners on various internet sites, via email, or via a Panel Portal to ensure the survey's high ecological validity. Most survey participants collected points that were subsequently exchanged for rewards.

We defined as "Twitter users" respondents who had a Twitter ID and active (post/share/like) on Twitter at least once a week. We analyzed Twitter handles provided by respondents and dropped those respondents who likely provided fake handles, such as celebrity Twitter handles, those with more than 10,000 followers or those that were located outside of the United States (based on their geolocation).

Ensuring sampling representativeness on Twitter is a tricky question, as no one knows exactly what a representative sample of Twitter users looks like. Because of high and non-random attrition (all respondents lacking Twitter handles, not sufficiently active on Twitter, those who provided identical Twitter handle names etc. were dropped from the analysis), we do not assume that our sample represents any well-defined population. However, to ensure that our study participants' demographic characteristics resemble the characteristics obtained from participants in other high-quality studies, we followed the below approach. First, the initial sample broadly representative of the general US population was collected by Lucid based on their Twitter users' quotas for age, gender, race, state of residence, and income representative of the US population. We used this sample for our basic analysis. Second, we also generated weights relying on a recent Pew study (Wojcik and Hughes 2019) that analyzed the characteristics of the US population on Twitter. The Pew study has found that Twitter users differ from the general US population in that they are much younger than the average American adult and are also more likely than the general public to have a college degree. To account for these differences between the general US population and Twitter users, we generated weights to make our sample comparable to the US Twitter population identified by the Pew study.

The dependent variable—frequency of engagement with Russia-aligned content on Twitter—was generated for the 21-days of the survey duration (from October 22nd to November 12th, 2020). The distribution of the dependent variable is shown in Figure 4.

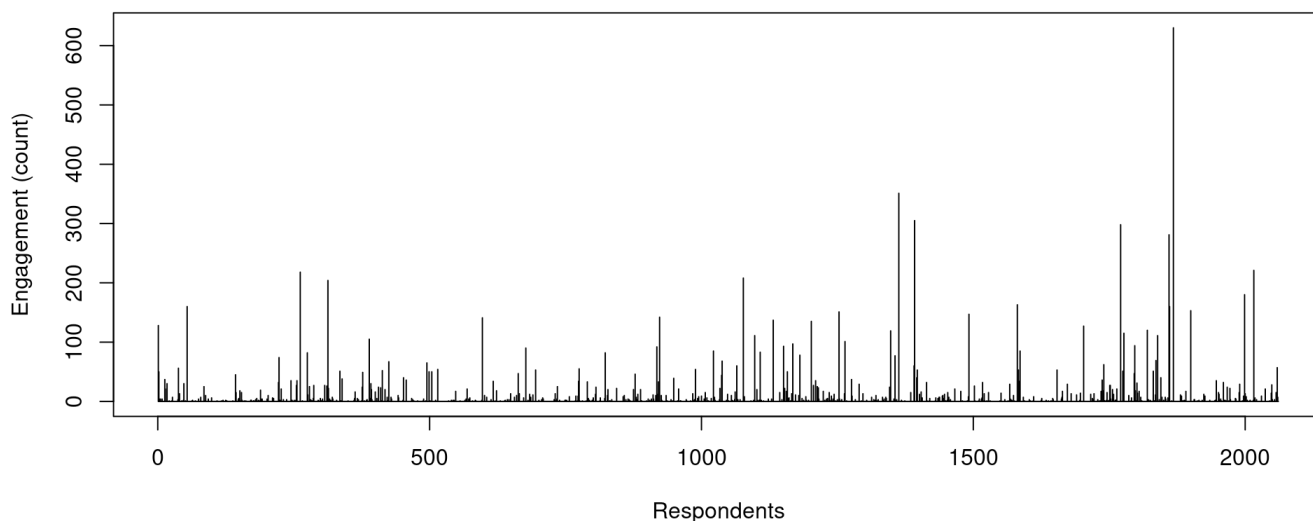


Figure 4. Dependent variable: Engagement with Russia-aligned accounts among the survey respondents

We then ran our analysis using OLS models set at the individual level on both samples with and without Pew weights to check robustness of our findings.⁸ For the robustness check we also measured our models using the binary probit model and the zero-inflated negative binomial regression (that fits the distribution of our dependent variable, where number of zeros is excessive). Most results were robust to alternative model specifications (available upon request).

Below we present the results of the analysis.

8 As to the error clustering, the primary filter we selected for sampling our respondents was pre-identified Twitter users. That by itself yields a sample that is very reflective of our target population. We did not target states specifically, so the end result across demographics (state included) could be a reflection of the prevalence of Twitter users (and further, those willing to provide accurate Twitter IDs) across subgroups. Looking at the data by state, all states are represented to a certain extent—albeit with very small numbers in some cases. For instance, Vermont and Maine have the fewest respondents of any states with just 2 each. But those numbers are not drastically different from the distribution of the US population as a whole. Those states each represent about 0.18% of the population and about 0.1% of the survey “completes.” Similarly, California’s 234 “completes” represent 11.3% of the survey, which lines up closely with the 11.9% of the US population that California represents. We therefore assumed that our respondents are fairly representatively distributed across different regions. Thus, we used robust standard errors rather than clustering errors by state of residence.

BASIC DEMOGRAPHIC CHARACTERISTICS

This section focuses on the basic demographic characteristics that identify Twitter users more likely to engage with Russia-aligned content. All regressions include a number of sociodemographic variables:

- *Gender* (male/female). “Female” gender chosen as base category.
- *Age*.
- *Quadratic age term*.
- *Race* (White / Black or African American / American Indian or Alaska Native / Asian / Pacific Islander / Some other race). “White” chosen as base category.
- *Education* (less than a high school diploma/ regular high school diploma / vocational school/ union certificate / some college, no degree/ bachelor’s degree / master’s degree / degree higher than a master’s). Degree higher than a master’s chosen as base category.
- *Household’s total income before taxes* (\$49,999-or less / \$50,000-\$74,999 / \$75,000-\$99,999 / \$100,000-\$149,999 / \$150,000 or more). “\$150,000 or more” option was chosen as base category.
- *Social class*—recorded based on answer to the question: “If you were asked to use one of four names for your social class, which would you say you belong in: the lower class, the working class, the middle class, or the upper class?” (lower class / working class / middle class / upper class). The “upper-class” option was chosen as the base category. Low socioeconomic status usually captures the interaction between low individual educational achievement and/or low household income.
- *Place of residence* a respondent lives in (a large central city / a suburb of a large central city / a medium size city (50,000 to 249,999) / a suburb of a medium size city / small city or town (10,000 to 49,999) / a town or village (2,500 to 9,999) / rural area less than 10 miles from the closest town / rural area more than 10 miles from the closest town). The “large central city” option was chosen as the base category.
- *Twitter Usage*—measured through answers to the question “How often are you on Twitter?” (the following categories ranked from 1 to 4: once a week/ several times a week/ once a day/ several times a day).

The Table 3 reports results from an OLS regression with robust standard errors using the index of engagement with Russia-aligned content as the dependent variable and including basic individual-level characteristics of respondents as explanatory variables.

	(1) Original sample	(2) Pew-weights adjusted sample
male	1.550	2.811***
	(1.215)	(1.646)
age	-0.429***	-0.490
	(0.255)	(0.351)
age squared	0.006***	0.007***
	(0.003)	(0.004)
Education:		
Less than a high school diploma	-3.011	-1.040
	(2.807)	(2.486)
Regular high school diploma	1.073	4.516
	(3.482)	(5.077)
Vocational school/ union certificate	0.930	1.648
	(3.469)	(2.814)
Some college, no degree	-0.012	0.505
	(2.556)	(2.060)
Bachelor's degree	-1.555	-1.114
	(2.136)	(1.940)
Master's degree	0.880	1.704
	(2.191)	(1.751)
Socioeconomic status:		
Lower class	5.973***	5.895***
	(2.643)	(2.467)
Working class	2.770***	2.246
	(1.671)	(1.687)
Middle class	2.033	1.906
	(1.324)	(1.284)
American Indian or Alaska Native	0.597	0.648
	(2.778)	(2.524)
Asian	5.514	7.660
	(5.023)	(7.150)
African American	3.010***	1.922
	(1.755)	(1.578)
Pacific Islander	0.514	2.802
	(3.361)	(3.938)
Some other race	-0.353	-0.838
	(1.305)	(1.630)
Medium size city (50,000 to 249,999)	-0.825	-1.021
	(1.335)	(1.381)
Place of residence:		

Suburb of a large central city	5.143***	6.552***
	(1.849)	(2.436)
Suburb of a medium size city	2.338	1.504
	(1.653)	(1.549)
Town or village (2,500 to 9,999)	3.887	3.903
	(3.133)	(3.125)
Rural area < 10 miles from the closest town	2.595	3.035
	(2.333)	(2.433)
Rural area > 10 miles from the closest town	-2.101	-0.943
	(1.726)	(1.957)
Small city or town (10,000 to 49,999)	3.446***	3.258***
	(1.950)	(1.648)
Income		
below -\$49,999	1.223	-0.150
	(2.514)	(2.748)
\$50,000-\$74,999	-0.339	-1.089
	(2.358)	(2.313)
\$75,000-\$99,999	1.459	3.300
	(2.720)	(3.809)
\$100,000-\$149,999	-0.429	-0.458
	(1.962)	(1.962)
Twitter Usage Frequency	4.057***	3.652***
	(0.521)	(0.494)
Constant	-8.699	-6.683
	(6.087)	(7.726)
Observations	2,048	2,048
R-squared	0.0381	0.0378

*** p<0.1, ** p<0.01, * p<0.05

Table 3. OLS regression model explaining engagement with Russia-Aligned Accounts (Basic Demographic Characteristics)

Looking at the results in Table 4, there are several demographic characteristics positively correlated with engagement with Russia-aligned users (however, not all are robust to alternative sample specification).

Gender: male respondents tend to be more exposed to Russia-aligned content (however, the effect of gender is only significant for Pew-weights adjusted sample). This might have to do with the fact that the male gender may be associated with higher odds of radicalization, as other studies have shown (Givens, 2004).

Age: interestingly, in our sample, younger age, as well as quadratic age term, positively correlates with frequency of engagement with Russia-aligned accounts. This might suggest that both older and younger respondents are more likely to engage with such content (although the impact is fairly small based on the size of the coefficient).

Socioeconomic status: respondents with lower socioeconomic status (subject-

tive measure) tend to more frequently engage with Russia-aligned content. This effect remains consistent when we adjust for weights.

Race: the African-Americans in our sample are more likely to engage with Russia-aligned content although the coefficient is only significant for the original sample and disappears when we adjust for Pew weights. This finding is consistent with earlier studies that emphasized that the Kremlin proxies have consistently targeted the African-American groups in an effort to polarize existing social divisions in the United States (see Chapter 4.1).

Place of residence: respondents residing in suburbs of large cities or in small towns are more likely to engage with Russia-aligned content.

Twitter Usage Frequency: ultimately, more frequent engagement with Twitter predictably significantly increases a respondent's odds to encounter Russia-aligned content.

Contrary to earlier studies (Chapter 4.1), we do not find effects of other factors such as education or lower income on engagement with Russia-aligned content. In the Appendix III we provide the same analysis including fixed controls for days of engagement (over an observed period of 21 days). The main conclusions remain unchanged to the inclusion of fixed day effects.

Overall, while we find that respondents' subjective perception of their socioeconomic status is clearly related to the engagement with Russia-aligned content, objective indicators of their status (education and income) are not related. This implies that the cultivation of grievances in social media is grounded in cultural and psychological dimensions (e.g. institutional trust and media trust). For example, if new policies improved the current economic crisis conditions and stopped the trend toward greater income inequality, this would not necessarily hinder the work of IRA et al.

IDEOLOGY

As our next step, we focus on the role of the respondents' political ideology in predicting engagement with Russia-aligned content. As described in Chapter 4.1, studies have consistently demonstrated that partisanship plays a significant role in explaining engagement with disinformation.

In this section, as a measure of respondents' political ideology we used the question "Where would you place yourself on a scale from 1 to 7 where 1 means very liberal and 7 means very conservative?" The responses, ranging from 1 to 7, were ranked as follows: 1 Very liberal / 2 Liberal / 3 Somewhat liberal / 4 Middle of the road / 5 Somewhat conservative / 6 Conservative / 7 Very conservative. Given that stronger political ideology is expected to predict higher engagement with Russia's disinformation, we chose the middle option "4" Middle of the road, as our base category.

The results are presented in Table 4.

	(1)	(2)
	Original sample	Pew-weights adjusted sample
Very liberal	3.851***	4.104***
	(1.800)	(1.793)
Liberal	2.115	4.879
	(2.762)	(5.349)
Somewhat liberal	-0.123	-0.878
	(1.457)	(1.593)
Somewhat conservative	-2.544***	-2.218***
	(1.146)	(1.172)
Conservative	1.743	2.584
	(1.974)	(2.122)
Very conservative	4.677***	4.029
	(2.805)	(2.449)
male	1.657	2.769***
	(1.197)	(1.504)
age	-0.384	-0.439
	(0.254)	(0.347)
age squared	0.006***	0.006***
	(0.003)	(0.004)
Bachelor's degree	-0.678	0.070
	(2.095)	(1.722)
Less than a high school diploma	0.271	2.644
	(2.984)	(2.702)
Master's degree	0.884	1.895
	(2.196)	(1.780)
Regular high school diploma	2.494	6.231
	(3.821)	(5.826)
Some college, no degree	1.422	2.096
	(2.528)	(2.089)
Vocational school/ union certificate	2.848	3.829
	(3.569)	(3.144)
American Indian or Alaska Native	0.970	1.291
	(2.676)	(2.352)
Asian	5.750	8.178
	(5.254)	(7.556)
African American	2.988***	1.733
	(1.808)	(1.675)
Pacific Islander	-1.208	-0.156

	(4.070)	(3.027)
Some other race	-0.990	-1.607
	(1.356)	(1.830)
Medium size city (50,000 to 249,999)	-0.331	-0.549
	(1.359)	(1.300)
Suburb of a large central city	5.543***	7.012***
	(1.920)	(2.658)
Suburb of a medium size city	2.560	1.759
	(1.698)	(1.583)
Town or village (2,500 to 9,999)	3.414	3.453
	(3.112)	(3.108)
Rural area < 10 miles from the closest town	2.823	3.273
	(2.446)	(2.536)
Rural area > 10 miles from the closest town	-2.086	-0.794
	(1.771)	(2.091)
Small city or town (10,000 to 49,999)	3.909***	3.957***
	(2.027)	(1.743)
below -\$49,999	2.855	1.283
	(2.507)	(3.019)
\$50,000-\$74,999	0.599	-0.467
	(2.337)	(2.468)
\$75,000-\$99,999	2.511	4.211
	(2.651)	(3.684)
\$100,000-\$149,999	0.173	-0.101
	(1.990)	(2.057)
Twitter Usage Frequency	3.867***	3.514***
	(0.515)	(0.496)
Constant	-9.949***	-8.773
	(5.805)	(6.931)
Observations	2,019	2,019
R-squared	0.042	0.043

*** p<0.1, ** p<0.01, * p<0.05

Table 4. OLS regression model explaining engagement with Russia-Aligned Users (Ideology)

The results in Table 4 suggest that respondents on both sides of the political spectrum indeed tend to show higher engagement with our measures of Russia-aligned content. Respondents who describe themselves as “Very Liberal” and “Very Conservative” tend to interact with Russia-aligned content more frequently, as compared to respondents who describe themselves as centrists (“Middle of the Road.”) This finding is consistent with earlier studies that have identified partisanship

as one of the key predictors of higher engagement with disinformation (see Chapter 4.1). While the ideological spectrum overlaps with partisanship, it's important to keep in mind that, in the US two-party system, each party has its own ideological spectrum. When ideological differences are exploited by Russia-aligned content, it might make it harder for each party to govern internally, in addition to making the country as a whole more polarized.

Similarly, Table 4 demonstrates a consistent association between the demographic characteristics described earlier and the engagement with Russia-aligned content, including place of residence, quadratic age term, gender, and race. The inclusion of controls for days of the survey does not alter these results (Appendix IV).

TRUST IN MEDIA AND INSTITUTIONS

Studies have demonstrated that higher propensity to believe in disinformation may be associated with lower trust in mainstream media (see Chapter 4.1). To test this hypothesis, we included in our analysis measures of media trust. To compose the trust in media variable we asked respondents whether they agreed with the following four statements:

- *The news media pay enough attention to important political topics.*
- *Over time most news media reporting is pretty accurate.*
- *In presenting the news dealing with political and social issues, news organizations deal fairly with all sides.*
- *The mainstream media is more interested in making money than telling the truth.*

Subsequently, we correlated the resulting (1–4 scale, 1 = “not at all,” 2 = “not very much,” 3 = “somewhat,” 4 = “completely”) variables to construct a cumulative media trust index based on factor analysis. The variables were recorded so that a higher value on the index is associated to a higher degree of media trust.

Higher propensity to engage with Russia-aligned content may also be associated with lower levels of institutional trust (Chapter 4.1). To control for this possibility, we also included in our analysis the index of institutional trust. To build this index we asked respondents how much confidence they had in the list of the below institutions (not at all, not very much, somewhat, completely):

- *Major news organizations*
- *Judicial institutions like Supreme Court*
- *Ivy League universities*
- *Global corporations*
- *International organizations like the United Nations (the UN), the World Trade Organization (the WTO), World Bank*
- *World Health Organization (WHO)*
- *The two main political parties*
- *Elected officials in Washington*
- *U.S. police*
- *U.S. military*

Subsequently, we correlated the resulting (1–4 scale, 1 = “not at all,” 2 = “not very much,” 3 = “somewhat,” 4 = “completely”) variables to construct a cumulative index institutional trust. Higher value on the index is associated with a higher degree institutional trust.

Next, we regressed the resulting indicators of media and institutional trust on our indicator of respondents’ engagement with Russia-aligned content. The results of the analysis are presented in Table 5.

	(1) Original sample	(2) Pew-weights	(3) Original sample	(4) Pew-weights	(5) Original sample	(6) Pew-weights
Media trust	-1.525*** (0.598)	-1.500*** (0.574)			-0.128 (0.741)	-0.564 (0.915)
Institutional trust			-2.435*** (0.613)	-1.904*** (0.673)	-2.361*** (0.761)	-1.582 (1.007)
Very liberal	4.163*** (1.807)	4.367*** (1.814)	3.672*** (1.810)	4.017*** (1.808)	3.704*** (1.854)	4.130*** (1.895)
Liberal	2.463 (2.789)	5.154 (5.386)	2.319 (2.744)	5.017 (5.327)	2.342 (2.813)	5.097 (5.426)
Somewhat liberal	0.154 (1.460)	-0.719 (1.590)	-0.217 (1.446)	-1.030 (1.571)	-0.190 (1.458)	-0.944 (1.532)
Somewhat conservative	-3.125*** (1.161)	-2.768*** (1.154)	-2.629*** (1.158)	-2.259*** (1.180)	-2.675*** (1.120)	-2.459*** (1.089)
Conservative	0.800 (1.890)	1.673 (2.000)	1.880 (1.963)	2.784 (2.099)	1.797 (1.875)	2.407 (1.887)
Very conservative	3.722 (2.648)	3.128 (2.288)	4.927*** (2.798)	4.340*** (2.439)	4.840*** (2.671)	3.949*** (2.276)
male	1.620 (1.194)	2.743*** (1.499)	1.448 (1.192)	2.613*** (1.525)	1.451 (1.194)	2.629*** (1.541)
age	-0.364 (0.255)	-0.427 (0.346)	-0.372 (0.255)	-0.436 (0.348)	-0.370 (0.254)	-0.432 (0.344)
age squared	0.006*** (0.003)	0.006*** (0.004)	0.006*** (0.003)	0.006 (0.004)	0.006*** (0.003)	0.006 (0.004)
Bachelor's degree	-0.849 (2.068)	-0.191 (1.726)	-0.745 (2.056)	-0.109 (1.695)	-0.758 (2.059)	-0.177 (1.716)
Less than a high school diploma	-0.539 (2.956)	1.794 (2.659)	-0.030 (2.936)	2.324 (2.678)	-0.089 (2.904)	2.058 (2.595)
Master's degree	0.983 (2.167)	1.929 (1.776)	1.445 (2.165)	2.225 (1.771)	1.436 (2.166)	2.182 (1.773)
Regular high school diploma	2.253 (3.795)	5.830 (5.773)	2.288 (3.805)	5.841 (5.909)	2.274 (3.789)	5.757 (5.814)
Some college, no degree	1.021 (2.483)	1.571 (2.047)	1.103 (2.488)	1.641 (2.072)	1.079 (2.475)	1.521 (2.037)
Vocational school/ union certificate	2.519 (3.524)	3.313 (3.087)	2.910 (3.537)	3.641 (3.146)	2.881 (3.500)	3.478 (3.035)
American Indian / Alaska Native	0.970 (2.606)	1.259 (2.283)	0.758 (2.608)	0.954 (2.289)	0.764 (2.607)	0.999 (2.281)

The Kremlin's Social Media Influence inside the United States: A Moving Target

Asian	5.591	8.001	5.888	8.232	5.871	8.157
	(5.242)	(7.532)	(5.252)	(7.558)	(5.212)	(7.467)
African American	3.172***	1.903	2.751	1.510	2.774	1.611
	(1.803)	(1.664)	(1.774)	(1.634)	(1.739)	(1.574)
Pacific Islander	-1.550	-0.418	-1.687	-0.160	-1.701	-0.258
	(4.225)	(3.208)	(5.547)	(4.156)	(5.514)	(4.030)
Some other race	-1.198	-1.750	-1.756	-2.128	-1.750	-2.094
	(1.374)	(1.844)	(1.395)	(1.775)	(1.392)	(1.747)
Medium size city	-0.643	-0.853	-1.101	-1.179	-1.104	-1.187
	(1.360)	(1.318)	(1.409)	(1.273)	(1.406)	(1.276)
Suburb of a large central city	5.144***	6.603***	4.841***	6.385***	4.828***	6.337***
	(1.865)	(2.594)	(1.928)	(2.771)	(1.896)	(2.716)
Suburb of a medium size city	2.168	1.365	1.866	1.264	1.854	1.200
	(1.702)	(1.612)	(1.720)	(1.550)	(1.714)	(1.579)
Town or village (2,500 to 9,999)	2.933	3.050	2.463	2.776	2.451	2.738
	(3.063)	(3.058)	(3.081)	(3.050)	(3.070)	(3.041)
Rural area < 10 miles from town	2.211	2.558	2.153	2.609	2.121	2.452
	(2.499)	(2.594)	(2.514)	(2.613)	(2.511)	(2.611)
Rural area > 10 miles from town	-2.630	-1.273	-2.810	-1.312	-2.834	-1.404
	(1.827)	(2.100)	(1.905)	(2.229)	(1.876)	(2.157)
Small city or town	3.584***	3.622***	3.174	3.362***	3.168	3.337***
	(2.028)	(1.757)	(2.078)	(1.824)	(2.072)	(1.817)
below -\$49,999	2.379	0.906	1.397	0.285	1.401	0.312
	(2.509)	(3.048)	(2.401)	(2.833)	(2.395)	(2.806)
\$50,000-\$74,999	0.284	-0.694	-0.518	-1.206	-0.511	-1.167
	(2.337)	(2.484)	(2.291)	(2.372)	(2.284)	(2.341)
\$75,000-\$99,999	2.091	3.833	1.572	3.585	1.565	3.548
	(2.633)	(3.645)	(2.703)	(3.814)	(2.692)	(3.776)
\$100,000-\$149,999	-0.182	-0.441	-0.560	-0.648	-0.567	-0.684
	(2.016)	(2.097)	(1.983)	(2.025)	(1.995)	(2.047)
Twitter Usage Frequency	3.960***	3.608***	3.990***	3.608***	3.994***	3.627***
	(0.526)	(0.503)	(0.532)	(0.513)	(0.530)	(0.507)
Constant	-9.720***	-8.316	-8.504	-7.419	-8.528	-7.476
	(5.795)	(6.949)	(5.675)	(6.651)	(5.669)	(6.609)
Observations	2,019	2,019	2,019	2,019	2,019	2,019
R-squared	0.044	0.045	0.048	0.046	0.048	0.046

*** p<0.1, ** p<0.01, * p<0.05

Table 5. OLS regression model explaining engagement with Russia-Aligned Users (Trust in Media)

The results demonstrate that trust in media and trust in institutions both are negatively correlated to the engagement with Russia aligned content, i.e., respondents in our sample with lower levels of institutional and media trust tend to be more engaged with Russia-aligned content. For every one-unit decrease in media trust, the predicted value of engagement with Russia-aligned media increases by about 1.5 times. For every one-unit decrease in institutional trust, the predicted value of engagement with Russia-aligned media increases about twofold.

That inclusion of the media trust variable eliminates the independent effect of ideology (being very conservative) on propensity to engage with Russia-aligned content, suggesting that for conservative respondents these effects may be mediated through trust in mainstream media (in fact, an interaction between the ideology variable and media trust variable confirms this – the interaction is significant for “very conservative” respondents; the results are available upon request).

Similarly, we also find that including the institutional trust variable tends to eliminate the independent effect of race, which suggests that higher propensity to engage with Russia-aligned content for African-Americans on Twitter might be associated with lower levels of institutional trust (although in this case we only find a significant interaction between race and police and military rather than other institutions; the results are available upon request).

When both trust measures are included together, the institutional trust coefficient remains significant (except in the model with pew sample weights) while the effect of media trust disappears, likely because the institutional trust variable already includes media trust indicators. The change in significance of the coefficient to the media trust variable may hence have to do with endogeneity issues.

This finding is also in line with other studies that have found that people skeptical about traditional news media and other institutions are more prone to engage with disinformation (Zimmermann and Kohring, 2020; Gauchat, 2012; Jones, 2004; Kraft, Lodge, and Taber, 2014; Lee, 2005; Pew Research Center, 2017; van der Linden, Panagopoulos, and Roozenbeek, 2020 and Chapter 3). Feeling betrayed by traditional institutions and media, such people often turn to alternative information sources, which in turn further alienate them from mainstream institutions, creating a vicious circle. Our findings provide some empirical support for the argument that disinformation spreads due to an erosion of institutional trust and trust in media, which leads respondents to form an opposition to the established information system (Bennett and Livingston, 2018).

IMPACT OF ENGAGEMENT WITH RUSSIA-ALIGNED ACCOUNTS ON VOTING BEHAVIOR

In our last section we examine the impact of the engagement with Russia-aligned content on voting intentions of our respondents. As described in Chapter 4.2, studies of the impact of Russia’s influence operations on voting intentions tend to return mixed results.

In this section, we have asked our respondents several measures of respondents’ voting intentions. First, we posed a question on the respondents’ willingness to take part in the election: “Are you planning to vote, or have you already voted, in the 2020 presidential election?” The responses were as follows: “Yes” / “No” / “Don’t Know.”

Given the binary nature of the dependent variable we used probit model in this specification. Table 6 reports results from a probit regression with robust standard errors using the engagement with Russia-aligned content and basic individual-level characteristics of respondents as explanatory variables.

Are you planning to vote, or have you already voted, in the 2020 presidential election?	(1) Original sample	(2) Marginal effects	(3) Pew-weights	(4) Marginal effects
Engagement with Russia-aligned content	0.006***	0.001***	0.004	0.000
	(0.003)	(0.000)	(0.003)	(0.000)
male	-0.036	-0.004	0.020	0.002
	(0.096)	(0.011)	(0.100)	(0.012)
age	0.023	0.001***	0.034***	0.001***
	(0.019)	(0.001)	(0.020)	(0.001)
age squared	-0.000		-0.000	
	(0.000)		(0.000)	
Bachelor's degree	0.195	0.022	0.257	0.031
	(0.325)	(0.041)	(0.336)	(0.047)
Less than a high school diploma	-0.906***	-0.194***	-0.770***	-0.165***
	(0.402)	(0.084)	(0.411)	(0.085)
Master's degree	0.366	0.037	0.369	0.041
	(0.358)	(0.042)	(0.368)	(0.048)
Regular high school diploma	-0.110	-0.015	0.002	0.000
	(0.346)	(0.045)	(0.358)	(0.050)
Some college, no degree	0.051	0.006	0.143	0.018
	(0.333)	(0.042)	(0.344)	(0.048)
Vocational school/ union certificate	0.150	0.017	0.350	0.039
	(0.389)	(0.047)	(0.397)	(0.050)
American Indian / Alaska Native	-0.368	-0.049	-0.358	-0.047
	(0.257)	(0.041)	(0.252)	(0.040)
Asian	-0.468***	-0.066***	-0.428***	-0.059***
	(0.167)	(0.029)	(0.169)	(0.028)
African American	-0.162	-0.019	-0.234***	-0.029
	(0.131)	(0.016)	(0.139)	(0.018)
Some other race	-0.213	-0.025	-0.042	-0.005
	(0.214)	(0.029)	(0.237)	(0.026)
Very liberal	0.404***	0.049***	0.441***	0.055***
	(0.144)	(0.016)	(0.146)	(0.017)
Liberal	0.487***	0.056***	0.519***	0.062***
	(0.162)	(0.016)	(0.173)	(0.018)
Somewhat liberal	0.066	0.010	0.134	0.020
	(0.137)	(0.020)	(0.151)	(0.022)
Somewhat conservative	0.257	0.034	0.382***	0.049***
	(0.179)	(0.021)	(0.185)	(0.021)
Conservative	0.334***	0.042***	0.387***	0.050***
	(0.188)	(0.021)	(0.192)	(0.021)
Very conservative	0.396***	0.048***	0.412***	0.052***
	(0.183)	(0.019)	(0.187)	(0.021)
Medium size city	-0.083	-0.009	-0.064	-0.006
	(0.161)	(0.017)	(0.169)	(0.017)
Suburb of a large central city	-0.171	-0.019	-0.214	-0.024
	(0.138)	(0.016)	(0.144)	(0.016)
Suburb of a medium size city	-0.195	-0.022	-0.264	-0.031

	(0.166)	(0.020)	(0.177)	(0.022)
Town or village (2,500 to 9,999)	-0.388***	-0.050	-0.437***	-0.057
	(0.212)	(0.032)	(0.238)	(0.037)
Rural area < 10 miles from town	0.259	0.021	0.123	0.011
	(0.238)	(0.018)	(0.231)	(0.020)
Rural area > 10 miles from town	0.077	0.007	-0.132	-0.014
	(0.260)	(0.024)	(0.270)	(0.031)
Small city or town	-0.206	-0.024	-0.256***	-0.030
	(0.153)	(0.018)	(0.154)	(0.019)
below -\$49,999	-0.576***	-0.058***	-0.739***	-0.075***
	(0.257)	(0.019)	(0.256)	(0.018)
\$50,000-\$74,999	-0.293	-0.024	-0.408	-0.032***
	(0.272)	(0.019)	(0.268)	(0.018)
\$75,000-\$99,999	-0.036	-0.002	-0.202	-0.013
	(0.285)	(0.018)	(0.283)	(0.018)
\$100,000-\$149,999	-0.196	-0.015	-0.312	-0.022
	(0.296)	(0.021)	(0.291)	(0.020)
Twitter Usage Frequency	0.105***	0.012***	0.092***	0.011***
	(0.048)	(0.006)	(0.052)	(0.006)
Constant	0.937		0.802	
	(0.588)		(0.625)	
Observations	1,981	1,981	1,981	1,981
r2_p	0.135	.	0.155	.

*** p<0.1, ** p<0.01, * p<0.05

Table 6. Probit regression model: predictor of willingness to take part in November 2020 election

The results indicate that higher engagement with Russia-aligned content predicts stronger willingness to vote in the election, although this effect is fairly small and disappears following the inclusion of Pew sample-based weights.⁹ This correlation between the Russia-aligned content and voting intentions may be related to the fact that our measure of Russia-aligned content corresponds to more partisan messages on both sides of the US political spectrum. Stronger partisan messaging may correspond to higher mobilization, which was higher among both liberals and conservatives in the November 2020 US election.

Next, we looked at specific voting preferences of our respondents by asking them which candidate they supported in the election: "For whom do you plan to (or have) vote(d) for in this 2020 presidential race?" The responses were as follows: "Donald Trump" / "Joe Biden" / "Another candidate" / "Don't plan to vote" / "Don't know." Given the binary nature of the dependent variable we used probit model in this specification. Table 7 reports the results of this analysis for those re-

9 Respondents who engaged with Russia-aligned content 10 times had an only 1% increase in the chance that the respondents would cast a vote when weighted by the Pew sample. The overall impact of Russia-aligned content engagement is small as our respondents engaged with such content 6 times on average between January and November. However 1% of respondents engaged with Russia-aligned content more than 100 times in the period, which increased their chance to cast vote by 10%.

spondents who said they will vote for Donald Trump in November 2020 election

The Kremlin's Social Media Influence Inside the United States: A Moving Target

	(1)	(2)	(3)	(4)
"For whom do you plan to (or have) vote(d) for in this 2020 presidential race? Donald Trump	Original sample	Marginal effects	Pew-weights	Marginal effects
Engagement with Russia-aligned content	-0.000	-0.000	-0.000	-0.000
	(0.001)	(0.000)	(0.001)	(0.000)
male	-0.155***	-0.037***	-0.110	-0.026
	(0.070)	(0.017)	(0.073)	(0.017)
age	0.052***	0.001***	0.055***	0.001***
	(0.014)	(0.001)	(0.015)	(0.001)
age squared	-0.001***		-0.001***	
	(0.000)		(0.000)	
Bachelor's degree	0.212	0.048	0.245	0.056
	(0.215)	(0.046)	(0.225)	(0.049)
Less than a high school diploma	-0.241	-0.048	-0.242	-0.049
	(0.355)	(0.070)	(0.355)	(0.071)
Master's degree	0.102	0.022	0.110	0.025
	(0.220)	(0.047)	(0.228)	(0.050)
Regular high school diploma	0.361	0.084	0.410***	0.098***
	(0.232)	(0.051)	(0.243)	(0.055)
Some college, no degree	0.239	0.054	0.224	0.051
	(0.221)	(0.048)	(0.232)	(0.051)
Vocational school/ union certificate	0.386	0.090	0.381	0.090
	(0.257)	(0.058)	(0.266)	(0.061)
American Indian / Alaska Native	-0.056	-0.014	-0.126	-0.032
	(0.283)	(0.070)	(0.264)	(0.064)
Asian	-0.194	-0.047	-0.147	-0.037
	(0.150)	(0.035)	(0.152)	(0.037)
African American	-0.639***	-0.139***	-0.593***	-0.132***
	(0.128)	(0.024)	(0.129)	(0.026)
Some other race	-0.354***	-0.083***	-0.357***	-0.085***
	(0.209)	(0.045)	(0.208)	(0.045)
Very liberal	-0.626***	-0.141***	-0.587***	-0.135***
	(0.111)	(0.023)	(0.114)	(0.024)
Liberal	-0.583***	-0.134***	-0.570***	-0.132***
	(0.127)	(0.026)	(0.134)	(0.028)
Somewhat liberal	-0.671***	-0.148***	-0.632***	-0.142***
	(0.134)	(0.025)	(0.141)	(0.027)

Somewhat conservative	0.811 ***	0.282 ***	0.791 ***	0.275 ***
	(0.116)	(0.041)	(0.122)	(0.043)
Conservative	1.190 ***	0.420 ***	1.205 ***	0.426 ***
	(0.113)	(0.038)	(0.119)	(0.040)
Very conservative	1.447 ***	0.504 ***	1.442 ***	0.503 ***
	(0.120)	(0.037)	(0.123)	(0.038)
Medium size city	0.033	0.008	0.046	0.011
	(0.127)	(0.029)	(0.136)	(0.032)
Suburb of a large central city	0.191 ***	0.045 ***	0.196 ***	0.047 ***
	(0.100)	(0.023)	(0.104)	(0.025)
Suburb of a medium size city	0.051	0.012	0.062	0.014
	(0.129)	(0.029)	(0.136)	(0.031)
Town or village (2,500 to 9,999)	0.195	0.046	0.200	0.048
	(0.151)	(0.036)	(0.155)	(0.038)
Rural area < 10 miles from town	0.257 ***	0.061 ***	0.248 ***	0.060
	(0.149)	(0.036)	(0.150)	(0.037)
Rural area > 10 miles from town	0.569 ***	0.144 ***	0.472 ***	0.119 ***
	(0.211)	(0.057)	(0.227)	(0.061)
Small city or town	0.293 ***	0.070 ***	0.320 ***	0.078 ***
	(0.122)	(0.030)	(0.133)	(0.033)
below -\$49,999	-0.374 ***	-0.091 ***	-0.392 ***	-0.097 ***
	(0.142)	(0.036)	(0.144)	(0.037)
\$50,000-\$74,999	-0.296 ***	-0.073 ***	-0.317 ***	-0.080 ***
	(0.151)	(0.038)	(0.151)	(0.039)
\$75,000-\$99,999	-0.074	-0.019	-0.106	-0.028
	(0.154)	(0.040)	(0.155)	(0.041)
\$100,000-\$149,999	-0.139	-0.036	-0.146	-0.038
	(0.158)	(0.041)	(0.157)	(0.041)
Twitter Usage Frequency	-0.042	-0.010	-0.039	-0.009
	(0.036)	(0.009)	(0.038)	(0.009)
Constant	-1.553 ***		-1.673 ***	
	(0.417)		(0.434)	
Observations	2,017	2,017	2,017	2,017
r ² _p	0.295	.	0.285	.

*** p<0.1, ** p<0.01, * p<0.05

Table 7. Probit regression model: predictor of voting for Donald Trump to take part in November 2020 election

The Table 8 reports the results of this analysis for those respondents who said they would vote for Joe Biden in November 2020 election.

"For whom do you plan to (or have) vote(d) for in this 2020 presidential race? Joe Biden	(1) Original sample	(2) Marginal effects	(3) Pew- weights	(4) Marginal effects
Engagement with Russia-aligned content	0.001 (0.001)	0.000 (0.000)	0.001 (0.001)	0.000 (0.000)
male	0.112*** (0.065)	0.033*** (0.019)	0.090 (0.068)	0.027 (0.020)
age	-0.031*** (0.013)	-0.000 (0.001)	-0.028*** (0.014)	-0.000 (0.001)
age squared	0.000*** (0.000)		0.000*** (0.000)	
Bachelor's degree	-0.271 (0.204)	-0.076 (0.055)	-0.288 (0.213)	-0.082 (0.058)
Less than a high school diploma	-0.898*** (0.314)	-0.265*** (0.091)	-0.962*** (0.332)	-0.290*** (0.098)
Master's degree	-0.124 (0.209)	-0.034 (0.056)	-0.130 (0.218)	-0.036 (0.060)
Regular high school diploma	-0.494*** (0.220)	-0.142*** (0.060)	-0.500*** (0.230)	-0.147*** (0.064)
Some college, no degree	-0.436*** (0.209)	-0.124*** (0.056)	-0.399*** (0.220)	-0.116*** (0.061)
Vocational school/ union certificate	-0.376 (0.249)	-0.106 (0.069)	-0.342 (0.257)	-0.099 (0.073)
American Indian / Alaska Native	-0.313 (0.238)	-0.095 (0.073)	-0.241 (0.233)	-0.074 (0.072)
Asian	-0.012 (0.132)	-0.004 (0.039)	-0.031 (0.137)	-0.010 (0.042)
African American	0.282*** (0.102)	0.081*** (0.029)	0.229*** (0.104)	0.068*** (0.030)
Some other race	0.149 (0.176)	0.044 (0.051)	0.196 (0.193)	0.058 (0.056)
Very liberal	0.751*** (0.097)	0.244*** (0.029)	0.707*** (0.103)	0.233*** (0.031)
Liberal	0.867*** (0.109)	0.271*** (0.030)	0.808*** (0.119)	0.258*** (0.034)
Somewhat liberal	0.549*** (0.105)	0.188*** (0.034)	0.542*** (0.113)	0.186*** (0.036)

Somewhat conservative	-0.663*** (0.117)	-0.247*** (0.041)	-0.595*** (0.125)	-0.223*** (0.045)
Conservative	-0.943*** (0.115)	-0.338*** (0.036)	-0.959*** (0.120)	-0.341*** (0.038)
Very conservative	-1.247*** (0.124)	-0.418*** (0.033)	-1.240*** (0.127)	-0.414*** (0.034)
Medium size city	0.002 (0.114)	0.001 (0.033)	0.010 (0.123)	0.003 (0.036)
Suburb of a large central city	-0.284*** (0.091)	-0.084*** (0.027)	-0.305*** (0.097)	-0.092*** (0.029)
Suburb of a medium size city	-0.075 (0.116)	-0.022 (0.033)	-0.097 (0.123)	-0.029 (0.037)
Town or village (2,500 to 9,999)	-0.328*** (0.148)	-0.097*** (0.045)	-0.330*** (0.178)	-0.100*** (0.055)
Rural area < 10 miles from town	-0.222*** (0.134)	-0.065 (0.040)	-0.299*** (0.137)	-0.090*** (0.042)
Rural area > 10 miles from town	-0.402*** (0.194)	-0.120*** (0.059)	-0.415*** (0.208)	-0.127*** (0.065)
Small city or town	-0.352*** (0.109)	-0.104*** (0.033)	-0.413*** (0.115)	-0.126*** (0.035)
below -\$49,999	0.067 (0.135)	0.020 (0.040)	0.052 (0.139)	0.016 (0.042)
\$50,000-\$74,999	0.261*** (0.143)	0.076*** (0.042)	0.248*** (0.144)	0.073*** (0.043)
\$75,000-\$99,999	0.065 (0.145)	0.019 (0.043)	0.001 (0.148)	0.000 (0.045)
\$100,000-\$149,999	0.097 (0.150)	0.029 (0.044)	0.086 (0.149)	0.026 (0.045)
Twitter Usage Frequency	0.096*** (0.033)	0.028*** (0.010)	0.084*** (0.035)	0.025*** (0.010)
Constant	0.708*** (0.378)		0.760*** (0.398)	
Observations	2,017	2,017	2,017	2,017
r ² _p	0.235	.	0.221	.

*** p<0.1, ** p<0.01, * p<0.05

Table 8. Probit regression model: predictor of voting for Joe Biden to take part in November 2020 election

Overall, we do not find a significant impact of engagement with Russia-aligned content on respondents' propensity to support Donald Trump or Joe Biden. This might be partly because Russia's disinformation targets respondents of various political ideologies.

We have also included interaction terms between engagement with Russia-aligned content and the demographic variables to further analyze its impact on people's voting behavior. We have found that Russia-aligned content has no interaction with respondents' race or political engagement but it has a statistically significant negative effect on voting intention for candidates from the opposite political camp: liberal respondents ('Very liberal' and 'Somewhat liberal') are less likely to support Donald Trump while conservative respondents ('Very conservative') are less likely to support Joe Biden when they frequently engage with Russia-aligned content (Table 9). This finding is consistent with an argument that the Kremlin's strategy attempts to exacerbate existing political divides in the US political climate.

	Donald Trump		Joe Biden	
	(1)	(2)	(3)	(4)
	Original sample	Pew-weights	Original sample	Pew-weights
Engagement with Russia-aligned content	0.001 (0.003)	0.002 (0.003)	0.002 (0.002)	0.001 (0.003)
Very liberal	-0.404*** (0.121)	-0.385*** (0.124)	0.701*** (0.103)	0.653*** (0.109)
Liberal	-0.503*** (0.136)	-0.499*** (0.142)	0.844*** (0.112)	0.780*** (0.122)
Somewhat liberal	-0.594*** (0.139)	-0.555*** (0.145)	0.533*** (0.109)	0.520*** (0.117)
Somewhat conservative	0.818*** (0.119)	0.800*** (0.125)	-0.659*** (0.120)	-0.594*** (0.128)
Conservative	1.184*** (0.116)	1.197*** (0.122)	-0.918*** (0.117)	-0.938*** (0.123)
Very conservative	1.372*** (0.126)	1.378*** (0.129)	-1.089*** (0.131)	-1.095*** (0.135)
Very liberal # Russia-aligned content	-0.206*** (0.085)	-0.179*** (0.075)	0.010 (0.007)	0.011 (0.007)
Liberal # Russia-aligned content	-0.058 (0.051)	-0.044 (0.047)	0.008 (0.009)	0.009 (0.009)
Somewhat liberal # Russia-aligned content	-0.047*** (0.026)	-0.045*** (0.025)	0.005 (0.008)	0.007 (0.008)
Somewhat conservative # Russia-aligned content	-0.000 (0.013)	-0.001 (0.013)	-0.002 (0.014)	-0.003 (0.015)
Conservative # Russia-aligned content	0.001 (0.004)	0.001 (0.005)	-0.006 (0.005)	-0.005 (0.005)
Very conservative # Russia-aligned content	0.021 (0.015)	0.016 (0.013)	-0.262*** (0.122)	-0.255*** (0.132)
male	-0.142*** (0.071)	-0.097 (0.074)	0.103 (0.065)	0.078 (0.069)
age	0.051*** (0.014)	0.055*** (0.015)	-0.032*** (0.013)	-0.029*** (0.014)
age squared	-0.001*** (0.000)	-0.001*** (0.000)	0.000*** (0.000)	0.000*** (0.000)
Bachelor's degree	0.196 (0.216)	0.229 (0.224)	-0.270 (0.205)	-0.273 (0.211)

Less than a high school diploma	-0.323 (0.376)	-0.293 (0.369)	-0.896*** (0.317)	-0.951*** (0.334)
Master's degree	0.087 (0.219)	0.098 (0.227)	-0.118 (0.210)	-0.116 (0.216)
Regular high school diploma	0.359 (0.234)	0.414*** (0.243)	-0.511*** (0.221)	-0.502*** (0.229)
Some college, no degree	0.220 (0.222)	0.209 (0.232)	-0.433*** (0.211)	-0.384*** (0.219)
Vocational school/ union certificate	0.375 (0.260)	0.371 (0.268)	-0.367 (0.252)	-0.323 (0.258)
American Indian or Alaska Native	-0.088 (0.282)	-0.155 (0.262)	-0.310 (0.239)	-0.234 (0.234)
Asian	-0.193 (0.151)	-0.145 (0.154)	-0.010 (0.133)	-0.029 (0.138)
Black, or African American	-0.651*** (0.126)	-0.603*** (0.127)	0.276*** (0.102)	0.221*** (0.104)
Some other race	-0.341 (0.213)	-0.349*** (0.212)	0.152 (0.176)	0.203 (0.195)
Medium size city (50,000 to 249,999)	0.035 (0.127)	0.049 (0.137)	0.017 (0.115)	0.026 (0.124)
Suburb of a large central city	0.212*** (0.102)	0.217*** (0.106)	-0.274*** (0.092)	-0.298*** (0.097)
Suburb of a medium size city	0.068 (0.130)	0.076 (0.137)	-0.063 (0.117)	-0.087 (0.124)
Town or village (2,500 to 9,999)	0.226 (0.156)	0.221 (0.159)	-0.320*** (0.151)	-0.321*** (0.180)
Rural area < 10 miles from the closest town	0.292*** (0.153)	0.279*** (0.153)	-0.216 (0.135)	-0.296*** (0.138)
Rural area > 10 miles from the closest town	0.619*** (0.216)	0.517*** (0.232)	-0.378*** (0.198)	-0.407*** (0.211)
Small city or town (10,000 to 49,999)	0.303*** (0.124)	0.325*** (0.135)	-0.349*** (0.111)	-0.406*** (0.117)
below -\$49,999	-0.345*** (0.141)	-0.368*** (0.143)	0.066 (0.135)	0.047 (0.140)
\$50,000-\$74,999	-0.261*** (0.150)	-0.282*** (0.151)	0.259*** (0.142)	0.241*** (0.144)
\$75,000-\$99,999	-0.045 (0.151)	-0.078 (0.153)	0.054 (0.144)	-0.014 (0.147)
\$100,000-\$149,999	-0.098 (0.157)	-0.105 (0.156)	0.092 (0.149)	0.080 (0.149)
Twitter Usage Frequency	-0.026 (0.037)	-0.028 (0.039)	0.093*** (0.033)	0.082*** (0.035)
Constant	-1.640*** (0.421)	-1.757*** (0.438)	0.731*** (0.379)	0.777*** (0.398)
Observations	2,017	2,017	2,017	2,017
r ² _p	0.308	0.296	0.242	0.227

*** p<0.1, ** p<0.01, * p<0.05

Table 9. Probit regression model: predictor of voting for Donald Trump to take part in November 2020 election.
Interaction with ideology

The inclusion of fixed controls for days of engagement (over an observed period of 21 days) does not alter our main conclusions (the results are available upon request).

DISCUSSION

Our content analysis of Twitter posts revealed that our respondents rarely engage with pro-Russian media accounts, but they occasionally engage with Russia-aligned accounts that promote narratives pushed by Kremlin proxies. The content of their posts tends to be about divisive political and social issues, and supportive of either the Republican or the Democrats. Such Twitter posts attract and reinforce the ideology of specific groups of Twitter users. The analysis allowed us to identify several individual characteristics among our respondents that predict higher engagement with Russia-aligned content.

First, we find that male gender and lower socioeconomic status of respondents increase the likelihood of engagement with Russia-aligned content. Regarding race, the African-American respondents in our sample were more likely to engage with Russia-aligned content. This is consistent with earlier studies that emphasized that this social group is commonly targeted by Kremlin proxies in an effort to deepen existing social divisions in the United States.

Second, we find the correlation between extreme ideological views on both sides of the political spectrum and higher propensity to engage with Russia-aligned content. This is also consistent with previous studies that also found that partisanship consistently predicts people's willingness to engage with disinformation (Kahan, 2017; Van Bavel and Pereira, 2018).

Our analysis also discovers a link between lower trust in institutions and mainstream media, and higher propensity to engage with Russia-aligned content. We show that individuals with lower levels of institutional trust and lower levels of trust in mainstream media tend to engage with Russia-aligned content more often. This result is consistent with other studies in Europe (Zimmermann and Kohring, 2020) that also find a link between lower trust in news media and politics, and higher belief in online disinformation. This finding implies that being prone to engage with disinformation may be a symptom (rather than a cause in itself) of growing disenchantment of specific social groups in the society with establishment and mainstream institutions. This suggests that solutions to the disinformation problem cannot rely only on measures to combat disinformation (which should still be continued and reinforced). They also need to focus on restoring trust in mainstream institutions among individuals on both sides of the political spectrum.

Ultimately, our analysis has discovered a higher propensity to participate in the 2020 presidential election among the respondents more actively engaged with Russia-aligned content. These results may be explained by the very strong correlation between our measure of Russia-aligned content and more partisan coverage of political events. We also find that engagement with Russia-aligned content correlates negatively with propensity to support the presidential candidates from the opposite political camp among individuals on both sides of the political spectrum. This finding is consistent with an argument that the Kremlin attempts to exacerbate the existing political divisions within the United States.

6. POLICY RECOMMENDATIONS

- Systematize the Datasets Pertaining to Russia's Influence Operations

In recent years, hardly any policy issue has received as much attention from the US policy community as Russia's influence operations. Yet, while working on this report, we faced serious challenges finding a platform integrating multiple data sources and links on Russia's disinformation. Multiple entities in the United States and worldwide track and collect data on disinformation, fake news sources, and social media influence operations, but many such studies are not up-to-date or publicly available for scholars and thus make little contribution to the general knowledge. We propose that GEC or other specialized agencies create a platform that would systematize the existing open databases so as to facilitate research outreach for scholars working on these topics. This would significantly boost the research on understanding Russia's influence operations. As an example, in Appendix I we provide links to databases identified throughout our work on this report (many turned out to be unusable for the reasons outlined above).

- Deepen Quantitative Research Analysis

Despite the attention that Russia's influence operations have received in recent years, the bulk of the analysis on these issues remains overwhelmingly qualitative and often repetitive. This prevents analysts from moving forward by tracking the impact of disinformation among specific targeted audiences, which (as we explain above) is the essence of the Kremlin approach and one of the main reasons for its success. The policy community thus needs to adopt quantitative techniques more often or to cooperate with academic scholars to apply them more pro-actively to address more urgent and nuanced questions pertaining to the impact of Russia's influence operations. Our study is one of the ongoing attempts to fill in this gap.

- Avoid Overfocusing on Twitter

The absolute majority of existing quantitative social media studies focus on Twitter, due to data availability issues. However, this report analysis demonstrates that Russia's influence operations target a variety of social media platforms. The 2016 IRA effort, for example, predominantly focused on Facebook, where it achieved a very large outreach to various US audiences. Given the importance of these questions for US national security, we recommend that social media platforms other than Twitter (including Facebook, Instagram, Reddit, YouTube, Parler, Tumblr, 4chan, 9GAG, and Pinterest) and direct messaging platforms (WhatsApp, Telegram) make their data more accessible for scholarly analysis.

- Punish / Deter the Aggressors

This section includes a number of measures designed to limit the Kremlin's ability to spread disinformation campaigns online. These might include publicly exposing those who are part of pro-Kremlin operations, either wittingly or unwittingly, and targeting individual Russian operatives through cyberoperations to deter them from spreading engaging in malicious activity (Barnes, 2018; Nakashima, 2019). Western companies should be warned against placing their ads with Kremlin-linked disinformation outlets (Kalensky, 2019: 13). We also recommend continuing the strategy of labelling websites as being funded by or linked to the Kremlin – studies have shown that this approach makes Twitter users less prone to liking and sharing tweets by news outlets labeled as state-affiliated (Schoenmakers and Liu, 2021). We also recommend sanctioning the worst disinformers and disinformation organizations. In particular, the United States should sanction Russia's most active propagandists, such as Dmitry Kiselyov, Vladimir Solovyov, and others.

- Work with Social Media Companies to Highlight and Block Kremlin-Linked Proxies and Malicious Actors in Russia

Our findings indicate that the countermeasures adopted in recent years to combat Russia's social media operations have been fairly successful. In particular, by 2020, blocking Kremlin-linked accounts and platforms had significantly scaled down the outreach of Kremlin proxies to US audiences. As the fight is far from over, this approach should be continued in the future. Scholars should determine whether labelling Russia-funded websites and pages (Paul, 2020)¹⁰ effectively reduces the engagement of US audiences with such content.

- Develop Targeted Media Literacy Training, Build the Resilience of At-Risk Populations

Media literacy training seeks to improve audiences' ability to access, analyze, and evaluate various forms of media (Bodine-Baron et al., 2018). However, such programs often remain generic and untailored to the needs of specific groups. This contrasts with the Kremlin social media approach, which, as we have shown above, is often deliberately crafted to target the interests and attitudes of specific social groups. Accordingly, media literacy programs (especially those identified as targets of the Kremlin influence campaigns) should also be developed for specific targeted groups (those of particular Kremlin interest) and adjusted to make them more relatable. Facebook algorithms that develop interest-based targeting may also come in handy when designing such programs.

Moreover, if lower trust in political institutions is one of the predictors of engagement with disinformation, media literacy programs that these social

¹⁰ https://blog.twitter.com/en_us/topics/product/2020/new-labels-for-government-and-state-affiliated-media-accounts.html

groups perceive as promoted by the political establishment will not be effective in changing their viewpoints. These groups require more nuanced approaches designed to restore their trust in existing institutions (Silverblatt 2015; Humprecht et al. 2020) before media literacy programs can be successfully implemented.

Most of the existing media literacy programs lack clear evidence of effectiveness (particularly for adults) and need to be improved (Callahan, 2019).

- Focus on Disinformation by Domestic Groups Susceptible to Disinformation

The above analysis shows, that, in recent years, the Kremlin's approach has shifted from creating its own fake or misleading content to promoting narratives originated by extremist groups on both (left and right) sides of the political spectrum in the United States, as well as other targeted groups. Russia's collocation strategy that blurs distinctions between the Kremlin proxies and American citizens with extreme partisan views makes monitoring information flows particularly challenging, given the ongoing polarization of US domestic politics. In view of the changing Kremlin disinformation approach, we suggest that scholars and policy analysts pay more attention to the roles the extreme-left and extreme-right groups play in spreading disinformation narratives, and develop strategies to counter them. It can be anticipated that having been barred from major social media platforms, they would move to platforms that include direct messaging services.

- Restore Trust in Traditional Media

Growing mistrust in traditional media among Americans and their ongoing polarization constitute significant points of concern. The polarization of traditional media is at least partly driven by their attempts to compete for audiences with social media (Klein, 2020). Our findings suggest that respondents mistrustful of traditional media outlets may be more prone to engage with Russia's disinformation. What seems to be missing in the US context is a credible, quality, trusted public broadcaster with a high audience outreach. As a possible solution, we recommend considering a possibility to increase public funding to US news broadcasters, which would make it a priority to maintain standards of professional and objective fact-based reporting. The funding currently received by the Public Broadcasting Service (PBS) and the National Public Radio (NPR) is too small to provide a serious alternative to major news outlets (Kirchick, 2017). We recommend basing a strategy on three simultaneous approaches:

- 1) Strengthening the Federal Communications Commission (FCC) as a regulator broadcasting content through licensing;
- 2) Increasing financial support to PBS and NPR; and
- 3) Innovating regulations to strengthen the finances of news operations that meet accuracy standards over time—standards set by journalism schools, not government. Meeting standards might qualify for a tax incentive.

7. ACKNOWLEDGEMENTS

This publication has benefited greatly from comments by Gregory Clay Ramsay, Andy Guess, Jakub Kalenský, Vasily Gatov, Mohammed Motiwala, Sergey Sarnovich, and John Sipher.

REFERENCES

- 116th Congress, 1st Session Senate. (2019). Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views (No. 116-XX). Available at: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
- Alba, Davey. (2020). How Russia's Troll Farm Is Changing Tactics Before the Fall Election. *The New York Times*. March 29. Available at: <https://www.nytimes.com/2020/03/29/technology/russia-troll-farm-election.html>
- Aleksejeva, Nika, Andriukaitis, Lukas, Bandeira, Luiza, Barojan, Donara, Brookie, Graham, Buziashvili, Eto, Carvin, Andy, Karan, Kanishk, Nimmo, Ben, Robertson, Iain, and Michael Sheldon. (2019). Operation "Secondary Infection": A Suspected Russian Intelligence Operation Targeting Europe and the United States. *DFRLab*, August. Available at: atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infection_English.pdf
- Alsmadi, I., & O'Brien, M. J. (2020). How Many Bots in Russian Troll Tweets?. *Information Processing & Management*, 57(6), 102303.
- Alperovitch, Dmitri. (2016). "Bears in the Midst: Intrusion into the Democratic National Committee". CrowdStrike Blog. Available at: <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>
- Bargaoanu, A., and Radu, L. (2018). Fake news or disinformation 2.0 some insights into romanians' digital behaviour. *Romanian Journal of European Affairs*, 18(1), 24-38.
- Barnes, Julian. (2018). U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections. *The New York Times*. October 23. Available at: <https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html>
- Barnes, Julian, and Adam Goldman. (2020). Russia Trying to Stoke U.S. Racial Tensions Before Election, Officials Say. *The New York Times*. March 10, 2020. Available at: <https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html>
- Baum, Matthew A. and Tim Groeling. (2008) New media and the polarization of American political discourse. *Political Communication*. 25:4, 345-365
- Bennett, W. L., and Livingston, S. (2018). The Disinformation Order: Disruptive Communication and The Decline of Democratic Institutions. *European journal of communication*, 33(2), 122-139.
- Bershidky, Leonid. (2019). The West Needs to Measure Russian Election Meddling. Here's How. *BNN Bloomberg*, November 18. Available at: <https://www.bnnbloomberg.ca/the-west-needs-to-measure-russian-election-meddling-here-s-how-1.1349609>
- Bodine-Baron, E. A., Helmus, T. C., Radin, A., & Treyger, E. (2018). *Countering Russian social media influence*. Santa Monica: RAND Corporation.
- Boyd, R. L., Spangher, A., Fournay, A., Nushi, B., Ranade, G., Pennebaker, J., & Horvitz, E. (2018). Characterizing the Internet Research Agency's social media operations during the 2016 US presidential election using linguistic analyses.

- Brandt, Jessica, and Amber Frankland. (2020). Leaks, Lies, and Altered Tape: Russia's Maturing Information Manipulation Playbook. The Alliance for Securing Democracy. October 14. Available at: <https://securingdemocracy.gmfus.org/russias-maturing-information-manipulation-playbook/>
- Brenan, Megan. (2019). Americans' Trust in Mass Media Edges Down to 41%. *Gallup*. Eptember 26. Available at: <https://news.gallup.com/poll/267047/americans-trust-mass-media-edges-down.aspx>
- Benoit, K., Watanabe, K., Wang, H., Nulty, P., Obeng, A., Müller, S., & Matsuo, A. (2018). quanteda: An R package for the quantitative analysis of textual data. *Journal of Open-Source Software*, 3(30), 774. <https://doi.org/10.21105/joss.00774>
- Bugayova, Nataliya. (2020). Putin's Offset: The Kremlin's Geopolitical Adaptations Since 2014. The Institute for the Study of War. Available at: www.understandingwar.org/report/putins-offset-kremlin%E2%80%99s-geopolitical-adaptations-2014
- Carmi, E., Yates, S. J., Lockley, E., and Pawluczuk, A. (2020). Data citizenship: Rethinking data literacy in the age of disinformation, misinformation, and malinformation. *Internet Policy Review*, 9(2), 1-22.
- Freeman Det al.2020Coronavirus conspiracy beliefs, mistrust, and compliance with government guidelines in England. *Psychol. Med.*1-30.
- Callahan, Amy. (2019). Media Literacy Isn't Coming to Save Us (But We Can Make It Better). *Education Week*, January 23. Available at: <https://www.edweek.org/teaching-learning/opinion-media-literacy-isnt-coming-to-save-us-but-we-can-make-it-better/2019/01>
- Carpenter, Michael. (2019). Undermining democracy: Kremlin tools of malign political influence. Testimony for the United States House of Representatives Committee on Foreign Affairs Subcommittee on Europe, Eurasia, Energy, and the Environment. May 21, 2019. Available at: <https://www.congress.gov/116/meeting/house/109537/witnesses/HHRG-116-FA14-Wstate-CarpenterM-20190521.pdf>
- Choi, J. (2016). Why do people use news differently on SNSs? An investigation of the role of motivations, media repertoires, and technology cluster on citizens' news-related activities. *Computers in Human Behavior*, 54, 249–256. <https://doi.org/10.1016/j.chb.2015.08.006>
- Choi, Y.-T., and Kwon, G.-H. (2019). New forms of citizen participation using SNS: An empirical approach. *Quality & Quantity*, 53(1), 1–17. <https://doi.org/10.1007/s11135-018-0720-y>
- Chomsky, N. (1997). What makes mainstream media mainstream. *Zmagazine*, 10(10), 17-23. Available at: https://chomsky.info/199710___/
- Collier, Kevin, and Ken Dilanian. (2020). Russian Internet Trolls Hired U.S. Journalists to Push Their News Website, Facebook Says. *NBC News*, September 1. Available at: <https://www.nbcnews.com/tech/tech-news/russian-internet-trolls-hired-u-s-journalists-push-their-news-n1239000>
- Cosentino, G. (2020). Polarize and Conquer: Russian Influence Operations in The United States. In *Social Media and the Post-Truth World Order* (pp. 33-57). Palgrave Pivot, Cham.
- Craft, S., Ashley, S., and Maks, A. (2017). News media literacy and conspir-

- acy theory endorsement: *Communication and the Public*. <https://doi.org/10.1177/2057047317725539>
- Cunningham, C. A. (2020). Russian Federation Information Warfare Primer. November 12. Available at: <https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/>
- Del Vicario, Michela, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H Eugene Stanley, and Walter Quattrociocchi. (2016). The Spreading of Misinformation Online. *Proceedings of The National Academy of Sciences* 113(3): 554 –559.
- Dilanian, Ken, and Kit Ramgopal. (2020). Facebook Blocks Russia-Backed Accounts, But Other Sites Keep Churning Out Content Aimed at Americans. *NBC News*, October 9. Available at: <https://www.nbcnews.com/politics/2020-election/facebook-blocks-russia-backed-accounts-other-sites-keep-churning-out-n1242683>
- DiResta, Renee, Dr Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr Jonathan Albright, and Ben Johnson. (2018). The Tactics and Tropes of the Internet Research Agency. *New Knowledge*. Available at: <https://www.yonder-ai.com/resources/the-disinformation-report/>
- DiResta, R., and Grossman, S. (2019). Potemkin Pages & Personas: Assessing GRU Online Operation, 2014-2019.
- Dubow, Benjamin, Hu, Evanna, Shapiro, Jacob N., Erdoğan, Ulaş, and Kamy Yadav. (2020). Here's how Russia's RT spread propaganda in the lead-up to the election. November 9. *The Bulletin*. Available at: <https://thebulletin.org/2020/11/heres-how-russias-rt-spread-propaganda-in-the-lead-up-to-the-election/>
- Dutt, R., Deb, A., & Ferrara, E. (2018, December). "Senator, We Sell Ads": Analysis of the 2016 Russian Facebook Ads Campaign. In *International Conference on Intelligent Information Technologies* (pp. 151-168). Springer, Singapore.
- Eady, G., Nagler, J., Guess, A., Zilinsky, J., and Tucker, J. A. (2019). How Many People Live in Political Bubbles on Social Media? Evidence from Linked Survey and Twitter Data. *SAGE Open*, 9(1), 2158244019832705. <https://doi.org/10.1177/2158244019832705>
- Einstein KL, Glick DM. (2015). Do I think BLS data are BS? The consequences of conspiracy theories. *Political Behavior*. 37, 679-701.
- Elswah, M., and P.N. Howard. (2020). "Anything that Causes Chaos": The Organizational Behavior of Russia Today (RT). *Journal of Communication*, 70(5), 623-645.
- Erickson, Amanda. (2017). If Russia Today is Moscow's propaganda arm, it's not very good at its job. *The Washington Post*, January 12. Available at: <https://www.washingtonpost.com/news/worldviews/wp/2017/01/12/if-russia-today-is-moscows-propaganda-arm-its-not-very-good-at-its-job/>
- Ferrara, E., Chang, H., Chen, E., Muric, G., & Patel, J. (2020). Characterizing social media manipulation in the 2020 US presidential election. *First Monday*.
- Freelon, Deen, and Tetyana Lokot. (2020). Russian disinformation campaigns on Twitter target political communities across the spectrum. Collaboration between opposed political groups might be the most effective way to counter it.

- Misinformation Review* 1(1).
- Fung, Brian. (2020). Why the US government hack is literally keeping security experts awake at night. CNN. December 16. Available at: www.cnn.com/2020/12/16/tech/solarwinds-orion-hack-explained/index.html
- Galeotti, Mark. (2016a). "Hybrid War or Gibrinaya Voina? Getting Russia's Non-Linear Military Change Right." Mayak Intelligence.
- Galeotti, M. (2016b). *Putin's hydra: inside Russia's intelligence services*. European Council on Foreign Relations. Available at: https://ecfr.eu/publication/putins_hydra_inside_russias_intelligence_services/
- Galeotti, Mark. (2017a). Policy Brief: Controlling Chaos: How Russia Manages Its Political War in Europe, London: European Council on Foreign Relations, August.
- Galeotti, M. (2017b). Russian intelligence is at (political) war. *NATO Review*.
- Gatewood, C., & O'Connor, C. (2020). *Disinformation Briefing: Narratives Around Black Lives Matter and Voter Fraud*. Institute for Strategic Dialogue. <https://www.isdglobal.org/isd-publications/disinformation-briefing-narratives-around-black-lives-matter-and-voter-fraud/>
- Gauchat, G. (2012). Politicization of science in the public sphere: A study of public trust in the United States, 1974 to 2010. *American Sociological Review*, 77(2), 167–187.
- Ghanem, B., Buscaldi, D., & Rosso, P. (2019). TextTrolls: identifying Russian trolls on Twitter from a textual perspective. *arXiv preprint arXiv:1910.01340*.
- Giles K, Hanson P, Lyne R, Nixey J, Sherr J, and A.Wood. (2015). *The Russian challenge*. Chatham House, London.
- Givens, T. E. (2004). The radical right gender gap. *Comparative Political Studies*, 37(1), 30-54.
- Glenski, M., Weninger, T., & Volkova, S. (2018). Propagation from Deceptive News Sources Who Shares, How Much, How Evenly, and How Quickly? *IEEE Transactions on Computational Social Systems*, 5(4), 1071–1082. <https://doi.org/10.1109/TCSS.2018.2881071>
- Global Engagement Center. (2020). GEC Special Report: August 2020 Pillars of Russia's Disinformation and Propaganda Ecosystem. U.S. Department of State, August. Available at: https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf
- Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A., & Tucker, J. A. (2020). Cross-Platform State Propaganda: Russian Trolls on Twitter and YouTube during the 2016 U.S. Presidential Election. *The International Journal of Press/Politics*, 25(3), 357–389. <https://doi.org/10.1177/1940161220912682>
- Graber, D. A., & Dunaway, J. (2017). Mass media and American politics. Cq Press.
- Guge, Ethan, "Targeted Disinformation Warfare: How and Why Foreign Efforts are Effective, and Recommendations for Impactful Government Action" (2020). Creative Components. Available at: <https://lib.dr.iastate.edu/cgi/view-content.cgi?article=1645&context=creativecomponents>
- Guglielmi, Giorgia. (2020). The next-generation bots interfering with the US election. *Nature*. October 28/ Available at: <https://www.nature.com/articles/d41586-020-03034-5#ref-CR2>

- Gunther, A. C., Storey, J. D. (2003). The influence of presumed influence. *Journal of Communication*, 53, 199-215.
- Hanlon, B. (2018). *It's Not Just Facebook: Countering Russia's Social Media Offensive*. German Marshall Fund of the United States. Available at: https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Social-Media-Policy_Final-edit.pdf
- Hanlon, Bradley, and Thomas Morley. (2019). Russia's Network of Millennial Media. The Alliance for Securing Democracy. February 15. Available at: <https://securingdemocracy.gmfus.org/russias-network-of-millennial-media/>
- Helmus, T. C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A., & Winkelman, Z. (2018). Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. Rand Corporation. Available at: https://www.rand.org/pubs/research_reports/RR2237.html
- Helmus, Todd C., James V. Marrone, Marek N. Posard, and Danielle Schlang, Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions. Santa Monica, CA: RAND Corporation, 2020. Available at: https://www.rand.org/pubs/research_reports/RA704-3.html
- Hopp, T., Ferrucci, P., & Vargo, C. J. (2020). Why do people share ideologically extreme, false, and misleading content on social media? A self-report and trace data-based analysis of countermedia content dissemination on Facebook and Twitter. *Human Communication Research*.
- Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., and Francois, C. (2018). The IRA, social media and political polarization in the United States, 2012-2018. Retrieved from the University of Oxford website: <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report-2018.pdf>
- Howell, Jen Patja. (2020). The Lawfare Podcast: Thomas Rid on 'Active Measures,' Part 2. *The Lawfare blog*. Available at: <https://www.lawfareblog.com/lawfare-podcast-thomas-rid-active-measures-part-2>
- Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to online disinformation: A framework for cross-national comparative research. *The International Journal of Press/Politics*.
- Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. *The International Journal of Press/Politics*, 25(3), 493–516. <https://doi.org/10.1177/1940161219900126>
- Im, J., Chandrasekharan, E., Sargent, J., Lighthammer, P., Denby, T., Bhargava, A., ... & Gilbert, E. (2020, July). Still out there: Modeling and identifying Russian troll accounts on twitter. In *12th ACM Conference on Web Science* (pp. 1-10).
- Jamieson, K. H. (2020). *Cyberwar: how Russian hackers and trolls helped elect a president: what we don't, can't, and do know*. Oxford University Press.
- Jerit, J., and Barabas, J. (2012). Partisan perceptual bias and the information environment. *The Journal of Politics*, 74(3), 672-684.
- Johnson, Matt. (2019). Tyranny's Mouthpiece. *Quillette*. October 26. Available at: <https://quillette.com/2019/10/26/tyrannys-mouthpiece/>

- Kahan, D. M. (2017). Misinformation and identity-protective cognition. *Fake News in Context*, 51.
- Kalensky, Jacob. (2019). Testimony by Jakub Kalenský, Senior Fellow at the Atlantic Council, to Foreign Affairs Subcommittee on Europe, Eurasia, Energy, and the Environment "Russian disinformation attacks on elections: Lessons from Europe." July 16. Available online at: <https://docs.house.gov/meetings/FA/FA14/20190716/109816/HHRG-116-FA14-Wstate-KalenskJ-20190716.pdf>
- Kandrik, Matěj and Matúš Jevčák. (2018). "Unprepared and Vulnerable: The Resilience of the Slovak Republic to Foreign, Foremost Kremlin-Led Disinformation Campaigns." In *Disinformation Resilience Index Central and Eastern Europe*, edited by Volha Damarad and Andrei Yelisseyeu, 1 – 10. Bratislava: Stratpol
- Kelly, M., and E., Samuels. (2019). How Russia weaponized social media, got caught and escaped consequences. *The Washington Post*. Available at: <https://www.washingtonpost.com/politics/2019/11/18/how-russia-weaponized-social-media-got-caught-escaped-consequences/>
- Kenney, C., Bergmann, M., & Lamond, J. (2019). Understanding and Combating Russian and Chinese Influence Operations. *Center for American Progress*, 28. Available at: <https://www.americanprogress.org/issues/security/reports/2019/02/28/466669/understanding-combating-russian-chinese-influence-operations/>
- Kim M, and X. Cao. (2016). The impact of exposure to media messages promoting government conspiracy theories on distrust in the government: evidence from a two-stage randomized experiment. *International Journal of Communications*. 10, 3808-3827.
- Kim, Y. M. (2018). Uncover: Strategies and Tactics of Russian Interference in US Elections. *Young*, 9, 04. Available at: https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/09/Uncover.Kim_v.5.0905181.pdf
- Kim, Young Mie (2020). "New Evidence Shows How Russia's Election Interference Has Gotten More Brazen". *Brennan Center for Justice*. May 5. Available at: <https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more>
- Kirchick, James. (2017). Why the US needs its own BBC. *GQ Magazine*. June 5. Available at: <https://www.gq-magazine.co.uk/article/donald-trump-pbs-bbc-usa>
- Klein, Ezra. (2020). Why the media is so polarized — and how it polarizes us. *Vox*. January 28. Available at: <https://www.vox.com/2020/1/28/21077888/why-were-polarized-media-book-ezra-news>
- Kohring, M., and Matthes, J. (2016). Trust in News Media: Development and Validation of a Multidimensional Scale. *Communication Research*. <https://doi.org/10.1177/0093650206298071>
- LaMarco, Nicky. (2018). Mainstream Vs. Alternative Media. *Chron*. October 12. Available at: <https://smallbusiness.chron.com/mainstream-vs-alternative-media-21113.html>
- Leonenko, S. (1995). "Refleksivnoe upravlenie protivnikom (Reflexive control of the enemy)," *Armeyskiy Sbornik*, no. 8.
- Linville, D. L., & Warren, P. L. (2020). Troll factories: Manufacturing specialized disin-

- formation on Twitter. *Political Communication*, 1-21.
- Lucas, E., and Pomeranzev, P. (2016). Winning the information war. Techniques and counter-strategies to Russian propaganda in Central and Eastern Europe. Washington: The Center for European Policy Analysis.
- Marcellino, W., Johnson, C., Posard, M. N., & Helmus, T. C. (2020). *Foreign Interference in the 2020 Election: Tools for Detecting Online Election Interference*. https://www.rand.org/pubs/research_reports/RRA704-2.html
- Martin, D. A., & Shapiro, J. N. (2019). Trends in online foreign influence efforts. Princeton University. Available online at: https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_foreign_influence_efforts_2019jul08_0.pdf
- Mayer, J. (2018). How Russia Helped Swing the Election for Trump. *The New Yorker*. <https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump>
- McCauley, M. (2013). *Russia, America and the Cold War: 1949-1991 (Revised 2nd Edition)*. Routledge.
- McFaul, M. (2020). Putin, Putinism, and the Domestic Determinants of Russian Foreign Policy. *International Security*, 45(2), 95-139.
- Meleshevich, Kirill, and Bret Schafer. (2018). "Online Information Laundering: The Role of Social Media," Alliance for Securing Democracy, January 9. Available at: <https://securingdemocracy.gmfus.org/online-information-laundering-the-role-of-social-media/>
- Mölder, H., and V. Sazonov. (2018). Information warfare as the Hobbesian concept of modern times—the principles, techniques, and tools of Russian information operations in the Donbass. *The Journal of Slavic Military Studies*, 31(3), 308-328.
- Mueller, R. S., III. (2019). Report on The Investigation into Russian Interference in the 2016 Presidential Election, Special Counsel Robert S. Mueller, Volume 1, Washington, DC: U.S. Department of Justice. March. Available at: <https://www.justice.gov/storage/report.pdf>
- Mueller, R. S., III. (2019). Report on The Investigation into Russian Interference in the 2016 Presidential Election, Special Counsel Robert S. Mueller, Volume 3, Washington, DC: U.S. Department of Justice. March.
- Nakashima, Ellen. (2019). U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. *The Washington Post*. February 27. Available at: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html
- Nakashima, Ellen, and Craig Timberg. (2020). Russian Government Hackers Are Behind A Broad Espionage Campaign That Has Compromised U.S. Agencies, Including Treasury and Commerce. *The Washington Post*. December 14. Available at: https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html
- Ng, Alfred. (2018). Russian Influencers Thrived on Instagram after Facebook, Twitter

- Caught On. C-Net. December 17. Available at: www.cnet.com/news/russian-influencers-thrived-on-instagram-after-pressure-on-facebook-twitter/
- Nimmo, Ben, Francois Camille, Eib, Shawn C., and Lea Ronzaud. (2020). IRA Again: Unlucky Thirteen. Graphika, September 1. Available at: <https://graphika.com/reports/ira-again-unlucky-thirteen/>.
- Nye, Joseph S. (1990). Soft Power. *Foreign Policy*, 80.
- O'Sullivan, Donie. (2018). Russian trolls created Facebook events seen by more than 300,000 users. *CNN Business*. January 26. Available at: <https://money.cnn.com/2018/01/26/media/russia-trolls-facebook-events/index.html>
- Office of the Director of National Intelligence. (2017). Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. *Intelligence Community Assessment*. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf?utm_source=fbia
- Pariser, Eli. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. Penguin, UK.
- Partin, Will. (2020). What if modern conspiracy theorists are altogether too media literate? The Outline. January 8. Available online at: <https://theoutline.com/post/8509/revolution-q-conspiracy-theorists-media-literacy?zd=3&zi=r4dkrpbl>
- Paul, Christopher, and Miriam Matthews. (2016). The Russian 'Firehose of Falsehood,' Propaganda Model. RAND Corporation. Available online at: https://www.rand.org/content/dam/rand/pubs/perspectives/PE_100/PE_198/RAND_PE_198.pdf
- Paul, Katie. (2020). Facebook to apply state media labels on Russian, Chinese outlets. *Reuters*, June 4. Available at: <https://www.reuters.com/article/us-facebook-media/facebook-to-apply-state-media-labels-on-russian-chinese-outlets-idUSKBN23B2PX>
- Pennycook, G., and Rand, D. G. (2019). Lazy, Not Biased: Susceptibility to Partisan Fake News Is Better Explained by Lack of Reasoning Than by Motivated Reasoning. *Cognition*, 39-50.
- Pennycook, G., Cannon, T., & Rand, D. G. (2018). *Prior Exposure Increases Perceived Accuracy of Fake News* (SSRN Scholarly Paper ID 2958246). Social Science Research Network. <https://doi.org/10.2139/ssrn.2958246>
- Perrin, Andrew and Monica Anderson. (2019). Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018. *Pew Research Center*, April 10. Available at: <https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/>
- Pew Research Center. (2017). *Public Trust in Government 1958–2017*. Retrieved from <http://www.people-press.org/2017/05/03/public-trust-in-government-1958-2017/>
- Posard, Marek N., Marta Kepe, Hilary Reininger, James V. Marrone, Todd C. Helmus, and Jordan R. Reimer. (2020). From Consensus to Conflict: Understanding Foreign Measures Targeting U.S. Elections. Santa Monica, CA: RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RRA704-1.html

- Ribeiro, M. H., Calais, P. H., Almeida, V. A., & Meira Jr, W. (2017). "Everything I Disagree With is #FakeNews": Correlating Political Polarization and Spread of Misinformation. *arXiv preprint arXiv:1706.05924*.
- Rid, Thomas. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux, April.
- Rosenberger, Laura. (2018). Written Testimony, Hearing before the Senate Select Committee on Intelligence, August. Available at <https://www.intelligence.senate.gov/hearings/open>.
- Rudolph, T., and Evans, J. (2005). Political trust, ideology, and public support for government spending. *American Journal of Political Science*, 49, 660–671.
- Sakwa, R. (2012). "Conspiracy Narratives as a Mode of Engagement in International Politics: The Case of the 2008 Russo-Georgian War." *The Russian Review*, 71(4).
- Salmon, Felix. (2021). Media trust hits new low. *Axios*, January 21. Available at: <https://www.axios.com/media-trust-crisis-2bf0ec1c-00c0-4901-9069-e26b21c283a9.html>
- Samuels, Elyse, and Monica Akhtar. (2019). Are 'bots' manipulating the 2020 conversation? Here's what's changed since 2016. *The Washington Post*. November 20. Available at: <https://www.washingtonpost.com/politics/2019/11/20/are-bots-manipulating-conversation-heres-whats-changed-since/>
- Sanger, David E., and Zolan Kanno-Youngs. (2020). "The Russian Trolls Have a Simpler Job Today. Quote Trump". *The New York Times*. September 25. Available at: <https://www.nytimes.com/2020/09/22/us/politics/russia-disinformation-election-trump.html>
- Svetoka, Sanda. (2016). *Social Media as a Tool of Hybrid Warfare*. NATO Strategic Communications Centre of Excellence, May. Available at: <https://www.stratcomcoe.org/social-media-tool-hybrid-warfare>
- Shane, S. (2018). Five Takeaways from New Reports on Russia's Social Media Operations. *The New York Times*.
- Schoenmakers, Kevin, and Claire Liu. (2021). China's Telling Twitter Story. *China Media Project*, January 18. Available at: <https://chinamediaproject.org/2021/01/18/chinas-telling-twitter-story/>
- Silverblatt, A., Ferry, J., & Finan, B. (2015). *Approaches to Media Literacy: A Handbook: A Handbook*. Routledge.
- Snegovaya, M. (2015). Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid Warfare. Institute for the Study of War.
- Snegovaya, M. (2020). Disinformation, Euroskepticism, and pro-Russian Parties in Eastern Europe. Report for Free Russia Foundation, December. Available at: <https://static1.squarespace.com/static/55510affe4b06afeca50df07/t/57d3923859cc684a23285460/1473483331787/Siloviki+Final+Aug+17+.pdf>
- Starbird, K. (2017, May). Examining the alternative media ecosystem through the production of alternative narratives of mass shooting events on Twitter. In *lcwsm* (pp. 230-239).
- Stretch, Colin. (2017). Responses by Facebook to SSCI Questions for the Record

- from hearing on November 1, 2017. Available at: <https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf>
- TASS. (2020). Russia May Allocate Around \$1.37 Bln To Support Media In 2021. September 17. Available at: <https://tass.com/economy/1201879>
- Tidy, Joe. (2020). "SolarWinds: Why the Sunburst hack is so serious". BBC. December 16. Available at: <https://www.bbc.com/news/technology-55321643>
- Timberg, Craig, Dwoskin, Elizabeth, Entous, Adam, and Karoun Demirjian. (2017). Russian ads, now publicly released, show sophistication of influence campaign. *The Washington Post*. November 1. Available at: http://static.cs.brown.edu/people/jsavage/VotingProject/2017_11_01_WaPo-RussianAdsShowSophisticationOfInfluenceCampaign.pdf
- Thomas, Timothy L. (1996) "Russian Views on Information-Based Warfare," *Airpower Journal* Special Edition.
- Thomas, Timothy L. (2004). "Russia's Reflexive Control Theory and The Military," *Journal of Slavic Military Studies*, 17: 237–256. Available at: https://www.rut.edu/~w-cmmc/literature/Thomas_2004.pdf.
- Thomas, Timothy L. (2009). Chapter 20 "Nation-State Cyber Strategies: Examples from China and Russia," *Cyber Power and National Security* Edited by Franklin D. Kramer, Stuart H. Starr, & Larry K. Wentz. Available at: <http://Ctnsp.Dodlive.Mil/Files/2014/03/Cyberpower-I-Chap-20.Pdf>.
- Tkacheva, Olesya, Lowell H. Schwartz, Martin C. Libicki, Julie E. Taylor, Jeffrey Martini, and Caroline Baxter. (2013). *Internet Freedom and Political Space*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RR295.html
- Tucker, Eric. (2020). "FBI Official: Russia Wants to See US 'Tear Ourselves Apart'". *Associated Press*. February 24. Available online at: <https://apnews.com/a55930e0a02d2e21d8ed2be7bc496a6f>
- Twitter Public Policy Blog. (2018). "Update on Twitter's review of the 2016 US election." January 19. Available online at: https://blog.twitter.com/en_us/topics/company/2018/2016-election-update.html
- Van Bavel, J. J., and Pereira, A. (2018). The partisan brain: An identity-based model of political belief. *Trends in cognitive sciences*, 22(3), 213-224.
- van der Linden S, Panagopoulos C, Azevedo F, and J.T. Jost. (2020). The paranoid style in American politics revisited: evidence of an ideological asymmetry in conspiratorial thinking. *Polit. Psychol.*
- Ward, Clarissa; Polglase, Katie; Shukla, Sebastian; Mezzofiore, Gianluca; Lister, Tim (March 12, 2020). "Russian election meddling is back — via Ghana and Nigeria — and in your feeds". *CNN*. Available at: <https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html>
- Watanabe, K. (2018). Conspiracist propaganda: how Russia promotes anti-establishment sentiment online? ECPR General Conference, Hamburg.
- Watanabe, Kohei. (2020). "Latent Semantic Scaling: A Semisupervised Text Analysis Technique for New Domains and Languages." *Communication Methods and Measures*. <https://doi.org/10.1080/19312458.2020.1832976>.
- Watts, Clint. (2017). Hearing before the Senate Select Committee on Intelligence,

- March 30. Available online at: <https://www.intelligence.senate.gov/hearings/open/>
- Weeks, B. E., and R. K. Garrett. (2014). Electoral Consequences of Political Rumors: Motivated Reasoning, Candidate Rumors, And Vote Choice During The 2008 US Presidential Election. *International Journal of Public Opinion Research*, 26, 401–422.
- Weisburd, A., Watts, C., and Berger, J. M. (2016). Trolling for Trump: How Russia Is Trying to Destroy Our Democracy. *War on the Rocks*, 6.
- Wojcik, S., and A. Hughes. (2019). Sizing up Twitter users. Washington, DC: Pew Research Center. Available at: <https://www.pewresearch.org/internet/2019/04/24/sizing-up-twitter-users/>
- Woolley, Samuel, and Phil Howard. (2017). Computational Propaganda Worldwide: Executive Summary, Computational Propaganda Research Project, Oxford Internet Institute, University of Oxford, November. Available at: <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>
- Yablokov, I. (2015). Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT). *Politics*, 35(3–4), 301–315.
- Zannettou, S., Bradlyn, B., De Cristofaro, E., Stringhini, G., & Blackburn, J. (2019a). Characterizing the Use of Images by State-Sponsored Troll Accounts on Twitter. *arXiv preprint arXiv:1901.05997*.
- Zannettou, S., Caulfield, T., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Blackburn, J. (2019b, May). Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the web. In *Companion proceedings of the 2019 world wide web conference* (pp. 218–226).
- Zannettou, S., Caulfield, T., Setzer, W., Sirivianos, M., Stringhini, G., & Blackburn, J. (2019c, June). Who let the trolls out? towards understanding state-sponsored trolls. In *Proceedings of the 10th acm conference on web science* (pp. 353–362).
- Zannettou, S., ElSherief, M., Belding, E., Nilizadeh, S., and Stringhini, G. (2020). Measuring and Characterizing Hate Speech on News Websites. *arXiv preprint arXiv:2005.07926*.
- Zimmermann, F., and Kohring, M. (2020). Mistrust, Disinforming News, and Vote Choice: A Panel Survey on the Origins and Consequences of Believing Disinformation in the 2017 German Parliamentary Election. *Political Communication*, 37(2), 215–237. <https://doi.org/10.1080/10584609.2019.1686095>¹¹
- Бюджет - 2021: как государство сокращает расходы на медицину. (2020) *Новые известия*. Available at: <https://newizv.ru/news/politics/24-11-2020/byudzhets-2021-kak-gosudarstvo-sokraschaet-rashody-na-meditinu>

APPENDIX I. RUSSIA'S SOCIAL MEDIA OPERATIONS DATABASES

Classification of the Info Sources as Hyper-partisan and Fake News (pp.20-21 and p.36):

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118471&download=yes

Corpus of QAnon posts known as "Q drops": <https://qresear.ch/q-posts>

Datasets with Profile Information, Tweets and Media (E.G., Images and Videos) From Accounts Connected to State-Backed Information Operations: <https://transparency.twitter.com/en/reports/information-operations.html>

Digital Society Project: <http://digitalsocietyproject.org>

EU vs Stratcom: <https://euvsdisinfo.eu>

FakeNewsChallenge: <https://github.com/FakeNewsChallenge>

Fake News Sources: <https://www.bettycjung.net/Pdfs/FakeNewsSources.pdf>

Fake News on Twitter During the 2016 U.S. Presidential Election (Grinberg et al., 2016): https://science.sciencemag.org/content/sci/suppl/2019/01/23/363.6425.374.DC1/aau2706_Grinberg_SM.pdf

False, Misleading, Clickbait-y, and Satirical "News" Sources": <https://d279m-997dpfwgl.cloudfront.net/wp/2016/11/Resource-False-Misleading-Clickbait-y-and-Satirical-%E2%80%9CNews%E2%80%9D-Sources-1.pdf>

GDELT project: <https://blog.gdelproject.org/new-gkg-2-0-article-metadata-fields/>

Hamilton 68: <https://securingdemocracy.gmfus.org/hamilton-dashboard/>

Misinformation Directory: <https://www.factcheck.org/2017/07/websites-post-fake-satirical-stories>

News Guard: <https://www.newsguardtech.com>

Repositories containing IRA datasets: Grafika Information Operations Archive (2018 Twitter and Reddit IRA datasets), 538 list of IRA tweets (2012–2018), Ushadrons (-2018)

StopFake: <https://www.stopfake.org/en/main/>

APPENDIX II. DESCRIPTIVE STATISTICS

Variable	Obs	Mean	Std.	Dev.	Min
Media trust	2,078	3.00e-09	1	-2.263854	1.909645
Institutional trust	2,078	-3.78e-09	1	-2.743565	2.206648
Male	2,078	.5409047	.4984439	0	1
Age	2,078	40.21752	15.03124	18	79
Education:					
Bachelor's degree	2,078	.3118383	.4633557	0	1
Degree higher than a master's	2,078	.0322425	.1766861	0	1
Less than a high school diploma	2,078	.0202117	.1407578	0	1
Master's degree	2,078	.1564004	.3633219	0	1
Regular high school diploma	2,078	.1515881	.3587075	0	1
Some college, no degree	2,078	.2853705	.4516994	0	1
Vocational school/ union certificate	2,078	.0423484	.2014313	0	1
Class:					
Lower class	2,048	.1293945	.3357181	0	1
Middle class	2,048	.4448242	.4970677	0	1
Upper class	2,048	.0717773	.2581819	0	1
Working class	2,048	.3540039	.4783271	0	1
Race:					
American Indian or Alaska Native	2,078	.0178056	.1322761	0	1
Asian	2,078	.0615977	.2404813	0	1
Black, or African American	2,078	.1506256	.3577697	0	1
Pacific Islander	2,078	.0009625	.0310161	0	1
Some other race	2,078	.0413859	.1992291	0	1
White	2,078	.7276227	.4452902	0	1
Place of residence:					
A large central city (over 250,000)	2,078	.2954764	.4563664	0	1
A medium size city (50,000 to 249,999)	2,078	.1102021	.3132169	0	1
A suburb of a large central city	2,078	.2285852	.4200225	0	1
A suburb of a medium size city	2,078	.1116458	.315006	0	1
A town or village (2,500 to 9,999)	2,078	.0481232	.214078	0	1
Rural area less than 10 miles from the	2,078	.0611165	.2396015	0	1
Rural area more than 10 miles from the	2,078	.0240616	.1532773	0	1
Small city or town (10,000 to 49,999)	2,078	.1207892	.3259606	0	1
Income:					
\$150,000 or more	2,078	.0890279	.2848526	0	1
\$100,00-\$149,999	2,078	.1179018	.3225695	0	1
\$75,000-\$99,999	2,078	.1366699	.3435812	0	1
\$50,000-\$74,999	2,078	.1857555	.3890029	0	1
below -\$49,999	2,078	.4706449	.4992577	0	1

Ideology:					
Very liberal	2,019	.1872214	.3901858	0	1
Liberal	2,019	.1475978	.3547887	0	1
Somewhat liberal	2,019	.1208519	.3260358	0	1
Middle of the road	2,019	.268945	.4435212	0	1
Somewhat conservative	2,019	.0797424	.2709612	0	1
Conservative	2,019	.1005448	.3007996	0	1
Very conservative	2,019	.0950966	.293421	0	1

Table 10. Descriptive Statistics

APPENDIX III. BASIC DEMOGRAPHIC CHARACTERISTICS AND ENGAGEMENT WITH RUSSIA-ALIGNED CONTENT

	(1) Original sample	(2) Pew-weights ad- justed sample
male	2.044 (1.304)	3.355*** (1.760)
age	-0.349 (0.255)	-0.405 (0.334)
age squared	0.005*** (0.003)	0.005 (0.003)
Bachelor's degree	-1.604 (2.162)	-1.333 (2.094)
Less than a high school diploma	-3.647 (3.011)	-1.390 (2.532)
Master's degree	0.990 (2.210)	1.694 (1.783)
Regular high school diploma	0.948 (3.422)	4.203 (4.825)
Some college, no degree	-0.021 (2.558)	0.365 (2.109)
Vocational school/ union certificate	1.086 (3.524)	1.782 (2.867)
Lower class	5.682*** (2.695)	5.232*** (2.658)
Middle class	2.150 (1.350)	1.909 (1.294)
Working class	2.767 (1.709)	1.981 (1.836)
American Indian or Alaska Native	1.195 (2.890)	1.240 (2.699)
Asian	6.285 (5.693)	9.086 (8.558)
African American	2.811*** (1.589)	1.677 (1.573)
Pacific Islander	2.669 (3.824)	6.122 (6.456)

The Kremlin's Social Media Influence inside the United States: A Moving Target

Some other race	-0.139	-0.486
	(1.369)	(1.573)
Medium size city (50,000 to 249,999)	-0.829	-0.811
	(1.302)	(1.267)
Suburb of a large central city	5.122***	6.549***
	(1.844)	(2.483)
Suburb of a medium size city	2.217	1.629
	(1.647)	(1.444)
Town or village (2,500 to 9,999)	3.724	3.675
	(3.077)	(3.112)
Rural area less than 10 miles from the closest town	2.465	2.896
	(2.265)	(2.384)
Rural area more than 10 miles from the closest town	-2.406	-1.006
	(1.894)	(2.206)
Small city or town (10,000 to 49,999)	3.453***	3.321***
	(1.926)	(1.641)
below -\$49,999	0.670	-1.115
	(2.684)	(3.170)
\$50,000-\$74,999	-0.809	-1.719
	(2.429)	(2.409)
\$75,000-\$99,999	1.190	3.115
	(2.844)	(4.012)
\$100,000-\$149,999	-0.594	-0.786
	(1.962)	(1.979)
Twitter Usage Frequency	4.067***	3.675***
	(0.526)	(0.497)
Oct 24	6.961	5.983
	(5.332)	(4.727)
Oct 25	4.642***	4.375***
	(2.683)	(2.294)
Oct 26	6.631***	8.740***
	(2.166)	(4.150)
Oct 27	6.425***	6.363***
	(1.765)	(2.020)
Oct 28	8.642***	8.113***
	(2.178)	(2.220)
Oct 29	4.077***	3.424
	(1.952)	(2.738)
Oct 30	7.543***	5.031

	(4.414)	(5.110)
Oct 31	-3.268	-5.807
	(5.848)	(8.336)
Nov 01	-4.044	-0.471
	(3.275)	(5.331)
Nov 02	4.215	1.798
	(3.280)	(5.022)
Nov 03	3.956***	2.753
	(1.628)	(1.913)
Nov 04	10.589	10.300
	(6.515)	(6.576)
Nov 05	6.795	4.999
	(4.176)	(4.143)
Nov 06	18.218	16.702
	(16.836)	(14.048)
Nov 07	3.611	4.574
	(3.750)	(4.782)
Nov 08	4.985	4.744
	(4.682)	(4.170)
Nov 09	6.789***	5.000
	(2.511)	(3.220)
Nov 10	2.833	1.795
	(1.862)	(2.512)
Nov 11	3.759***	3.179
	(1.545)	(1.960)
Nov 12	2.457	1.841
	(1.668)	(2.162)
Constant	-15.541***	-12.654
	(6.873)	(8.687)
Observations	2,048	2,048
R-squared	0.0452	0.0458

*** p<0.1, ** p<0.01, * p<0.05

Table 11. OLS regression model explaining engagement with Russia-Aligned Accounts (Basic Demographic Characteristics) with day fixed effects

APPENDIX IV. IDEOLOGY AND ENGAGEMENT WITH RUSSIA-ALIGNED CONTENT

	(1) Original sample	(2) Pew-weights adjusted sample
Very liberal	3.817*** (1.812)	4.119*** (1.827)
Liberal	1.996 (2.767)	4.905 (5.380)
Somewhat liberal	-0.360 (1.415)	-1.006 (1.501)
Somewhat conservative	-2.796*** (1.172)	-2.433*** (1.197)
Conservative	1.735 (2.046)	2.696 (2.202)
Very conservative	4.585 (2.822)	4.129 (2.537)
male	2.254*** (1.278)	3.334*** (1.552)
age	-0.311 (0.258)	-0.380 (0.344)
age squared	0.005*** (0.003)	0.005 (0.003)
Bachelor's degree	-0.754 (2.125)	-0.294 (1.900)
Less than a high school diploma	-0.451 (3.339)	2.292 (2.841)
Master's degree	0.962 (2.216)	1.748 (1.799)
Regular high school diploma	2.364 (3.678)	5.724 (5.323)
Some college, no degree	1.432 (2.527)	1.808 (2.106)
Vocational school/ union certificate	2.968 (3.580)	3.779 (3.045)
American Indian or Alaska Native	1.520 (2.789)	1.995 (2.601)
Asian	6.472	9.629

	(5.959)	(9.034)
African American	2.688***	1.498
	(1.615)	(1.656)
Pacific Islander	0.848	3.074
	(3.991)	(4.522)
Some other race	-0.714	-1.119
	(1.413)	(1.725)
Medium size city (50,000 to 249,999)	-0.360	-0.324
	(1.338)	(1.213)
Suburb of a large central city	5.547***	7.070***
	(1.921)	(2.718)
Suburb of a medium size city	2.461	1.903
	(1.702)	(1.494)
Town or village (2,500 to 9,999)	3.140	3.193
	(3.065)	(3.098)
Rural area < 10 miles from the closest town	2.634	3.136
	(2.390)	(2.505)
Rural area > 10 miles from the closest town	-2.636	-1.117
	(1.965)	(2.337)
Small city or town (10,000 to 49,999)	3.849***	3.986***
	(2.006)	(1.781)
below -\$49,999	2.171	0.110
	(2.762)	(3.648)
\$50,000-\$74,999	0.163	-1.077
	(2.444)	(2.629)
\$75,000-\$99,999	2.259	3.988
	(2.761)	(3.837)
\$100,000-\$149,999	0.026	-0.408
	(1.995)	(2.084)
Twitter Usage Frequency	3.884***	3.541***
	(0.525)	(0.505)
Oct 24	3.703	3.349
	(6.144)	(5.562)
Oct 25	1.602	1.692
	(3.820)	(3.623)
Oct 26	4.122	6.679
	(3.625)	(5.450)
Oct 27	3.812	4.191
	(3.261)	(3.388)

Oct 28	5.987***	5.883***
	(3.532)	(3.562)
Oct 29	1.603	1.418
	(3.255)	(3.487)
Oct 30	4.315	2.305
	(5.286)	(5.648)
Oct 31	-6.179	-8.066
	(5.998)	(7.620)
Nov 01	-6.429	-2.066
	(4.644)	(7.141)
Nov 02	1.944	-0.162
	(4.205)	(5.224)
Nov 03	0.887	0.355
	(3.158)	(3.133)
Nov 04	8.681	9.395
	(7.444)	(7.860)
Nov 05	3.543	1.950
	(5.002)	(4.860)
Nov 06	21.766	19.756
	(22.346)	(18.568)
Nov 07	0.443	0.791
	(5.134)	(6.604)
Nov 08	1.191	-0.346
	(6.105)	(5.399)
Nov 09	3.816	2.399
	(3.724)	(3.947)
Nov 10	-0.040	-0.290
	(3.252)	(3.331)
Nov 11	1.024	0.929
	(3.140)	(3.211)
Nov 12	-0.369	-0.443
	(3.153)	(3.196)
Constant	-13.832***	-11.962
	(6.957)	(8.019)
Observations	2,019	2,019
R-squared	0.050	0.052

*** p<0.1, ** p<0.01, * p<0.05

Table 12. OLS regression model explaining engagement with Russia-Aligned Accounts (Ideology) with day fixed effects

APPENDIX V. IDEOLOGY AND TRUST IN MEDIA AND INSTITUTIONS (OLS MODEL)

	(1) Original sample	(2) Pew- weights	(3) Original sample	(4) Pew- weights	(5) Original sample	(6) Pew- weights
Media trust	-1.450*** (0.620)	-1.465*** (0.602)			-0.105 (0.793)	-0.610 (1.002)
Institutional trust			-2.344*** (0.591)	-1.801*** (0.698)	-2.284*** (0.760)	-1.454 (1.086)
Very liberal	4.111*** (1.830)	4.370*** (1.855)	3.667*** (1.820)	4.041*** (1.842)	3.692*** (1.872)	4.161*** (1.940)
Liberal	2.334 (2.802)	5.190 (5.426)	2.212 (2.749)	5.053 (5.351)	2.231 (2.826)	5.143 (5.466)
Somewhat liberal	-0.079 (1.423)	-0.820 (1.495)	-0.413 (1.399)	-1.113 (1.477)	-0.391 (1.413)	-1.015 (1.435)
Somewhat conservative	-3.343*** (1.179)	-2.957*** (1.173)	-2.876*** (1.183)	-2.475*** (1.207)	-2.913*** (1.144)	-2.685*** (1.112)
Conservative	0.866 (1.948)	1.842 (2.071)	1.900 (2.034)	2.904 (2.173)	1.832 (1.919)	2.509 (1.935)
Very conservative	3.675 (2.659)	3.252 (2.361)	4.814*** (2.816)	4.421*** (2.524)	4.742*** (2.681)	3.999*** (2.318)
Male	2.195*** (1.274)	3.273*** (1.542)	2.025 (1.273)	3.162*** (1.580)	2.027 (1.275)	3.170*** (1.587)
Age	-0.297 (0.259)	-0.374 (0.344)	-0.310 (0.258)	-0.387 (0.342)	-0.309 (0.257)	-0.383 (0.339)
Age squared	0.005 (0.003)	0.005 (0.003)	0.005 (0.003)	0.005 (0.003)	0.005 (0.003)	0.005 (0.003)
Bachelor's degree	-0.931 (2.105)	-0.585 (1.915)	-0.776 (2.089)	-0.446 (1.867)	-0.788 (2.099)	-0.538 (1.921)
Less than a high school diploma	-1.177 (3.296)	1.474 (2.782)	-0.671 (3.306)	2.033 (2.827)	-0.718 (3.227)	1.743 (2.708)
Master's degree	1.032 (2.190)	1.735 (1.793)	1.499 (2.194)	2.050 (1.805)	1.490 (2.199)	1.986 (1.821)
Regular high school diploma	2.122 (3.656)	5.298 (5.259)	2.230 (3.661)	5.387 (5.404)	2.216 (3.644)	5.274 (5.277)
Some college, no degree	1.040 (2.490)	1.267 (2.080)	1.165 (2.488)	1.392 (2.069)	1.143 (2.484)	1.247 (2.069)
Vocational school/ union certificate	2.653 (3.535)	3.246 (2.987)	3.103 (3.545)	3.645 (3.037)	3.077 (3.509)	3.449 (2.936)

The Kremlin's Social Media Influence inside the United States: A Moving Target

American Indian or Alaska Native	1.582	2.048	1.272	1.712	1.283	1.788
	(2.720)	(2.535)	(2.721)	(2.548)	(2.726)	(2.564)
Asian	6.356	9.508	6.527	9.640	6.517	9.588
	(5.946)	(9.011)	(5.963)	(9.048)	(5.932)	(8.979)
Black, or African American	2.947***	1.774	2.473	1.316	2.498	1.466
	(1.617)	(1.634)	(1.594)	(1.621)	(1.586)	(1.540)
Pacific islander	0.636	3.034	0.121	3.019	0.125	3.013
	(4.243)	(4.762)	(5.496)	(5.504)	(5.482)	(5.418)
Some other race	-0.882	-1.219	-1.506	-1.641	-1.497	-1.582
	(1.429)	(1.739)	(1.439)	(1.675)	(1.431)	(1.635)
Medium size city (50,000 to 249,999)	-0.649	-0.610	-1.076	-0.907	-1.079	-0.913
	(1.339)	(1.228)	(1.381)	(1.199)	(1.378)	(1.201)
Suburb of a large central city	5.174***	6.679***	4.892***	6.489***	4.882***	6.438***
	(1.860)	(2.645)	(1.929)	(2.842)	(1.892)	(2.780)
Suburb of a medium size city	2.095	1.529	1.817	1.455	1.807	1.385
	(1.701)	(1.515)	(1.718)	(1.478)	(1.711)	(1.494)
Town or village (2,500 to 9,999)	2.702	2.820	2.275	2.597	2.265	2.557
	(3.020)	(3.059)	(3.028)	(3.040)	(3.018)	(3.035)
Rural area < 10 miles from the closest town	2.052	2.442	2.008	2.531	1.982	2.359
	(2.441)	(2.564)	(2.453)	(2.578)	(2.452)	(2.578)
Rural area > 10 miles from the closest town	-3.133	-1.553	-3.316	-1.578	-3.334	-1.671
	(1.998)	(2.338)	(2.077)	(2.471)	(2.041)	(2.395)
Small city or town (10,000 to 49,999)	3.545***	3.672***	3.155	3.440***	3.151	3.414***
	(1.998)	(1.782)	(2.045)	(1.867)	(2.038)	(1.856)
below -\$49,999	-0.116	-1.289	-0.872	-1.769	-0.865	-1.724
	(2.449)	(2.649)	(2.407)	(2.524)	(2.399)	(2.486)
\$50,000-\$74,999	1.886	3.644	1.361	3.386	1.357	3.359
	(2.743)	(3.794)	(2.819)	(3.983)	(2.811)	(3.953)
\$75,000-\$99,999	3.973***	3.632***	3.995***	3.626***	3.999***	3.647***
	(0.534)	(0.510)	(0.540)	(0.521)	(0.537)	(0.514)
\$100,000-\$149,999	-0.320	-0.761	-0.716	-0.970	-0.722	-1.009
	(2.023)	(2.132)	(1.987)	(2.038)	(1.998)	(2.064)
Twitter Usage frequency	1.321	1.347	0.613	1.037	0.618	1.020
	(3.871)	(3.639)	(3.821)	(3.668)	(3.831)	(3.678)
Oct 24	3.762	6.286	2.916	5.747	2.921	5.763
	(3.657)	(5.411)	(3.701)	(5.664)	(3.721)	(5.692)
Oct 25	3.555	3.954	2.648	3.418	2.659	3.468
	(3.340)	(3.431)	(3.303)	(3.438)	(3.320)	(3.475)

Maria Snegovaya, Kohei Watanabe

Oct 26	5.616 (3.574)	5.467 (3.573)	4.704 (3.512)	4.940 (3.607)	4.710 (3.525)	4.948 (3.627)
Oct 27	1.123 (3.322)	0.921 (3.535)	0.378 (3.259)	0.592 (3.415)	0.375 (3.265)	0.544 (3.446)
Oct 28	4.144 (5.406)	1.982 (5.759)	3.411 (5.392)	1.514 (5.624)	3.422 (5.390)	1.532 (5.635)
Oct 29	-6.077 (6.098)	-7.883 (7.664)	-5.264 (6.221)	-7.398 (7.946)	-5.281 (6.256)	-7.450 (7.986)
Oct 30	-6.634 (4.662)	-2.362 (7.103)	-5.928 (4.560)	-1.817 (7.041)	-5.956 (4.495)	-1.988 (6.865)
Oct 31	1.261 (4.257)	-0.942 (5.312)	0.704 (4.165)	-1.228 (5.019)	0.686 (4.185)	-1.347 (5.127)
Nov 01	0.527 (3.225)	0.038 (3.180)	-0.258 (3.176)	-0.533 (3.127)	-0.254 (3.184)	-0.494 (3.149)
Nov 02	8.712 (7.484)	9.425 (7.882)	8.502 (7.359)	9.244 (7.791)	8.509 (7.367)	9.285 (7.819)
Nov 03	3.132 (4.988)	1.568 (4.855)	2.085 (4.889)	0.998 (4.719)	2.093 (4.898)	1.022 (4.725)
Nov 04	20.493 (22.575)	18.410 (18.731)	19.593 (21.988)	18.093 (18.383)	19.557 (22.124)	17.853 (18.514)
Nov 05	0.145 (5.300)	0.296 (6.996)	-0.511 (5.574)	0.098 (6.913)	-0.508 (5.574)	0.025 (7.023)
Nov 06	0.046 (6.191)	-1.589 (5.413)	-0.204 (5.940)	-1.353 (5.250)	-0.251 (5.963)	-1.677 (5.316)
Nov 07	3.487 (3.782)	2.042 (3.989)	2.737 (3.724)	1.642 (3.868)	2.741 (3.730)	1.639 (3.884)
Nov 08	-0.316 (3.334)	-0.560 (3.383)	-1.286 (3.287)	-1.180 (3.339)	-1.274 (3.301)	-1.121 (3.365)
Nov 09	0.622 (3.216)	0.486 (3.255)	-0.241 (3.166)	-0.034 (3.184)	-0.238 (3.173)	-0.033 (3.204)
Nov 10	-0.555 (3.242)	-0.615 (3.248)	-0.821 (3.199)	-0.671 (3.215)	-0.823 (3.206)	-0.699 (3.236)
Nov 11						
Nov 12	-13.169*** (6.936)	-10.998 (8.060)	-11.120*** (6.688)	-9.662 (7.497)	-11.142*** (6.685)	-9.704 (7.477)
Observations	2,019	2,019	2,019	2,019	2,019	2,019
R-squared	0.052	0.054	0.056	0.055	0.056	0.055

*** p<0.1, ** p<0.01, * p<0.05

Table 13. OLS Regression Model Explaining Engagement with Russia-Aligned Accounts (Trust in Media) With Day Fixed Effects

**FREE
RUSSIA**



www.4freerussia.org
info@4freerussia.org