Research Report

MAREK N. POSARD, MARTA KEPE, HILARY REININGER, JAMES V. MARRONE, TODD C. HELMUS, AND JORDAN R. REIMER

From Consensus to Conflict

Understanding Foreign Measures Targeting U.S. Elections

Throughout the remaining U.S. political campaign season of 2020, Russia might try again to manipulate and divide U.S. voters through social media. This report is the first in a four-part series aimed at helping policymakers and the public understand—and mitigate—the threat of online foreign interference in national, state, and local elections.[1]

Concerns over foreign influence in U.S. politics date back to the founding of this country. Alexander Hamilton warned about "the desire in foreign powers to gain an improper ascendant in our councils" (Hamilton, 1788). George Washington's farewell speech cautioned that "foreign influence is one of the most baneful foes of republican government" (Washington, 1796). During the Civil War, the Confederacy solicited the support of Britain and France against the Union (Central Intelligence Agency, undated). In 1940, the British covertly intervened in the U.S. presidential election in hopes to garner support for U.S. intervention in World War II (Usdin, 2017). During the Cold War, the Soviet Union operated a sophisticated program involving covert and overt information efforts against the United States (Jones, 2019; Schoen and Lamb, 2012).

More recently, the U.S. Senate Committee on Intelligence presented evidence that Russia directed

KEY FINDINGS

- Foreign interference in U.S. politics has been a concern since the nation was founded.
- Russian information efforts aim to elicit strong reactions and drive people to extreme positions to lower the odds they will reach a consensus—the bedrock of U.S. democracy.
- New technologies have made Russia's information efforts easier to implement than the propaganda campaigns that the Soviets conducted during the Cold War.
- Studies about how to defend against these efforts have focused on different units of analysis: Some studies focus on the original content; others focus on how this content spreads within networks; and still others focus on protecting consumers.
- To respond to foreign interference, we recommend (1) taking a holistic approach that anticipates which groups of Americans are likely to become targets and (2) designing evidence-based preventive practices to protect them.

activities against state and local election infrastructures and tried to spread disinformation on social media during the 2016 presidential election (Select Committee on Intelligence of the United States Senate, 2019, undated, 2020). In 2018, the Department of Justice indicted the Internet Research Agency LLC, located in St. Petersburg, Russia, for interfering in U.S. elections as far back as 2014 (*United States v. Internet Research Agency LLC*, 2018).

Given these past and likely extant threats to U.S. elections, the California Governor's Office of Emergency Services asked the RAND Corporation's National Security Research Division for research to help them analyze, forecast, and mitigate threats by foreign actors targeting local, state, and national elections.

This four-part series (Figure 1) will present

- what the literature says about information efforts by foreign actors
- the results of an analysis of social media to identify potential exploits
- a survey experiment to assess interventions to defend against some of these exploits
- qualitative interviews of survey respondents to understand their views on falsehoods.

In this report, we review some of the research on information efforts by foreign actors, focusing mainly on online environments.[2] First, we review what we believe is the intellectual basis of existing Russian information efforts: reflexive control theory.[3] Second, we review examples of information efforts by the Soviet Union and Russian Federation. Third, we review select research on strategies that inform how to defend against online information efforts.

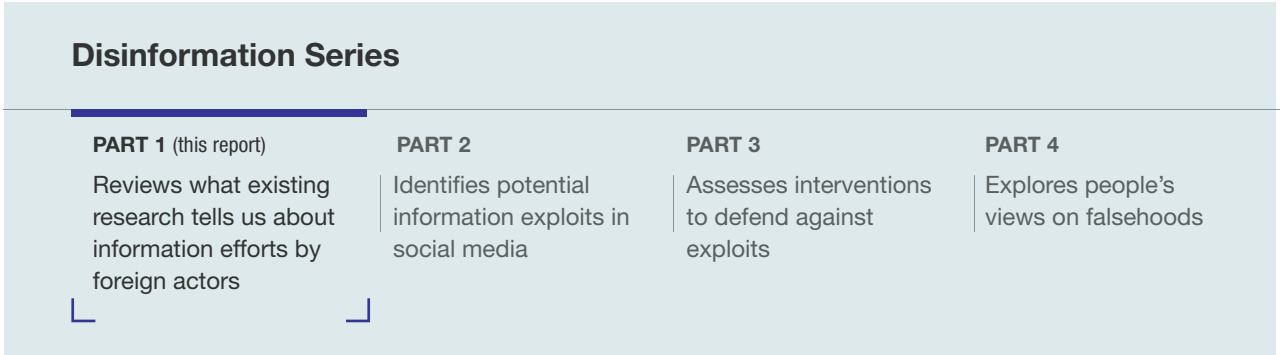
We recommend that any strategies for responding to foreign information efforts be broad rather than narrow and that they anticipate which subgroups of Americans are likely targets of information efforts by foreign adversaries. Additionally, there is a need to develop evidence-based preventive interventions for those who are most likely targets within our society.

Modern Methods Are Rooted in the Cold War

We believe that reflexive control theory is, in part, the intellectual basis of current information efforts targeting the United States that are perpetrated by Russia and its proxies.[4] Scholars have described *reflexive control* as a means of conveying information to others that leads them to make some predetermined decision (Thomas, 2004). *Reflexive control theory* is a formal theoretical research program exploring this technique; it was developed by Vladimir Lefebvre and others and first appeared in Soviet military literature in the 1960s (Chotikul, 1986; Radin, Demus, and Marcinek, 2020; Thomas, 2004). Unlike game theory, this theory does not assume that individuals act rationally; rather, it assumes that people act "according to their image of the world and their image of their adversary's image of the world."[5] (Appendix A has a more detailed description of the reflexive control theory.)

In general, reflexive control theory presents the world as a set of binary relationships: People are

FIGURE 1
What This Series Covers



either in conflict or cooperation with one another, and their actions are either passive or aggressive in nature (Lefebvre, 1965, 1966). Although the binary view is an oversimplification, this assumption is based on how some historians characterize human relationships in the Soviet Union.[6]

The model structure implies that a person's decisions depend on what is socially desirable, insofar as they perceive what is desirable to others. Outside parties can manipulate this perception, which forms the basis for reflexive control as a tool for understanding information efforts. Belief in falsehoods is merely a byproduct of reflexive control, not the end goal. Disseminating false content is a tactic to manipulate one group's view of others.

We have identified at least two key features of reflexive control theory that seem applicable to recent information efforts targeting U.S. elections.

One Feature of Reflexive Control Theory Is to Alter People's Perceptions

First, the model accepts as a given that relationships between individuals are defined by conflict or collaboration. The interpersonal influences between groups of people are inputs. Information efforts are trying to shift people's perceptions, not alter this fundamental group structure. For example, reflexive control does not try to convince people in political party A that they are in conflict with those from political party B. It assumes this conflict already exists. Instead, these information efforts try to amplify the degree that people from party A believe that those from party B view them as adversaries.

Another Feature Is to Elicit Reactions, Not Necessarily to Change Behavior

The second relevant feature of reflexive control theory is the goal of eliciting reactions from targets. The theory views the world as a dichotomy between conflict and collaboration. Successful information efforts sow deep divisions between groups of people and generate a perception of "us" versus "them" that, in turn, elicits strong reactions in people. The ultimate goal is to reduce the probability that groups of people find common ground on issues of public concern. After all, it's difficult to find commonality on such topics as property taxes or farm subsidies when opponents see each other as un-American or racist and each believes these views are deep-seated within the other.

This binary framework also suggests a direct way to operationalize reflexive control. Manipulating someone's perception of others is most feasible, and most effective, if that perception can be collapsed into a one-dimensional caricature. If someone is "one of them" and if "they" are a monolithic group easily summarized by one characteristic, then perceptions are more easily manipulated and reinforced. Thus, we hypothesize that reflexive control in practice is a priming technique that encourages people to self-identify with a particular group and to simplify the characterization of that group as homogenous and ultimately in conflict with another group.

Thus, foreign adversaries might try to operationalize reflexive control by targeting those who are likely to have the strongest reactions to group-based differences. The sources of these differences are broad: They might focus on race, class, gender, sexual orientation, political affiliation, or geography

Defining Key Concepts

- **Information efforts:** Activities that "influence, disrupt, corrupt, or usurp the decision-making of targets while protesting one's own" (Chairman of the Joint Chiefs of Staff, 2014, p. A-1).
- **Creation and dissemination:** Content—which might be authentic (for example, created by human users or trolls) or inauthentic (for example, created by bots)—is created and disseminated by state-sponsored actors or their proxies (who could be willing or unwilling participants).
- **Information environment:** The area in which information efforts exist, broadly defined as "the aggregate of individuals, organizations, and systems" (Chairman of the Joint Chiefs of Staff, 2014, p. GL-6). These environments involve any collection of people who interact with each other online or in person.

Active measures are covert and overt information efforts organized by a government to affect a target's domestic and foreign politics and are used as an instrument of power.

(urban versus rural dwellers). Foreign information efforts might target these differences by activating the salient group identity within them and framing this identity as being in conflict with people in other groups. By diminishing consensus, adversaries can potentially cause political paralysis.

These tactics and goals are reflected in the observations of researchers who have tracked Russian information efforts over the past several years. The extensive use of memes focusing on particular groups and repeatedly characterizing them in particular ways works to create a simple but consistent framing of that group. These framings tend to have high emotional resonance and often involve passive statements about identity (as opposed to calls for action). They prime the viewer to think about "us" versus "them" in ways that assume the viewer already knows who "we" and "they" are.[7] The uses of cross-platform communication and consistent cross-platform branding give the impression that these characterizations are more universal than they actually are.[8]

Russia is not the only foreign actor who conducts information efforts (see Appendix B for brief descriptions of efforts by China, Iran, and Venezuela), but it appears Russia has been an active presence in the United States in recent years (*United States v. Internet Research Agency LLC*, 2018; Select Committee on Intelligence of the United States Senate, 2019, undated). Furthermore, we believe that Russia is an equal opportunity exploiter of social cleavages, as evidenced by reporting that online Russian trolls appeared to have targeted white supremacists and civil rights activists (Derysh, 2020; Glaser, 2018; Lockhart, 2018; Ward, 2018). In the next section, we discuss some of the ways that Russia and its proxies appear to conduct these efforts within the United States.

Russia's Aim Is to Preserve the Regime by Weakening the West

Russia has long used various forms of active measures—a specific term that falls within the broader category of information efforts—against the United States, with a focus on U.S. domestic issues. *Active measures* (in Russian, *aktivinyye meropriatia* or *aktivka*) are covert and overt information efforts organized by a government to affect a target's domestic and foreign politics and are used as an instrument of power (Godson and Shultz, 1985). These measures have helped shape the course of international and domestic events in Russia's favor and helped subvert actions and trends that contradict the government's intentions.

Although many countries have sought to use active measures, the Soviet Union and then Russia institutionalized them over many decades and advanced them into a comprehensive foreign policy tool, particularly against the United States (Allen and Moore, 2018). This tool is used to undermine democratic governance processes in the United States and its allies with the overarching aim of weakening the United States and advancing Russia as a global power. This would then support Russia's view of itself as the promoter of a world order and values that are alternative to the ones represented by the United States and its allies and their view of the liberal rules-based world order (Government of Russia, 2016; Radin and Reach, 2017; Stent, 2019).

This section is divided into two parts. First, we discuss the objectives of Russian information efforts in the post–Cold War era. Second, we review some of the ways that Russia has applied these efforts against the United States. The research for this section draws on open-source publications, such as official documents,

research reports and analysis, and commentary and case study databases by Western and Russian authors.

Russian Information Efforts Reflect Four Objectives

In general, a key strategic aim of Russia's information efforts is to ensure the survival of its regime and diminish the global dominance of the United States and its allies. Russia seeks to make Western-style democracy less attractive by damaging the global status of the United States, destabilizing it internally, and weakening its unity with Western allies (Taylor, 2019). Russia seeks to achieve these aims by using asymmetric and often long-term methods, which are sowing discord, undermining democratic forms of governance, and seeking to compromise the core values of the United States (Jenkins, 2019). Moreover, examples of active measures toward Europe suggest that the aims of information efforts could be "opaque, as they are designed to produce second- and third-order effects" (Pomerantsev, 2015b). In reality, that plays out as the target continually guesses the real purpose of the information efforts targeted against it.[9]

Open-source reports crystalize Russia's four main objectives for its active measures in the United States:[10]

1. Polarize and disrupt societal cohesion by exacerbating important and divisive issues, such as race, social class, and gender.
2. Undermine public confidence in democratic institutions and processes.
3. Spread confusion, generate exhaustion, and create apathy.
4. Gain strategic influence over U.S. political decisionmaking and public opinion.

Polarize and Disrupt Societal Cohesion by Exacerbating Divisive Issues

Russia seeks to manipulate important and divisive social and political issues as a way to alter public opinion, create and exacerbate fissures, and disrupt political processes. According to Russian author Alexander Doronin, subversion by inflating conflict situations, specifically ones that encourage the feelings of infringement and dissatisfaction with those who are perceived to be more privileged, might lead to the creation of a "fifth column"—a group that is sympathetic to or works in favor of the adversary (Doronin, 2010).

Example 1

An Argument for Every Audience

During the 2016 presidential election, politically right-leaning groups were targeted with conspiracy theories about voter fraud and election stealing. The narratives targeting African Americans were largely apolitical but included attempts at voter suppression through discouraging them from voting altogether. Politically left-leaning populations were targeted with tailored anti-establishment narratives. Lesbian, gay, bisexual, transgender, and other (LGBT+) populations, Native Americans, and Muslims were targeted with tailored narratives emphasizing the identity and pride of these groups. (DiResta et al., 2019)

Open-source reports indicate that Russian-backed attempts to sow discord in U.S. society have largely focused on exploiting racial and immigration issues and that they both make use of existing extremist movements across the U.S. political ideological spectrum and create new such movements. Russian-backed efforts have even promoted secessionist initiatives (e.g., CalExit and Texit) (Yates, 2017). Russia and its proxies use the strategies of generating extreme anger and suspicion on political issues when trying to co-opt some politically right-leaning groups. When targeting some in the African American community, it has tried to build on the issues of societal alienation and police brutality (Lockhart, 2018).

Undermine Public Confidence in Democratic Institutions and Processes

The Russian government seeks to undermine the U.S. democratic system and institutions by disrupting public trust and manipulating the public's lack of familiarity with the institutions and processes (Spaulding, Nair, and Nelson, 2019; Thomas, 2015).[11] It tries to achieve this by exploiting the vulnerabilities of a democratic governance system, especially populist agendas (Aceves, 2019; Conley et al., 2019; Endicott, 2017). Studies on Russian influence in Europe have found that unstable and weak democratic institutions

Example 2

Voter Fraud and Suppression

During the 2016 elections, Russia-backed actors appeared to have promoted anti-establishment sentiments and slandered the U.S. intelligence community. Several reports observe that digital voter suppression campaigns, mostly done via social networking platforms, specifically targeted African Americans in an attempt to alienate them from government institutions and cause them to doubt the influence of their votes. (DiResta et al., 2019; Conley et al., 2019; Root and Barclay, 2018)

and political and economic volatility make a country more vulnerable to Russian influence, manipulation, and even state capture (Conley et al., 2019). Disinformation has become a key part of undermining trust between society and government institutions in democratic countries. Some Western authors draw a link between the spread of disinformation and declining citizen confidence, which further undermines trust in official information sources and pushes people toward so-called alternative news sources (Bennett and Livingston, 2018).

Spread Confusion, Generate Exhaustion, and Generate Apathy

Spreading confusion and obfuscation, specifically through disruption or denigration of truthful reporting, is one part of Russia's contemporary propaganda model (Paul and Matthews, 2016). Over time, it appears that Russia has become more confident in using falsehoods to make people confused, paranoid, and passive and to reduce their ability to understand what is true and create a perception that "nothing is ever knowable" (Endicott, 2017; Paul and Matthews, 2016; Soufan Center, 2018). Disseminating intentionally false news stories online and in traditional media can give repeated falsehoods legitimacy and has the potential to create an environment of confusion and disorientation (Bennett and Livingston, 2018). Confusion is directly relevant to the ability to make decisions. One Russian author writes that decisionmaking is greatly affected by the level of confidence in signs and their meanings—i.e., confidence about

Example 3

Denial and Distraction

When accused of shooting down a Malaysia Airlines jet over Ukraine in 2014, Russia's response was to overwhelm the audience with alternative accusations (Pomerantsev, 2014).

reality, meaning, and facts (Karjukin and Chausov, 2017). Likewise, Western marketing literature speaks about "consumer confusion" through information overload and ambiguous and misleading information, making consumers less likely to make rational choices, less decisive, more anxious, and exhibiting lower levels of trust and understanding (Walsh and Mitchell, 2010). This is in line with RAND's recent Truth Decay research about the growing conflict between fact and opinion, the increasing volume of opinion over fact, and the public's diminishing trust in factual information (Kavanagh and Rich, 2018).

Gain Strategic Influence over U.S. Political Decisionmaking and Public Opinion

Russia seeks to gain strategic influence in the U.S. decisionmaking process by developing access to policymaking circles and influential groups and increasing control over U.S. public opinion. These targets are assets that might knowingly or unknowingly help Russia gain long-term political influence through Russia's making relatively low-profile investments today. For example, Russian agent Maria Butina was sentenced to 18 months in prison in 2019 and then deported after the U.S. Department of Justice accused her of "infiltrating organizations having influence in U.S. politics, for the purpose of advancing the interests of the Russian Federation" (U.S. Department of Justice, 2018; also see Lamond, 2018). Prior to that, Russia attempted to use information efforts to curb fracking in the United States. The decline in oil prices in 2015 had a severe impact on Russia's economy, which is highly dependent on oil and natural gas. One report concluded that Russia exploited genuine concerns about the environmental impact of fracking in its covert efforts to curb the practice, which produces a cheaper source

Example 4

Infiltrating Influential Circles

In 2018, the Department of Justice charged Maria Butina with being a Russian agent and "infiltrating organizations having influence in U.S. politics, for the purpose of advancing the interests of the Russian Federation." The National Rifle Association was one of Butina's targets. (Sullivan, 2019)

of energy that threatens Russia's exports to Europe.[12] As a result, the Department of Justice charged three Russian agents with spying on U.S. "efforts to develop alternative energy resources." Russia's information campaign included releasing a documentary about illnesses allegedly triggered by fracking in the United States using manipulated testimonies from trusted sources (Rogan, 2015). Russia has also sought to support and establish relations with social movements in the United States and Europe that tend to operate outside the traditional political party structure, such as secessionist movements in California and Texas.[13]

Technology Puts New Twists on Cold War Techniques

Although the techniques that were tried and tested during the Cold War have not been forgotten, new technologies and increased cultural and economic links between Russia and the United States offer a wider array of means and methods by which to manipulate information. Interactions today have been augmented with internet-based media, social networking sites, trolls, and bots. Technological development has opened new means of manipulation via information and facilitates more-scalable, bigger, and more-effective operations with minimal expense. The role of the internet has been recognized at the highest levels in Russia. In 2014, Russian President Vladimir Putin noted that "the rapid progress of electronic media has made news reporting enormously important and turned it into a formidable weapon that enables public opinion manipulations" (Pomerantsev, 2015a). One Russian author further elaborates that even small amounts of information distributed during "crisis situations" might lead to serious results (Doronin, 2010).

Russian active measures do still employ more-traditional methods—which in today's world are facilitated by the availability of informal communication networks via economic, cultural cooperation, expatriate, or proxy individuals or groups, as well as other more-conventional means. This seemingly reflects the views of Russian military thinker Colonel S. Leonenko, who pointed out that information technology poses a challenge to reflexive control because computers lack "the intuitive reasoning of a human being" but also offers new methods of influence—e.g., anonymity, whitewashing of false information, and wide dissemination (Thomas, 2004). Different techniques are not isolated from each other, and campaigns often move from the virtual and media environment into the real world by rallying protests online, hiring individuals to organize rallies, or hiring individuals to participate in rallies and protests.

The techniques used might vary because they are tailored to the issue, environment, target, and intended result (Doronin, 2010). Russia uses a wide variety of methods that are tailored to situations, and it continually seeks opportunities to achieve the aims and objectives we have described. Figure 2 displays several widely used techniques identified in open-source reports.

When using these techniques, Russia contacts a variety of individuals and groups from across the political and social spectrum, often reaching for the fringe elements on both the political right and left, even if Russia is not always ideologically aligned with such groups. Its information operation narratives are tailored to different target audiences.

In Europe, for example, Russia has seduced different political groups using anti-EU messages, anti-U.S. hegemony narratives, and appeals to those interested in preventing fracking (which appears to benefit Russia's interest in maintaining European dependence on Russian gas). In the United States, Russia has seduced some religious conservatives with anti-LGBT+ stances (Pomerantsev, 2014).

Several U.S. authors have tackled the relationship between Russia and fringe groups, politically extreme right- and left-leaning groups, the so-called angry young men groups, motorcycle gangs, and fight clubs. They note that these groups might become—sometimes unwittingly—Russia's agents of

FIGURE 2
Overview of Select Russian Active Measures

TAILORED DISINFORMATION

Pit different groups against each other by identifying content and topics to which each targeted group might be most susceptible.

AMPLIFIED CONSPIRATORY NARRATIVES

Promote or denigrate an issue, sow distrust, and spread confusion by disseminating constitutional narratives, rumors, and leaks.

PAID ADVERTISING

Push people to like pages, follow accounts, join events, and visit websites.

AMERICAN ASSET DEVELOPMENT

Reduce the likelihood of detection by recruiting Americans to perform tasks for handlers.

NARRATIVE LAUNDERING

Move a narrative from its state-run origins to the wider media ecosystem through witting or unwitting participants.

HACK AND LEAK OPERATIONS

Illegally procure information and share via platforms such as WikiLeaks.

FALSE ONLINE PERSONAS

Create false personas, sometimes with information that belongs to real people, to hide real identities.

SOCIAL MEDIA GROUPS

Exacerbate existing issues, gather information, and recruit for events by creating social media groups dedicated to divisive issues.

MEMES AND SYMBOLS

Utilize memes to create easy-to-share snippets of information that can emotionally resonate with people.

SECESSIONIST SUPPORT

Undermine the United States by establishing links with and supporting secessionist ideas and movements.

FRINGE MOVEMENT SUPPORT

Build support for Russia's values and society by establishing links to extremist groups.

influence. Michael, 2019, writes that Russia's cultural conservatism, nationalist government, and large white population allows it to be perceived as a potential ally to the political far right in the United States, especially on issues for which some on the political far right feel they are in the minority in a multicultural and liberal environment. According to Carpenter, 2018, manipulating extreme political groups is part of Russia's strategy to undermine Western democratic institutions: Russia seeks out marginal groups and social outcasts who can be motivated to fight the institutions of their own country and amplify divisive narratives, thus providing Russia with a "shield of deniability" that it can use to suggest that any links between Russia and such groups occurred extemporaneously. It is not clear in the literature whether such "partnerships are always marriages of convenience or are genuine partnerships based on shared values" (Carpenter, 2018).

In the next section, we review a sample of recent research to better understand what types of practices might help respond to these information efforts.

Research Focused on Responding to Foreign Election Interference

In this section, we present results from a systematic review of research related to information efforts and foreign election interference. We reviewed a total of 142 documents and focused on 78 that featured data. (For the methodological details of this effort, see Appendix C.) We begin by describing a framework

for organizing this literature, followed by a review of some general trends.

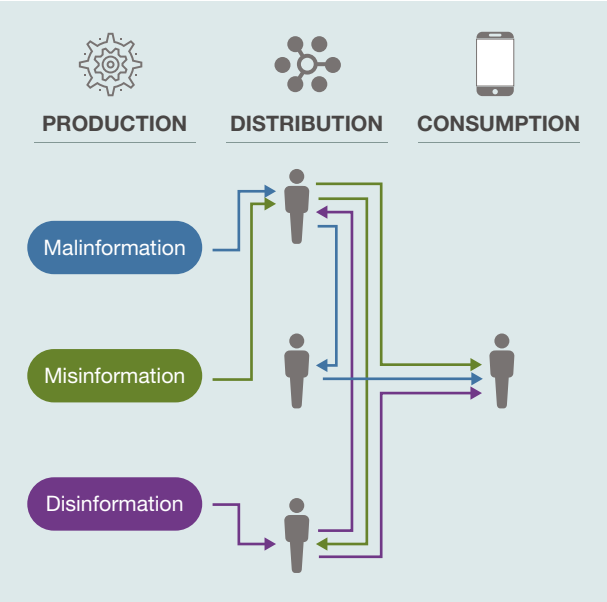
Three Features Describe How Russia's 'Firehose of Falsehoods' Works

Russia's information efforts have been described as a "firehose of falsehood" because they produce large volumes of partial truths and objective falsehoods, continually and repetitively, via multiple channels—e.g., text, video, audio, imagery (Paul and Matthews, 2016).[14] Here, we describe the pathology of this firehose. Figure 3 describes three key features of this pathology: production, distribution, and consumption of content (Matthews et al., forthcoming).

We found that the unit of analysis—defined as the subject (i.e., who or what) of a study—typically differs for each of the three features in Figure 3.[15] For production, the unit of analysis tends to be the content itself, including malinformation (e.g., leaked documents), misinformation (e.g., misleading content that features half-truths), and disinformation (e.g., complete falsehoods, such as forgeries or fictitious-declarative statements). For distribution, the unit of analysis is the social network on which users share original content or create derivative content to share with others.[16] For consumption, the unit of analysis is the individual user who views and shares this content—typically, individual users are the general public who express their support for content but they can also be inauthentic users, such as bots.

The research on foreign information efforts does not always reflect the neatly patterned framework described in Figure 3, and there is no shortage of alternative frameworks and models that describe various features of information efforts. For example, the firehose of falsehood framework characterizes Russian propaganda efforts as producing large volumes of rapid, continuous, and repetitive content through multiple channels (Paul and Matthews, 2016). Other research has identified a "Russian disinformation chain" that describes how Russian leaders use media proxies (e.g., *Russia Today* or *Sputnik*) and amplification channels (e.g., social media platforms or U.S. news media) to reach consumers (Bodine-Baron et al., 2018). Studies have revisited the terms and definitions

FIGURE 3
Framework for Understanding the Pathology of Falsehoods



surrounding these information efforts. For example, some have employed the broad term "hostile social manipulation," which encompasses any purposeful, systematic generation and dissemination of harmful information (Mazarr et al., 2019, p. 15). Recently, scholars have called for a common lexicon for describing the characteristics of information efforts (Paul and Matthews, 2018). Given these debates, we use the framework in Figure 3 as a starting point to help organize some relevant lines of research.

Production Focuses on New Content Containing Falsehoods

The unit of analysis for research related to production is the content itself. In general, the studies in our sample focused on two topical areas. This first was the targeting and specific features of content. For example, one study examined a data set of 705,381 unique accounts during the 2016 presidential election to show how bots skew perceptions of candidates on social media (Heredia, Prusa, and Khoshgoftaar, 2018).[17] In another study using Twitter data, researchers found evidence that Russian information efforts targeted both conservative and liberal conversations online by impersonating Americans (Starbird, Arif, and Wilson,

2018). Although many of these studies focused on U.S. online communities, we did identify relevant studies from other countries. In one study from China, for example, researchers analyzed microblog posts from Sina Weibo and Tencent Weibo platforms related to the avian influenza A (H7N9) (Chen et al., 2018). Of the 1,680 microblog posts, researchers classified about 20 percent (n = 341) as misleading. The authors report that users who posted misleading messages had the highest average rank of reposts compared with other types of messages, but they ranked lowest in number of followers and existing posts.

The second topical area focuses on automated methods for classifying content that contains falsehoods within information environments. For example, one proposed framework for detecting falsehoods analyzes the text (e.g., title length, percentage of proper nouns) and verifies the accuracy of information compared with a corpus of trusted sources (Ibrishimova and Li, 2019). In another study, the authors describe a classifier that estimates the probability that a news story is false using such features as the headline (e.g., whether a news title had capital letters), authorship characteristics, sourcing, origin or publisher, and the content's political perspective (Snell et al., 2019). Other research has applied topic modeling to examine differences in Russian content versus English content (Chew and Turnley, 2017).

Distribution Research Explains How Falsehoods Spread

The unit of analysis for research related to distribution is the social network. We highlight two types of studies: those focusing on the role of social media platforms in preventing the spread of online falsehoods and those focusing on the role of machine-learning approaches to accomplish the same task.

The unit of analysis for research related to distribution is the social network.

First, we found several studies that focused on the role of social media platforms in this area. Research on how the conspiracy theory linking vaccines with autism spread via Twitter and Reddit showed that each platform served different functions in the dissemination of this disinformation (Jang et al., 2019). Twitter was found to drive news agendas while news content drives Reddit discussions. Understanding how platforms contribute to different aspects of the diffusion chain would help in detecting the flow of disinformation articles and targeting appropriate interventions on these platforms. Likewise, another study investigated the impact of WhatsApp's policy that limited the number of times a user could forward a message to just five. On public WhatsApp groups in Brazil, Indonesia, and India, this policy helped slow the spread of disinformation but did not block it entirely (de Freitas Melo et al., 2019). The openness and control of the platform has an impact on the flow of disinformation. A study comparing Twitter's open platform with Sino Weibo's more-closed, government-controlled platform showed that sharing misinformation about Ebola outbreaks was less prevalent on Chinese microblogs (Fung et al., 2016). Another study on the spread of the chemtrails conspiracy on several online platforms suggests that anonymity online appears to help spread conspiracies (Tingley and Wagner, 2017).

Second, there was a growing body of research about using machine-learning models to track, understand, and mitigate the spread of existing falsehoods on social media. One study proposed using these models for situational awareness in understanding a multipolar political landscape prior to an election. In a study of 60 million exchanges among 2.4 million Twitter users around the 2017 French election, researchers qualified and quantified various characteristics of online political communities, tracking their temporal evolution, structures, alliances, and semantic features during the campaign (Gaumont, Panahi, and Chavalarias, 2018). This situational awareness might provide a foundation for understanding how falsehoods spread across a country's electorate

and what communities are most affected. Other studies looked at how to detect disinformation accurately in these conversations. A graph-based machine-learning model tracked the stance of 72 rumors in more than 100,000 tweets in a semisupervised approach (Giasemidis et al., 2020). This model measured whether the tweeter felt positive, neutral, or negative about the rumor and was used to help predict the accuracy of information. Results showed the algorithm was fast and accurate, exceeding 80 percent average accuracy. Using semisupervised machine-learning algorithms to classify the stance of rumor tweets might lead to fast, scalable, and accurate differentiation of information. Advances in machine-learning might help researchers accurately classify false information, understand its spread, and gain insight into how users receive it.

Consumption Research Focuses on the Role of Consumers

The unit of analysis for research related to consumption is the individual consumer. Much of the research focused on consumer views of content and the impacts of fact-checking on these views.

The first theme focused on consumers' features and views surrounding exposure to falsehoods, which could lead to more consumers taking action against false information. Pew surveyed representative samples of adults in 11 emerging economies and found that respondents felt they regularly encountered false information on social media (Smith et al., 2019). Furthermore, an analysis of a three-country survey comparing voters in the United States, the United Kingdom, and France reports that conservative voters in the latter two countries were no more likely than nonconservative voters to report that they were exposed to falsehoods. This was not true in the United States. Those on the political right in the United States reported feeling much more exposed to false news and that they could trust news much less than did people reporting to be nonconservative voters (Koc-Michalska et al., 2020). This deterioration of trust in news media for U.S. conservatives implies that news and government might need to communicate differently with these consumers.

The unit of analysis for research related to consumption is the individual consumer.

Additionally, Budak, 2019, researched how the 2016 presidential election correlated with the prevalence of false news online. Budak randomly sampled 5,000 tweets each from tweets mentioning President Donald J. Trump or former Secretary of State Hillary Rodham Clinton from May 2014 to January 2017. This study showed that the prevalence of falsehoods in news increased over the course of the campaign and that voter perceptions of former Secretary of State Clinton were more in line with false news accounts. Finally, in a study of more than 5 million tweets, researchers applied machine-learning algorithms embedded in network models to find user attributes that accurately predict how they will react to online content (Gallo et al., 2020). Among four factors (the Big Five personality traits, time interval, predominant sentiment, and sentiment distribution), they found that the Big Five personality traits (i.e., openness to experience, conscientiousness, extroversion, agreeableness, neuroticism)[18] had the most impact on user reactions to false information.

A second theme focused on the effects of fact-checking of content on consumers, which is a popular approach to countering false information. One study looked at Facebook's "rated false" and "disputed" tags on different headline types (false pro-President Trump, false anti-President Trump, and true headlines) using respondents from Amazon's Mechanical Turk crowdsourcing platform (Clayton et al., 2019). Results showed that both tags reduce beliefs in false news, but the rated false tag was more effective than tagging headlines as disputed.

Because not all news stories can be checked and tagged, providing general warnings might help alert users to false news. A related study on StopFake—a Ukrainian fact-checking organization

founded in response to Russian information efforts in 2014—showed that fact-checking organizations have different focuses. StopFake focused on finding falsified evidence, such as manipulated or misrepresented images and quotes. However, most U.S. fact-checking organizations assume quotes and images are legitimate and focus on evaluating nuanced political claims. Some researchers claim most U.S. fact-checking groups are ill-equipped to detect disinformation that is wholly falsified (Haigh, Haigh, and Kozak, 2018).

Conclusions and Recommendations

This report reviews some of the research that is relevant to foreign information efforts targeting U.S. elections. It provides a general framework for understanding these efforts and will inform our analysis in future volumes of this series. We focused on efforts by Russia and its proxies because these actors appear to have been the most active in recent years, but we note that other state and nonstate actors also might target the United States. As a result of this work, we reached four general conclusions.

Conclusions

Foreign Interference in U.S. Politics Is Not a New Phenomenon

Foreign influence in U.S. domestic affairs dates back to the founding of this country, and there are several examples in our 244 years of existence.

How the Russians Have Tried to Interfere in Recent U.S. Elections Follows Some Logic

We hypothesize that *reflexive control theory*—a theoretical research program first developed in the 1960s and used by the Soviet military—is part of the intellectual basis for current Russian efforts. At its core, reflexive control theory assumes that people live in a polarized world defined by either cooperation or conflict and that people make decisions based on these views. We believe that Russia is trying to generate, spread, and amplify falsehoods that distort views of "us" versus "them," with the desired outcomes of (1) driving people to view each other as either friends or adversaries, or (2) exhausting people to the point that they disengage from civic affairs altogether, with the result of political paralysis.

Russia's Tactics Aim to Polarize Americans and Paralyze the U.S. Political Process

These tactics consist of attempts at polarizing and disrupting social cohesion. Some tactics aim to exacerbate divisive issues, such as racial inequities or immigration. Others target public confidence in democratic institutions and processes as a way to undermine social trust. Underlying these efforts is a broader tactic of using falsehoods to spread confusion, drive groups of people to extreme positions, and generate collective exhaustion within U.S. society. Finally, there is evidence that Russia has tried—and continues to try—to gain direct influence over the U.S. political decisionmaking process, although we do not know how effective these efforts have been.

Our Sample of Relevant Research Revealed Some Trends for Responding to Falsehoods

Although our sample of studies is not representative of all research on this topic, it does provide some ideas for emerging practices in responding to foreign information efforts. Much of this research is fragmented and cuts across multiple disciplines, causing us to organize it by primary unit of analysis: the production of new falsehoods, the distribution of existing falsehoods, or the consumers of this content.

Research on production largely focused on targeting of falsehoods and the features of this content. For studies on the distribution of existing falsehoods, research focused on the role of social media platforms in preventing the spread of online falsehoods and the role of machine-learning models to mitigate this spread. Finally, research on consumption largely focused on consumer views of content and the impacts of fact-checking.

Recommendations for Responding to Foreign Information Efforts

Foreign interference has occurred throughout U.S. history and likely will continue in the future. Russia

seems to have advanced its information efforts in recent years, and we suspect other countries will try to emulate these practices. We offer three recommendations for how to start designing responses to these existing and emerging threats that target U.S. democracy. In future volumes of this series, we will present results with more-specific recommendations for responding to these foreign information efforts.

A Holistic Strategy Is the Optimal Response to Information Efforts by Foreign Countries

During the Cold War, Secretary of State Lawrence Eagleburger recommended a "balanced approach" to Soviet information efforts that neither ignores the threat nor becomes obsessed with it (Eagleburger, 1983). Our assumption is that reflexive control theory is part of the intellectual basis for Russian efforts targeting U.S. elections. The unit of analysis of this theory is broad, spanning the entirety of U.S. society and any particular piece of online content, social media platform, or individual consumer. We recommend that any defensive strategy account for the complex relationships among the production of falsehoods, how others distribute content (particularly online), and the impacts of this content on consumers.

Any Defense Should Anticipate Those Who Are Likely to Become Targets of These Efforts

We believe that a key goal for information efforts is to alter people's perceptions to amplify a view of "us versus them," with political paralysis as the ultimate goal. Social or political issues tied to identities (such as race, gender, social class, or political affiliation) that hold meaning for people are useful starting points because false content tied to these characteristics might elicit strong reactions (Marwick, 2018). We suspect that foreign efforts will likely produce content that plays on these identities in an effort to amplify differences and deepen preexisting fault lines in U.S. society. Thus, we recommend developing strategies that anticipate which subgroups are most vulnerable to such efforts without publicly shaming these groups or targeting specific individuals.

Any Response Should Attempt to Protect Potential Targets Against Foreign Information Efforts

The antidote to manufacturing intergroup conflict is convincing people that they have more in common with those who are different from them than they might believe at first glance. We recommend collecting, analyzing, and evaluating preventative interventions to protect people from reacting to falsehoods meant to divide the country (e.g., public campaigns that emphasize shared interests of Californians, public warnings about broader information efforts by foreign adversaries, or media literacy programs for subgroups that are potential targets).

In conclusion, democracy depends on citizens finding consensus with people whom they might view as different from them. Foreign adversaries have made attempts at undermining the formation of this consensus and will continue to do so. There is a logic to these attempts. The best defense is a holistic approach that accounts for the preexisting fault lines that exist within U.S. society.

Democracy depends on citizens finding consensus with people whom they might view as different from them. Foreign adversaries have made attempts at undermining the formation of this consensus and will continue to do so.

Appendix A: Detailed Description of Reflexive Control Theory

The mathematical models of reflexive control theory evolved from a scenario with one decisionmaker torn between two actions to a *group* of decisionmakers embedded within a social network, each of whom must choose one of two actions (Lefebvre, 1966, 1980, 2009, 2010). These decisionmakers operate in a world of binary relationships. First, the theory assumes that others in the network are either friends or enemies of the actor. Second, reflexive control theory assumes that the ethical belief system of the society in which actors exist is also binary: Either the ends justify the means or they do not. Finally, the theory assigns each person's influence a value of either 0 or a 1 (in less neutral terms, influence can be thought of as urging someone to choose between two polar opposites on a spectrum of behaviors).[19] Finally, according to reflexive control theory, one person might influence another in these direct and indirect ways depending on the parameters over which they exert control.[20]

Furthermore, the outcome is also binary: Each person might choose between two polar opposite actions—represented by a value of 0 or 1—while being influenced by their neighbors in the social network. The choices can be thought of as "passive" or "aggressive" behaviors—or, as a more specific example, violence versus peacebuilding. Given the assumed ethical norms and the types of relationships that bind people on the network, actors might behave differently depending on the influence exerted by the others.

For example, under some conditions, everyone in a network might decide to adopt the "aggressive" behavior. With a different combination of influences, some people might switch their behavior. In yet other situations, no behavior might be consistent with a person's relationships and influences; the actors are then considered "frustrated" and cannot make a choice.[21]

Each person's chosen behavior is the solution to a mathematical formula—drawing from graph theory and abstract algebra—that captures the reflexive concept at the core of this theory.[22] Specifically, people's decisions depend not only on their views of themselves and others (as described by the network of relationships in which they exist), but also on how others view them and everyone else as described by the network of relationships. For example, let us say that two people named A and B are friends. A thinks of herself as being a friend of B and views B as being her friend. She also believes that B thinks of A as a person who is her friend. The formulae determining each person's action captures this series of recursive self-images: how you view yourself, how you view others, and how you think others view you.

Appendix B: Overview of China, Iran, and Venezuela's Influence Efforts Targeting the United States

Although Russia appears to be the most active and persistent state actor attempting to influence U.S. domestic politics, other countries have also pursued foreign policy goals by seeking to influence U.S. decisionmakers and society via online news and social media. This section discusses how China, Iran, and Venezuela approach influence operations.[23] The Director of National Intelligence and major social media sites (e.g., Facebook and Twitter) have identified these countries as having carried out online information campaigns that target the United States, and their previous activities suggest they might try again in 2020.[24]

China

China considers itself to be in an ideological competition with the West and the United States, and the internet to be its battlefield. Although China has a long history of using information manipulation techniques, censorship, and propaganda to achieve domestic or regional effects, campaigns beyond its immediate neighborhood have lacked the range and finesse of Russian foreign influence operations.[25] Its influence activities are embedded into its regional and global policy objectives, which consist of preventing the United States from curtailing China's global influence and destroying U.S. global and regional influence.[26] According to Diamond and Schell, 2018, China is also at least partly motivated by the view that U.S. ideals and values of freedom are a "direct challenge to its defense of its own form of one-party rule."[27]

Chinese influence operations outside the immediate region use overt and covert measures. They tend to focus on establishing and exploiting human relationships, specifically targeting ethnic Chinese. These operations try to cultivate relationships with key foreign decisionmakers, opinion leaders, and the business community; inject Chinese narratives into foreign educational establishments, media, and public opinion; and tarnish the reputation of politicians (Mattis, 2018; Mazarr et al., 2019; Watts, 2020). China is primarily interested in achieving longer-term policy objectives (Doshi and Williams, 2018). One Chinese author explains that public opinion warfare "during peacetime pays more attention to long-term infiltration into the objects of the society's and culture's deep structure, changing the awareness and conviction of the enemy masses" (Wang Lin and Wang Guibin, 2004, cited in in Beauchamp-Mustafaga and Chase, 2019). Until recently, China's external influence efforts in both traditional and new media mostly focused on burnishing China's image and achieving favorable reactions.

Lately, however, China has been more aggressive in using online media to spread divisions in target groups, echoing the online techniques used by Russia (Watts, 2020). Figure B.1 displays an overview of select Chinese-government narratives targeting the United States. China has allegedly sought to influence the population, domestic politics, and election processes of the United States, although not on the same scale as Russia. For example, China has been accused of trying to make illegal donations during the 1996 U.S. presidential campaign and to gubernatorial and congressional campaigns in 2013 and 2018, and the placement of paid propaganda newspaper inserts has been part of China's toolbox for some time (Beauchamp-Mustafaga and Chase, 2019). For example, in September 2018, leading up to elections, the Chinese government published a paid insert in the *Des Moines Register* highlighting Chinese President Xi Jinping's ties to Iowa, the benefits to Iowans of trade with China, and the costs of President Trump's trade war (Niquette and Jacobs, 2018). Although there is limited evidence of Chinese interference with the 2016 presidential elections, one report observes that the spreading social media owned by Chinese companies (for example, WeChat) might provide China with more tools of influence. Although Microsoft claimed in 2019 that China's hacking threat to political groups is not as significant as those posed by Russia and Iran, Google announced more recently that Chinese hackers are targeting the personal accounts of former Vice President Jospeh Biden (Sanger and Perlroth, 2020). China-linked Twitter accounts have also been found

FIGURE B.1
Overview of Key Selected Chinese Government Narratives

BENIGN NONPOLITICAL NARRATIVES	BENIGN POLITICAL NARRATIVES	PERSUASIVE NARRATIVES	HOSTILE NARRATIVES
• China's beautiful landscapes and scenery • China's heritage • China's accomplishments and positive impact on the world	• Visits of Chinese leaders • Explanation of events via the Party lens • Touting the Party and China's leadership	• Touting the benefits of free trade for U.S. farmers • Discussing the risks of U.S.-Chinese economic tensions	• Western political interference in Chinese domestic issues (e.g., Hong Kong protests, Taiwan)

to recycle tweets calling for the independence of California and comparing the "Yes California" campaign with the Hong Kong independence movement. However, it is likely that the aim of this activity was to liken the independence of Taiwan to California breaking away from the rest of the United States and trying to discredit protestors in Hong Kong (Thomas and Zhang, 2020).

The populism and divisions in the United States today might present China with an opportunity to promote the values supported by the Chinese government and carry out targeted messaging.[28] Experts suggest that China is increasingly seeking to cultivate influence abroad via Western-based online platforms, as illustrated by Chinese government organizations and government-supported media agencies opening accounts on Western-based social media sites (Bradshaw and Howard, 2019). Experts expect China to seek to create confusion in the U.S. information space by making use of existing conflicts, such as exacerbating public scandals, disseminating rumors, or publishing personal information to denigrate political or community leaders.[29]

China seems to have little interest in creating complex false online personas (Wallis et al., 2020). Analysis of China's social media activities show that "astroturfing" and other covert means of disseminating pro-China narratives are among its preferred online methods, specifically when accomplished via hirelings or purchased bots that offer plausible deniability.[30] One analysis of Twitter data also suggests a penchant for images embedded in Chinese-language text (Wallis et al., 2020). China's use of disinformation techniques during the 2019 coronavirus pandemic suggests a willingness to transition from a strategy of avoiding confrontation and controversial issues to embracing more-aggressive tactics, such as promoting conspiracy theories and sowing confusion (Kendall-Taylor and Shullman, 2020; King, Pan, and Roberts, 2017). Although Chinese writers discuss the value of tailored messaging to different audiences, there is little evidence so far of such nuanced narratives.

China could also seek to establish a network among younger population groups. One Chinese author, when discussing propaganda in Hong Kong, writes that China should "use social networking platforms such as Facebook and Twitter to establish virtual, voluntary, and loose groups amongst all social groups, especially the youth, [so that] at any time and any place we can push to them web postings we have processed and edited to propagandize our ideas" (Yu, cited in Mazarr et al., 2019).

Iran

Iran's online influence techniques are becoming increasingly sophisticated and diverse (Hanlon, 2018). Figure B.2 displays an overview of select aims and techniques of Iran's influence efforts targeting the United States. Although Iran's online operations were considered clumsy just a few years ago, its methods have become more subtle and varied. Recent analysis indicates that Iran's techniques now consist

FIGURE B.2

Overview of Select Aims and Techniques of the Iranian Government's Influence Efforts Targeting the United States

MAIN AIMS	MAIN TECHNIQUES
• Disseminate Pro-Iranian narratives • Exaggerate Iran's moral authority • Polarize U.S. society • Discredit U.S. critiques of Iran	• Iranian TV, radio networks in English • Social media posts in English by Iranian leaders, state-supported media networks • Doctored photos and memes • False online personas (designed to appear American) • Botnets and online trolls

of information operations, social engineering via LinkedIn, denial-of-service attacks, defacement, and hacking techniques (Glyer and Carr, 2020). Iranian manufactured online personas have evolved from having an obvious affiliation with Iran or inauthentic news websites supported by the Iranian government (e.g., *Liberty Front Press*) into more-authentic American personas or impersonations of real Americans who appear to be affiliated with local progressive movements (Revelli and Foster, 2019). Iran has also placed propaganda in genuine online and print media outlets in the United States in an effort to promote Iranian interests (FireEye Intelligence, 2018; Nimmo, 2018). For example, Facebook in 2020 removed an online network of hundreds of fake social media accounts that had been spreading Iranian propaganda since 2011. A 2018 investigation by the Reuters news agency uncovered more than 70 inauthentic news websites disseminating propaganda in more than 15 countries, and Microsoft revealed in 2019 that it had detected significant malign cyber activity from Iran (Burt, 2019).

Iran uses cyber operations—a relatively cheap means to gain influence while ensuring plausible deniability—as foreign policy and statecraft. The Iranian government has been accused of carrying out several cyberattacks against U.S. political organizations,[31] and Iran or its proxies have allegedly sought to influence or attack U.S. elections and political leaders. During the 2016 U.S. presidential elections, Iranian trolls posted anti-President Trump messages, and Iran has also attacked U.S. government officials and Iranians living abroad (Center for Strategic and International Studies, undated; Martin and Shapiro, 2019). Analysis by the data analysis firm Graphika, 2020, shows that Iran is mainly focused on pursuing the foreign policy goals of discrediting the U.S. critique of human rights in Iran and the U.S. sanctions against Iran.

Analysts note that Iranian online influence operations against the United States so far have sought to polarize the U.S. population and politics by distributing divisive content on social media and amplifying conspiracy theories (e.g., related to the terrorist attacks of September 11, 2001), disseminating pro-Iranian propaganda, and discrediting U.S. critique of Iran's policies and human rights record (Martin and Shapiro, 2019). There is no evidence of substantial Iranian attempts to influence U.S. elections, but Iran's efforts to support Scotland's referendum to achieve independence from the United Kingdom in 2014 indicate that Iran has experimented with online election meddling beyond its immediate neighborhood (Stubbs and Paul, 2020; Bradshaw and Howard, 2019).

Venezuela

Venezuela has a history of trying to pursue its anti-U.S. foreign policy in the United States through *social power*—providing generous financial handouts and developing networks with socially disadvantaged organizations or other groups. The aim is to generate support for the Venezuelan government and its ideological stance and to use these efforts as publicity stunts (Corrales, 2011). The cases discussed in the

literature show Venezuela's preference for the use of proxies, such as nongovernmental organizations or business enterprises in the United States, that at least superficially shield Venezuela from the effort.[32]

Venezuela seeks to pursue several aims: positively portray its government, criticize the U.S government, and sow divisions within the United States (Tromblay, 2018). Recent Twitter data analysis also shows that Venezuela and its proxies have started using online news and social media to pursue these goals: In 2019, Twitter removed accounts located in Venezuela that were "engaging in platform manipulation targeted outside of the country" (Roth, 2019).

Conclusion

Online influence operations are often difficult to detect and categorize. They are carried out in a complex information environment that has multiple actors and narratives, and the true motives or origin of the disseminated information might be obscured from the consumer. Iran, Venezuela, and particularly China seem to be increasingly invested in developing online influence techniques, which might further complicate efforts to detect, identify, and respond to them. U.S. adversaries seem specifically interested in online influence operations because they are cost-effective and provide plausible deniability. Increased societal polarization and discord further fertilize the U.S. ground for foreign influence operations, allowing foreign actors to exploit the interests and disagreements among different social, political, or other camps. Furthermore, existing analysis notes that small groups and weaker actors might achieve a disproportionally large effect by disseminating false information online.

Appendix C: Systematic Literature Review

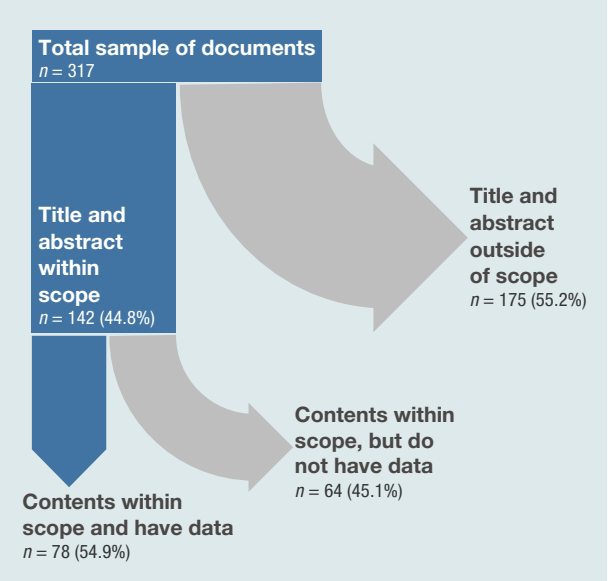
We developed a search string that identified documents related to the creation, spread, and consumption of falsehoods on a variety of media, such as the internet, television, and radio. This string also covered mitigation strategies and four key state-based foreign actors: Russia, China, Iran, and Venezuela. We ran versions of this search string on 13 academic databases and the Defense Technical Information Center database.[33] We focused on studies published from 2013 to April 2020. The searches yielded 317 documents; we determined that 44.8 percent (142 documents) of them were relevant to this study. Figure C.1 displays the documents we used or discarded in this systematic literature review.

Next, four analysts split up 142 documents in our final sample for review. We used a three-step approach for making this decision:

1. The complete document must have been written in English.
2. It must relate to information efforts.
3. The documents must use some type of qualitative or quantitative data.

FIGURE C.1

Breakdown of Documents Considered in this Analysis



Using a subsample of 40 documents, our team of analysts were in agreement on which documents to use in the final sample 85.8 percent of the time.[34]

Our sample of documents does not represent all research on responding to information efforts. The topic cuts across many areas of research, such as communications studies, sociology, psychology, political science, public policy, economics, computer science, and philosophy. Thus, our sample of articles, book chapters, and reports provides a snapshot to better understand the types of topics that are studied. Toward this end, we developed the following search string to identify relevant studies in our sample:

> (TITLE-ABS(misinformation OR disinformation OR false OR mislead OR "fake news")
>
> AND TITLE-ABS(internet or "social media" OR news OR television OR radio OR *phone* OR email OR mail)
>
> AND TITLE-ABS(spread OR propogat* OR disseminat* OR circulat* OR communicat* OR diffuse OR broadcast)
>
> AND TITLE-ABS(Mitigat* OR Interven* or Counter* or Measure* or reduc* or increas* or decreas*)
>
> And TITLE-ABS(elect* or Russia* OR China OR Chinese OR Iran* OR Venezuela* OR domestic)
>
> AND pubyear aft 2013)

We ran this search string in the following databases:

- Academic Search Complete
- APA Psycinfo
- Applied Science and Technology Full Text
- Business Source Complete
- CINAHL Plus with Full Text (Cumulative Index to Nursing and Allied Health Literature)
- Index to Legal Periodicals & Books
- Library, Information Science, and Technology Abstracts (LISTA)
- Military Database
- PAIS Index (Public Affairs Information Service)

- PolicyFile
- Scopus
- Sociological Abstracts
- Web of Science.

We then ran the following similar but modified string in the Defense Technical Information Center database, limited to accessible reports only:[35]

Citation(misinformation OR disinformation OR false OR mislead OR "fake news")

AND (Citation(internet OR "social media" OR news OR television OR radio OR *phone* OR email OR mail)

AND (Citation(spread OR propogat* OR disseminat* OR circulat* OR communicat* OR diffuse OR broadcast)

AND (Citation(mitigat* OR interven* OR counter* OR measure* OR reduc* OR increas* OR decreas*)

AND (Citation(election* OR russia* OR china OR chinese OR iran* OR venezuela* OR domestic)

AND (Citation("information operations" OR "info ops" OR "psychological operations" OR psyops OR "psy-ops" OR "information warfare")

Notes

[1] We note that the lines between foreign and domestic are blurred surrounding information efforts.

[2] This review provides a framework for interpreting the results in subsequent parts of this series. We draw from the Chairman of the Joint Chiefs of Staff in defining what information efforts are and where they take place, and define information efforts as activities that "influence, disrupt, corrupt, or usurp the decision making of targets while protesting one's own" (Chairman of the Joint Chiefs of Staff, 2014, p. A-1). These efforts might include authentic content (such as that from human trolls) and inauthentic content (such as that from bots) that is created and disseminated by state-sponsored actors or their proxies (who could be willing or unwilling participants). Such efforts exist in an information environment, broadly defined as "the aggregate of individuals, organizations, and systems" (Chairman of the Joint Chiefs of Staff, 2014, p. GL-6). These environments involve any collection of people who interact with each other online or in person. (For more details, see Chairman of the Joint Chiefs of Staff, 2014.)

[3] Vladimir Lefebvre personal e-mail with the lead author, March 3, 2018.

[4] This hypothesis is largely based on past research, but Vladimir Lefebvre confirmed that while he did not have specific information concerning Russia's use of the theory, it was his belief that the Russian Federation uses reflexive control theory in its information efforts against the United States (Lefebvre personal e-mail with the lead author, March 3, 2018).

[5] The mathematical framework describing reflexive control is distinct from the language of most game theory, although both deal with the strategic use of information. Reflexive control theory does not use an equilibrium concept to predict outcomes, and it does not assume agents behave rationally according to a utility function; rather, it assumes agent behavior is internally consistent with an ethical belief function (Lefebvre and Farley, 2007, p. 636).

[6] In general, reflexive control theory assumes that ethical frameworks differ in the United States and Soviet Union: The former assumes that bad ethical means should not be implemented for good ethical outcomes; the latter is less concerned when there is conflict between bad means and good goals. For more details, see Chotikul, 1986; Lefebvre and Farley, 2007; and Umpleby, 2016.

[7] See, for example, the "roster of identities" listed by DiResta et al., 2019, p. 11.

[8] The cross-platform tactic has been described as a "media mirage" that creates an "immersive information ecosystem," (DiResta et al., 2019, pp. 14, 42; Howard et al., 2018, p. 8).

[9] Pomerantsev, 2015b, provides an example: Estonia must constantly guess whether the Kremlin's threats about Russia having the capabilities to invade Estonia are an effort to show real intention, affect the morale of the Estonian population, or seek publicity from reporters elsewhere.

[10] Note that this selection of key objectives is based on an analysis of a selection of open-source publications and is focused on aims that are relevant for U.S. domestic politics only.

[11] For a more detailed discussion of Russia's approach to information warfare, see Thomas, 2004.

[12] Rogan, 2015, concludes that Russia used a "three-pronged strategy" and tried to (1) make covert payments to well-intentioned environmental groups in the West, often even without their knowledge, (2) gather intelligence on the U.S. energy industry, and (3) mount an information campaign against fracking, calling it a hoax.

[13] Tweets originating in Russia supported California and Texas secession movements (Martin and Shapiro, 2019).

[14] We focus on information efforts by Russia and their proxies because they appear to be some of the most organized in the world. Furthermore, much of the contemporary research on this topic is focused on Russia and its proxies. We acknowledge, however, that other countries also engage in similar efforts. For more information on those efforts, see Appendix B.

[15] Research on information efforts often touches on different units of analysis. Thus, many documents in our sample are classified across the pathology of falsehoods described in Figure 3. See Lewis-Beck, Bryman, and Liao, 2004.

[16] We broadly define *users* to include humans and software agents, commonly known as *bots*.

[17] This research could be categorized under consumption because it also looked at public opinion as measured by sentiment and volume baselines in the data.

[18] The OCEAN model/Big-Five personality traits in this article assigned scores to people's character based on the following five dimensions: openness, conscientiousness, extraversion, agreeableness, and neuroticism. For more details, see Gallo et al., 2020, p. 921.

[19] Formally, the *social network* is a complete graph whose edges comprise two disjoint subsets separating contentious from cooperative relationships. Every such graph with N that meets a simple criterion can be mapped to a Boolean function in N variables, where the operations + and x correspond to either contentious or cooperative edges. The action chosen by person n is calculated by setting n equal to the function, inputting others' influences on n for the other variables, and solving for n. There are extensions of the model that incorporate more than two possible actions, but these extensions are somewhat stylized and do not always have intuitive real-world interpretations.

[20] Chapter 9 of Lefebvre, 2010, refers to these as "conscious" and "subconscious" influences.

[21] For a benign example of a son frustrated by his parents' influences in choosing a spouse, see Chapter 10 of Lefebvre, 2010.

[22] In some cases, the solution might be a fraction between 0 and 1, which would then be interpreted as the probability the person chooses the action labeled 1.

[23] This overview does not present a comprehensive discussion of Chinese, Iranian, and Venezuelan online influence efforts. Rather, it considers key online-based influence elements that these countries have used or might use in the future to affect U.S. domestic politics.

[24] Facebook and Twitter have removed accounts engaged in "coordinated inauthentic behavior" that is linked to a gov-

ernment actor or a political party and are engaged in foreign influence operations. Note that this discussion only discusses foreign-focused influence efforts from these countries, with a specific focus on the United States. Our analysis is not intended as a comprehensive account of the strategies, means, and methods of these countries or the information threats that the United States might encounter, and is based only on relevant literature that has already been published. (Bradshaw and Howard, 2019; Sebenius, 2019)

[25] For example, China's external influence activities in the region have specifically focused on Taiwan.

[26] For a discussion of China's foreign policy and influence activities, see Mazarr et al., 2019.

[27] For an in-depth discussion on China's approach to influence operations, see Beauchamp-Mustafaga and Chase, 2019.

[28] Likewise, China could be expected to tie in existing or emerging issues in the United States with China's overall foreign policy objectives. One such example would be using racial discrimination issues to hurt the reputation of the United States with its allies or to distract from China's abysmal human rights record. (Mazarr et al., 2019; Wallis et al., 2020)

[29] This assertion is based on an analysis of Chinese authors in Beauchamp and Chase, 2019.

[30] *Astroturfing* refers to organized activities that intend to create a false impression of widespread support for a position ("Astroturfing," undated).

[31] A report by Microsoft names Iran among the countries that carried out hacking attempts in 2019 (Volz, 2019).

[32] The Bolivarian Circles, for example, was created in 2001 and is a group that seeks to promote the values of Simon Bolivar but was also a means for neighborhood groups to request assistance for community programs directly from the President of Venezuela Hugo Chavez (U.S. Bureau of Citizenship and Immigration Services, Resource Information Center, 2002).

[33] Details of these search strings and the databases are provided in Appendix C.

[34] We estimated five different agreement coefficients among the four raters for a randomly selected subset of 40 documents that were coded by all raters. Each of these coefficients were above widely accepted benchmarks for interrater reliability, including Gwet's Agreement Coefficient (0.69) and Krippendorf's Alpha (0.69). (For more details, see Klein, 2018, p. 880.)

[35] We modified this search term in DTIC because an initial screening with the original parameters led to an overwhelming amount of false positives related to electronic warfare and command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) in military operations.

References

Aceves, William J., "Virtual Hatred: How Russia Tried to Start a Race War in the United States," *Michigan Journal of Race & Law*, Vol. 24, No. 177, 2019.

Allen, T. S., and A. J. Moore, "Victory Without Casualties: Russia's Information Operations," *Parameters*, Vol. 48, No. 1, Spring 2018, pp. 59–71.

"Astroturfing," Merriam-Webster.com, undated. As of July 29, 2020:
https://www.merriam-webster.com/dictionary/astroturfing

Beauchamp-Mustafaga, Nathan, and Michael S. Chase, *Borrowing a Boat Out to Sea: The Chinese Military's Use of Social Media for Influence Operations*, John Hopkins School of Advanced International Studies, policy paper, 2019. As of July 29, 2020:
https://www.fpi.sais-jhu.edu/borrowing-a-boat-out-to-sea-pdf

Bennett, W. Lance, and Steven Livingston, "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions," *European Journal of Communications*, Vol. 33, No. 2, April 2, 2018, pp. 122–139. As of July 20, 2020:
https://journals.sagepub.com/doi/full/10.1177/0267323118760317

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence*, Santa Monica, Calif.: RAND Corporation, RR-2740-RC, 2018. As of July 20, 2020:
https://www.rand.org/pubs/research_reports/RR2740.html

Bradshaw, Samantha, and Philip N. Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Oxford, England: The Computational Propaganda Project at the Oxford Internet Institute, 2019.

Budak, Ceren, "What Happened? The Spread of Fake News Publisher Content During the 2016 U.S. Presidential Election," *WWW '19: The World Wide Web Conference, May 13–17, 2019, San Francisco, CA, USA*, Geneva, Switzerland: International World Wide Web Conference Committee, May 2019, pp. 139–150. As of August 1, 2020:
https://dl.acm.org/doi/pdf/10.1145/3308558.3313721

Burt, Tom, "New Cyberthreats Require New Ways to Protect Democracy," Microsoft On the Issues," blog post, July 17, 2019. As of September 1, 2020:
https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/

Carpenter, Michael, "Russia Is Co-Opting Angry Young Men," *The Atlantic*, August 29, 2018. As of August 31, 2020:
https://www.theatlantic.com/ideas/archive/2018/08/russia-is-co-opting-angry-young-men/568741/

Center for Strategic and International Studies, "Significant Cyber Incidents," webpage, undated. As of June 5, 2020:
https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

Central Intelligence Agency, *Intelligence in the Civil War*, Washington, D.C., undated. As of July 29, 2020:
https://www.cia.gov/library/publications/intelligence-history/civil-war/Intel_in_the_CW1.pdf

Chairman of the Joint Chiefs of Staff, *Joint Information Operations Proponent*, Instruction 3210.01C, February 14, 2014. As of July 29, 2020:
https://www.jcs.mil/Portals/36/Documents/Library/Instructions/3210_01.pdf

Chen, Bin, Jian Shao, Kui Liu, Gaofeng Cai, Zhenggang Jiang, Yuru Huang, Hua Gu, and Jianmin Jiang, "Does Eating Chicken Feet with Pickled Peppers Cause Avian Influenza? Observational Case Study on Chinese Social Media During the Avian Influenza A (H7N9) Outbreak," *JMIR Public Health and Surveillance*, Vol. 4, No. 1, January–March 2018.

Chew, Peter A., and Jessica G. Turnley, "Understanding Russian Information Operations Using Unsupervised Multilingual Topic Modeling," in Dongwon Lee, Yu-Ru Lin, Nathaniel Osgood, and Robert Thomson, eds., *Social, Cultural, and Behavioral Modeling: 10th International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*, London: Springer Nature, 2017, pp. 102–107.

Chotikul, Diane, *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study*, Monterey, Calif.: Naval Postgraduate School, No. NPS55-86-013, 1986.

Clayton, Katherine, Spencer Blair, Jonathan A. Busam, Samuel Forstner, John Glance, Guy Green, Anna Kawata, Akhila Kovvuri, Jonathan Martin, Evan Morgan, et al., "Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-Check Tags in Reducing Belief in False Stories on Social Media," *Political Behavior*, February 2019, pp. 1–23.

Conley, Heather A., Donatienne Ruy, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook 2: The Enablers*, Washington, D.C.: Center for Strategic and International Studies, March 2019.

Corrales, Javier, "Conflicting Goals in Venezuela's Foreign Policy," in Ralph S. Clem and Anthony P. Maingot, eds., *Venezuela's Petro-Diplomacy: Hugo Chávez's Foreign Policy*, Gainesville, Fla.: University of Florida Press, 2011, pp. 32–48.

de Freitas Melo, Philipe, Carolina Coimbra Vieira, Kiran Garimella, Pedro O. S. Vaz de Melo, and Fabrício Benevenuto, "Can WhatsApp Counter Misinformation by Limiting Message Forwarding?" in Hocine Cherifi, Sabrina Gaito, José Fernendo Mendes, Esteban Moro, and Luis Mateus Rocha, eds., *Complex Networks and Their Applications VIII*, Vol. 1, *Proceedings of the Eight International Conference on Complex Networks and Their Applications*, London: Springer Nature, 2019, pp. 372–384.

Derysh, Igor, "Russia Trying to 'Incite Violence by White Supremacist Groups' in US Ahead of 2020 Election: Report," *Salon*, March 10, 2020. As of July 29, 2020: https://www.salon.com/2020/03/10/russia-trying-to-incite-violence-by-white-supremacist-groups-in-us-ahead-of-2020-election-report/

Diamond, Larry, and Orville Schell, eds., *China's Influence & American Interests: Promoting Constructive Vigilance*, Washington, D.C.: Hoover Institution, October 2018. As of September 5, 2020: https://www.hoover.org/research/chinas-influence-american-interests-promoting-constructive-vigilance

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson, *The Tactics and Tropes of the Internet Research Agency*, New Knowledge, 2019.

Doronin, Alexander, "Anti-Extremism: Who Will Be the Target?" in *Business-Intelligence* [*Biznes Razvedka*], 2010. As of September 10, 2020: https://web.archive.org/web/20090621054933/http://www.agentura.ru/

Doshi, Rush, and Robert D. Williams, "Is China Interfering in American Politics?" *Lawfare*, October 1, 2018. As of September 1, 2020: https://www.lawfareblog.com/china-interfering-american-politics

Eagleburger, Lawrence S., "Unacceptable Intervention: Soviet Active Measures," *NATO Review*, Vol. 31, No. 1, 1983.

Endicott, Marisa, "Propaganda's New Goals: Create Confusion, Sow Doubt," U.S. News, January 31, 2017. As of July 20, 2020: https://www.usnews.com/news/national-news/articles/2017-01-31/russian-propagandas-new-goals-create-confusion-sow-doubt

FireEye Intelligence, "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East," blog post, August 21, 2018. As of September 1, 2020: https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html

Fung, Isaac Chun-Hai, King-Wa Fu, Chung-Hong Chan, Benedict Shing Bun Chan, Chi-Ngai Cheung, Thomas Abraham, and Zion Tsz Ho Tse, "Social Media's Initial Reaction to Information and Misinformation on Ebola, August 2014: Facts and Rumors," *Public Health Reports*, Vol. 131, No. 3, May–June 2016, pp. 461–473.

Gallo, Fabio R., Gerardo I. Simari, Maria Vanina Martinez, and Marcelo A. Falappa, "Predicting User Reactions to Twitter Feed Content Based on Personality Type and Social Cues," *Future Generation Computer Systems*, Vol. 110, September 2020, pp. 918–930.

Gaumont, Noé, Maziyar Panahi, and David Chavalarias, "Reconstruction of the Socio-Semantic Dynamics of Political Activist Twitter Networks—Method and Application to the 2017 French Presidential Election," *PLoS One*, Vol. 13, No. 9, September 2018.

Giasemidis, Georgios, Nikolaos Kaplis, Ioannis Agrafiotis, and Jason R. C. Nurse, "A Semi-Supervised Approach to Message Stance Classification," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 32, No. 1, January 1, 2020, pp. 1–11.

Glaser, April, "Russian Trolls Were Obsessed with Black Lives Matter," *Slate*, May 11, 2018. As of July 29, 2020: https://slate.com/technology/2018/05/russian-trolls-are-obsessed-with-black-lives-matter.html

Glyer, Christopher, and Nick Carr, "State of the Hack: Spotlight Iran—From Cain & Abel to Full SANDSPY," FireEye, blog post, February 12, 2020. As of September 1, 2020: https://www.fireeye.com/blog/products-and-services/2020/02/state-of-the-hack-spotlight-iran.html

Godson, Roy, and Richard Shultz, "Soviet Active Measures: Distinctions and Definitions," *Defense Analysis*, Vol. 1, No. 2, 1985, pp. 101–110.

Government of Russia, "Foreign Policy Concept of the Russian Federation," November 30, 2016. As of February 10, 2020: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248

Graphika, "Briefing: China, Iran, and Russia State Accounts on U.S. Protests," blog post, June 3, 2020. As of September 1, 2020: https://graphika.com/posts/briefing-china-iran-and-russia-state-accounts-on-u-s-protests/

Haigh, Maria, Thomas Haigh, and Nadine I. Kozak, "Stopping Fake News: The Work Practices of Peer-to-Peer Counter Propaganda," *Journalism Studies*, Vol. 19, No. 14, 2018, pp. 2062–2087.

Hamilton, Alexander, "The Federalist Papers, No. 68: The Mode of Electing the President," *New York Packet*, March 14, 1788 (via Lillian Goldman Law Library). As of July 29, 2020: https://avalon.law.yale.edu/18th_century/fed68.asp

Hanlon, Bradley, "Iran's Newest Info Op Shows an Evolution of Tactics," Disinfo Portal, November 13, 2018. As of September 1, 2020: https://disinfoportal.org/irans-newest-info-op-shows-an-evolution-of-tactics/

Heredia, Brian, Joseph D. Prusa, and Taghi M. Khoshgoftaar, "The Impact of Malicious Accounts on Political Tweet Sentiment," *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, conference proceedings, 2018, pp. 197–202.

Howard, Philip N., Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François, "The IRA, Social Media and Political Polarization in the United States, 2012–2018," Computation Propaganda Research Project, University of Oxford, 2018.

Ibrishimova, Marina Danchovsky, and Kin Fun Li, "A Machine Learning Approach to Fake News Detection Using Knowledge Verification and Natural Language Processing," in Leonard Barolli, Hiroaki Nishino, and Hiroyoshi Miwa, eds., *Advances in Intelligent Networking and Collaborative Systems: the 11th International Conference on Intelligent Networking and Collaborative Systems*, London: Springer Nature, 2019, pp. 223–234.

Jang, S. Mo, Brooke W. Mckeever, Robert Mckeever, and Joon Kyoung Kim, "From Social Media to Mainstream News: The Information Flow of the Vaccine-Autism Controversy in the US, Canada, and the UK," *Health Communication*, Vol. 34, No. 1, 2019, pp. 110–117.

Jenkins, Brian Michael, *America's Great Challenge: Russia's Weapons of Mass Deception*, WeaponsofMassDeception.net, 2019. As of July 29, 2020: https://weaponsofmassdeception.net/

Jones, Seth G., "Russian Meddling in the United States: The Historical Context of the Mueller Report," Center for Strategic and International Studies, March 2019. As of August 27, 2020: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190328_RussianMeddlingintheUS_WEB_V.2.pdf

Karjukin, V., and V. F. S. Chausov, "Reflexive Games Counter," in V. E. Lepsky, *Reflexive Processes and Management* [*Refleksivnye Processy I Upravlyenye*], Moscow: Russian Academy of Sciences, 2017.

Kavanagh, Jennifer, and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica, Calif.: RAND Corporation, RR-2314-RC, 2018. As of July 20, 2020: https://www.rand.org/pubs/research_reports/RR2314.html

Kendall-Taylor, Andrea, and David Shullman, "Converging Chinese and Russian Disinformation Compounds Threat to Democracy," Power 3.0, May 26, 2020. As of September 1, 2020: https://www.power3point0.org/2020/05/26/converging-chinese-and-russian-disinformation-compounds-threat-to-democracy/

King, Gary, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review*, Vol. 111, No. 3, August 2017, pp. 484–501.

Klein, Daniel, "Implementing a General Framework for Assessing Interrater Agreement in Stata," *Stata Journal*, Vol. 18, No. 4, 2018, pp. 871–901.

Koc-Michalska, Karolina, Bruce Bimber, Daniel Gomez, Matthew Jenkins, and Shelley Boulianne, "Public Beliefs About Falsehoods in News," *International Journal of Press/Politics*, Vol. 25, No. 3, 2020, pp. 447–468.

Lamond, James, *The Origins of Russia's Broad Political Assault on the United States*, Washington, D.C.: Center for American Progress, October 3, 2018.

Lefebvre, Vladimir A., "The Basic Ideas of Reflexive Games Logic," *Systems and Structures Research Problems*, conference proceedings, Moscow, 1965.

Lefebvre, Vladimir A., "The Elements of Reflexive Game Logic," *Problems in Engineering Psychology*, No. 4, 1966.

Lefebvre, Vladimir A., "An Algebraic Model of Ethical Cognition," *Journal of Mathematical Psychology*, Vol. 22, No. 2, 1980.

Lefebvre, Vladimir A., "Reflexive Analysis of Groups," in Shlomo Argamon and Newton Howard, eds., *Computational Methods for Counterterrorism*, Berlin: Spring-Verlag, 2009, pp. 173–210.

Lefebvre, Vladimir A., *Lectures on Reflexive Game Theory*, Los Angeles: Leaf & Oaks Publishers, 2010.

Lefebvre, Vladimir A., and Jonathan David Farley, "The Torturer's Dilemma: A Theoretical Analysis of the Societal Consequences of Torturing Terrorist Suspects," *Studies in Conflict & Terrorism*, Vol. 30, No. 7, 2007, pp. 635–646.

Lewis-Beck, Michael S., Alan E. Bryman, and Tim Futing Liao, *The SAGE Encyclopedia of Social Science Research Methods*, Thousand Oaks, Calif.: Sage Publications, 2004.

Lockhart, P. R., "How Russia Exploited Racial Tensions in America During the 2016 Elections," *Vox*, December 17, 2018. As of July 29, 2020: https://www.vox.com/identities/2018/12/17/18145075/russia-facebook-twitter-internet-research-agency-race

Martin, Diego A., and Jacob N. Shapiro, "Trends in Online Foreign Influence Efforts," Princeton University, version 1.2, July 8, 2019. As of September 1, 2020: https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_foreign_influence_efforts_2019jul08_0.pdf

Marwick, Alice E., "Why Do People Share Fake News? A Sociotechnical Model of Media Effects," *Georgetown Law Technology Review*, Vol. 2, No. 2, 2018, pp. 474–512.

Matthews, Miriam, Alyssa Demus, Elina Treyger, Marek N. Posard, Hilary Reininger, and Christopher Paul, *Understanding and Defending Against Russia's Malign and Subversive Information Efforts in Europe*, Santa Monica, Calif.: RAND Corporation, RR-3160-EUCOM, forthcoming.

Mattis, Peter, "Contrasting China's and Russia's Influence Operations," *War on the Rocks*, January 16, 2018. As of September 1, 2020: https://warontherocks.com/2018/01/contrasting-chinas-russias-influence-operations/

Mazarr, Michael J., Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*, Santa Monica, Calif.: RAND Corporation, RR-2713-OSD, 2019. As of July 22, 2020: https://www.rand.org/pubs/research_reports/RR2713.html

Michael, George, "Useful Idiots or Fellow Travelers? The Relationship Between the American Far Right and Russia," *Terrorism and Political Violence*, Vol. 31, No. 1, 2019, pp. 64–83.

Nimmo, Ben, "#TrollTracker: An Iranian Messaging Laundromat," DFRLab, April 29, 2018. As of September 1, 2020: https://medium.com/dfrlab/trolltracker-an-iranian-messaging-laundromat-218c46509193

Niquette, Mark, and Jennifer Jacobs, "China Looks to Influence Iowa in Trade War over Trump Tariffs," Bloomberg, September 23, 2018. As of September 1, 2020: https://www.bloomberg.com/news/articles/2018-09-23/china-looks-to-influence-iowa-in-trade-war-over-trump-tariffs

Paul, Christopher, and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016. As of July 14, 2020: https://www.rand.org/pubs/perspectives/PE198.html

Paul, Christopher, and Miriam Matthews, *The Language of Inform, Influence, and Persuade: Assessment Lexicon and Usage Guide for U.S. European Command Efforts*, Santa Monica, Calif.: RAND Corporation, RR-2655-EUCOM, 2018. As of July 20, 2020: https://www.rand.org/pubs/research_reports/RR2655.html

Pomerantsev, Peter, "Russia and the Menace of Unreality," *The Atlantic*, September 9, 2014. As of August 31, 2020: https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/

Pomerantsev, Peter, "Authoritarianism Goes Global (II): The Kremlin's Information War," *Journal of Democracy*, John Hopkins University Press, Vol. 26, No. 4, October 2015a.

Pomerantsev, Peter, "The Kremlin's Information War," *Journal of Democracy*, Vol. 26, No. 4, October 2015b.

Radin, Andrew, Alyssa Demus, and Krystyna Marcinek, *Understanding Russian Subversion: Patterns, Threats, and Responses*, Santa Monica, Calif.: RAND Corporation, PE-331-A, 2020. As of July 14, 2020: https://www.rand.org/pubs/perspectives/PE331.html

Radin, Andrew, and Clint Reach, *Russian Views of the International Order*, Santa Monica, Calif.: RAND Corporation, RR-1826-OSD, 2017. As of August 31, 2020: https://www.rand.org/pubs/research_reports/RR1826.html

Revelli, Alice, and Lee Foster, "Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests," FireEye, May 28, 2019. As of September 1, 2020: https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html

Rogan, Tom, "Russia's War on Fracking," *National Review*, February 3, 2015. As of July 24, 2020: https://www.nationalreview.com/2015/02/russias-war-fracking-tom-rogan/

Root, Danielle, and Aadam Barclay, *Voter Suppression During the 2018 Midterm Elections: A Comprehensive Survey of Voter Suppression and Other Election Day Problems*, Washington, D.C.: Center for American Progress, November 20, 2018.

Roth, Yoel, "Information Operations on Twitter: Principles, Process, and Disclosure," Twitter Blog, blog post, June 13, 2019. As of September 1, 2020: https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html

Sanger, David E., and Nicole Perlroth, "Chinese Hackers Target Email Account of Biden Campaign Staff, Google Says," *New York Times*, June 4, 2020.

Schoen, Fletcher, and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *INSS Strategic Perspectives*, Vol. 11, June 1, 2012.

Sebenius, Alyza, "U.S. Sees Russia, China, Iran Trying to Influence 2020 Elections," Bloomberg, June 24, 2019. As of September 1, 2020: https://www.bloomberg.com/news/articles/2019-06-24/u-s-sees-russia-china-iran-trying-to-influence-2020-elections

Select Committee on Intelligence of the United States Senate, *Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Vol. 1: *Russian Efforts Against Election Infrastructure with Additional Views*, 116th Congress, Report 116-XX, 2019. As of July 29, 2020: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

Select Committee on Intelligence of the United States Senate, *(U) Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Vol. 2: *Russia's Use of Social Media with Additional Views*, 116th Congress, Report 116-XX, undated. As of July 29, 2020: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Select Committee on Intelligence of the United States Senate, *(U) Russian Active Measures Campaigns and Interference in the 2016 Election, Vol. 5: Counterintelligence Threats and Vulnerabilities*, 116th Congress, Report 116-XX, 2020. As of August 27, 2020: https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf

Smith, Aaron, Laura Silver, Courtney Johnson, Kyle Taylor and Jingjing Jiang, "Publics in Emerging Economies Worry Social Media Sow Division, Even as They Offer New Chances for Political Engagement," Pew Research Center, May 2019. As of July 29, 2020: https://www.pewinternet.org/wp-content/uploads/sites/9/2019/05/Pew-Research-Center_Technology-and-Politics-in-Emerging-Economies-Report_2019-05-13.pdf

Snell, Nicholas, Jeremy Straub, Brandon Stoick, Terry Traylor, and William Fleck, "Assessing Online Media Reliability: Trust, Metrics and Assessment," in Misty Blowers, Russell D. Hall, and Venkateswara R. Dasari, eds., *Disruptive Technologies in Information Sciences II*, Vol. 11013, International Society for Optics and Photonics, 2019.

Soufan Center, "IntelBrief: Russian Disinformation Campaigns Continue to Sow Doubt in the West," December 17, 2018. As of July 21, 2020: https://thesoufancenter.org/intelbrief-russian-disinformation-campaigns-continue-to-sow-doubt-in-the-west/

Spaulding, Suzanne, Devi Nair, and Arthur Nelson, "Russia's Attacks on Democratic Justice Systems," Center for Strategic and International Studies, May 2019. As of July 2020: https://www.csis.org/features/russias-attacks-democratic-justice-systems

Starbird, Catharine, Ahmer Arif, and Tom Wilson, *Technical Proposal: Understanding the Structure and Dynamics of Disinformation in the Online Information Ecosystem*, Arlington, Va.: prepared for the Office of Naval Research, grant number N00014-17-1-2980, August 14, 2018. As of July 29, 2020: https://apps.dtic.mil/sti/pdfs/AD1058867.pdf

Stent, Angela, *Putin's World: Russia Against the West and with the Rest*, New York: Hachette Book Group, 2019.

Stubbs, Jack, and Katie Paul, "Facebook Says It Dismantles Disinformation Network Tied to Iran's State Media," Reuters, May 5, 2020. As of September 1, 2020: https://www.reuters.com/article/us-iran-facebook/facebook-says-it-dismantles-disinformation-network-tied-to-irans-state-media-idUSKBN22H2DK

Sullivan, Eileen, "Maria Butina, Russian Who Infiltrated Conservative Circles, Is Deported," *New York Times*, October 25, 2019.

Taylor, Margaret L., "Combatting Disinformation and Foreign Interference in Democracies: Lessons from Europe," Brookings Institution, blog post, July 31, 2019. As of July 29, 2020: https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/

Thomas, Elise, and Albert Zhang, *COVID-19 Attracts Patriotic Troll Campaigns in Support of China's Geopolitical Interests*, Australian Strategic Policy Institute, June 25, 2020.

Thomas, Timothy L., "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies*, Vol. 17, 2004, pp. 237–256.

Thomas, Timothy, *Russia's 21st Century Information War: Working to Undermine and Destabilize Populations*, Riga, Latvia: Defense Strategic Communications: The Official Journal of the NATO Strategic Communications Center of Excellence, 2015. As of July 29, 2020: https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations

Tingley, Dustin, and Gernot Wagner, "Solar Geoengineering and the Chemtrails Conspiracy on Social Media," *Palgrave Communications*, Vol. 3, No. 1, December 2017, pp. 1–7.

Tromblay, Darren E., *Political Influence Operations: How Foreign Actors Seek to Shape U.S. Policy Making*, Lanham, Md.: Rowman & Littlefield, 2018.

Umpleby, Stuart, "Vladimir Lefebvre's Theory of Two Systems of Ethical Cognition," *Journal on Systemics, Cybernetics and Informatics*, Vol. 14, No. 5, 2016, pp. 65–67.

United States v. Internet Research Agency LLC, 2018 W.L. 914777, 2018. As of July 29, 2020: https://www.justice.gov/file/1035477/download

U.S. Bureau of Citizenship and Immigration Services, Resource Information Center, *Venezuela: Information on Círculos Bolivarianos (Bolivarian Circles)*, VEN02001.ZMI, April 30, 2002. As of September 1, 2020: https://www.refworld.org/docid/3dec9b4b4.html

U.S. Department of Justice, "Russian National Charged in Conspiracy to Act as an Agent of the Russian Federation Within the United States," July 16, 2018. As of July 25, 2020: https://www.justice.gov/opa/pr/russian-national-charged-conspiracy-act-agent-russian-federation-within-united-states

Usdin, Steve, "When a Foreign Government Interfered in a U.S. Election—to Reelect FDR," *Politico*, January 16, 2017. As of July 29, 2020: https://www.politico.com/magazine/story/2017/01/when-a-foreign-government-interfered-in-a-us-electionto-reelect-fdr-214634

Volz, Dustin, "Russia, Iran, North Korea Launch Hundreds of Cyberattacks on U.S. Political Groups, Microsoft Says," *Wall Street Journal*, July 17, 2019.

Wallis, Jake, Tom Uren, Elise Thomas, Albert Zhang, Samantha Hoffman, Lin Li, Alex Pascoe, and Danielle Cave, *Retweeting Through the Great Firewall: A Persistent and Undeterred Threat Actor*, Australian Strategic Policy Institute, Policy Brief Report No. 33, 2020.

Walsh, Gianfranco, and Vincent-Wayne Mitchell, "The Effect of Consumer Confusion Proneness on Word of Mouth, Trust, and Customer Satisfaction," *European Journal of Marketing*, Vol. 44, No. 6, 2010.

Wang Lin [王林] and Wang Guibin [王贵滨], "An Analysis of Public Opinion Warfare and Psychological Warfare [舆论战与心理战辨析]," PLA Daily [解 放军报], June 8, 2004.

Ward, Alex, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference," Vox, December 17, 2018. As of July 29, 2020: https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram

Washington, George, Farewell Address, September 19, 1796, (via Avalon Project at Yale Law School). As of July 29, 2020: https://www.ourdocuments.gov/doc.php?flash=true&doc=15&page=transcript

Watts, Clint, "Triad Against Disinformation: How Russia, Iran, & China Ally in A Messaging War Against America," GMF Alliance for Securing Democracy, commentary, May 15, 2020. As of September 1, 2020: https://securingdemocracy.gmfus.org/triad-of-disinformation-how-russia-iran-china-ally-in-a-messaging-war-against-america/

Yates, Will, "'Russian Trolls' Promoted California Independence," BBC, November 4, 2017. As of July 29, 2020: https://www.bbc.com/news/blogs-trending-41853131

Yu Mingsong, "Research on United Front Work for Hong Kong Middle Class Professionals [香港中产专业人士统战工作研究]," *United Front Science*, March 2017.

About This Report

Throughout the U.S. political campaign season of 2020, Russia might try again to manipulate and divide U.S. voters through social media. This report is the first in a four-part series aimed at helping policymakers and the public understand—and mitigate—the threat of online foreign interference in national, state, and local elections.

Given the past and likely extant threats to U.S. elections, the California Governor's Office of Emergency Services (Cal OES) asked RAND's National Security Research Division (NSRD) for research to help them analyze, forecast, and mitigate threats by foreign actors targeting local, state, and national elections.

We would like to thank our sponsors at the California Governor's Office of Emergency Services (Cal OES). We are grateful to Melissa Bauman, whose dedicated work improved the prose of this report. Finally, we thank Christopher Paul of RAND and Herbert Lin of Stanford University for their thoughtful reviews.

This research was sponsored by the California Governor's Office of Emergency Services (Cal OES) and conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the defense agencies, the Navy, the Marine Corps, the U.S. Coast Guard, the U.S. Intelligence Community, allied foreign governments, and foundations.

For more information on the RAND International Security and Defense Policy Center, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

For more information on this publication, visit www.rand.org/t/RRA704-1.

www.rand.org