Hostile Social Manipulation

Present Realities and Emerging Trends

Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, James Sladden

RAND CORPORATION

For more information on this publication, visit www.rand.org/t/RR2713

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-1-9774-0260-8

Published by the RAND Corporation, Santa Monica, Calif.

Contents

Figures v
Tables vii
Summary ix
Acknowledgments xvii
Abbreviations xix

CHAPTER ONE
Introduction: Information and Democracy—A Perilous Relationship 1
The Growing Danger of Social Manipulation 2
Study Design, Methodology, and Scope 5
The Broader Danger: A Corrupted Information Environment 8

CHAPTER TWO
Understanding Social Manipulation: Definitions and Typologies 11
Defining Key Categories 11
The Goals of Social Manipulation 18
The Range of Options: Examples of Hostile Social Manipulation 20
The Past: Understanding the Context for Social Manipulation 23

CHAPTER THREE
Hostile Social Manipulation: Russian Activities 29
Methodology 31
History: Soviet and Russian Approaches to Social Manipulation 33
Doctrine: Russia's Conceptualization of Social Manipulation 49
Strategies: How Russia Conducts Social Manipulation Today 62

Actions: What Russia Is Doing and How 77
Effectiveness of Russia's Efforts 92
Conclusions 103

CHAPTER FOUR
Hostile Social Manipulation: Chinese Activities 105
History: China's Approach to Social Manipulation 107
Doctrine: China's Goals for Foreign Policy and Information Operations 110
"Magic Weapons": China's Offensive Approach to Defense 113
Strategies: Who Manages the Media and the Messages? 121
Actions: China's Information Operations Through Social Media 131
Effectiveness of China's Efforts 151
Conclusions and Implications for U.S. Policy 162

CHAPTER FIVE
Does Hostile Social Manipulation Work? Measures of Success in Russian Activities in Europe and the United States 167
United States 171
United Kingdom 184
France 194
Germany 206
The Baltic States 210
Poland 215
Summary of Outcome Evidence 219

CHAPTER SIX
Hostile Social Manipulation: The Experience to Date—Conclusions and Implications 225

Bibliography 231

Figures

2.1. The Boundaries of Social Manipulation 16
4.1. Articles Referencing *Russia Today* in Chinese-Language Publications Since 2016 117
4.2. Articles Referencing Social Media in *Party Construction* 123
4.3. Articles Referencing Social Media in *United Front Science* ... 124
4.4. Articles Referencing Social Media in *International Communications* 125
4.5. Articles Referencing Social Media in *Military Correspondent* 129
4.6. Articles on Chinese Diaspora and Social Media in *International Communications* 137
4.7. Global Opinion of China 152
4.8. Chinese Journal Articles on Foreign Public Opinion of China 153
4.9. *International Communications* Articles on Shaping Foreign Public Opinion of China 154
5.1. Favorable Ratings for Russia Among American Public, 2013–2017 172
5.2. Favorability Ratings of Russia Among British Public, 2013–2017 186
5.3. British Attitude Toward Relationship with European Union 189
5.4. Favorability Ratings of Russia Among French Republic, 2013–2017 195
5.5. Political Content Shared by Twitter Users in Rounds One and Two of the 2017 French Election 199

5.6. Political Content Shared by Twitter Users in Several Elections 200
5.7. Favorability Ratings for Russia Among German Public, 2013–2017 207
5.8. Favorability Ratings for NATO Among German Public, 2013–2017 209
5.9. Favorability Ratings of Russia Among Polish Public, 2013–2017 216
5.10. Favorability Ratings for NATO Among Polish Public, 2013–2017 218
5.11. Percentage of Various Publics with Favorable View of European Union 220
5.12. Percentage of Various Publics with Favorable View of NATO 221

Tables

2.1. Categorizing Informational Behavior 12
2.2. Goals and Objectives of Social Manipulation Campaigns 19
2.3. Techniques and Mechanisms for Social Manipulation..... 22
4.1. Taxonomy of Chinese Influence Operations via Social Media..... 132
4.2. Select Chinese Government and Media Accounts on Western Social Media Platforms..... 155
5.1. Comparing Metrics of Social Manipulation Efforts and Effects in Rounds One and Two of French Election 198
5.2. Recent Security Initiatives in the Baltics..... 213
5.3. NATO Collective Initiatives Since 2014..... 223

Summary

The role of information warfare in global strategic competition has become much more apparent in recent years. Today's practitioners of what this report terms *hostile social manipulation* employ targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, distribution of rumors and conspiracy theories, and other tools and approaches to cause damage to the target state. This emerging practice reflects an updated and modified version of many long-established forms of influence, including propaganda, "active measures," disinformation, and political warfare, a group of techniques sometimes referred to with the overarching term *measures short of war*. The subject has become a leading topic of debate in the West in the wake of reports of Russian election interference, not only in the United States but throughout Europe.

These emerging tools and techniques represent a potentially significant threat to U.S. and allied national interests. This report represents an effort to better define and understand the challenge by focusing on the activities of the two leading authors of such techniques—Russia and China. Our goal is to evaluate the forms of hostile social manipulation both countries have employed and to conduct an initial assessment of how effective they have been. To do that, we examine three somewhat distinct issues:

- We first build an understanding of the essential idea of social manipulation by surveying the various terms and concepts in play and offering a framework for distinguishing them.

- We then review what we know about recent and ongoing efforts at hostile social manipulation strategies and activities of first Russia and then China in these areas.
- Finally, we examine evidence on the potential effectiveness of those techniques by evaluating the area where we have the best evidence—Russia's efforts to shape opinion and social dynamics in Europe and the United States.

The report's focus is what we term *hostile social manipulation*. As Chapter Two explains, the activities of states in this realm—broadly speaking, seeking to gain competitive advantage by manipulating political, social, and economic conditions in target countries by various informational means—range across a variety of partly overlapping categories. This research is concerned with the use of social media–based campaigns, but also with the creation of narratives and sometimes fabricated information to use in those campaigns. It is concerned with direct media broadcasting, for example through state-owned media outlets; other forms of classic propaganda; and paid advertising. The category includes the theft of compromising information and its employment in these public campaigns, as occurred in the 2016 U.S. presidential election. It is concerned with the use of cyberintrusions, thefts, and attacks to the degree they play a direct role in creating the basis for informational campaigns designed to achieve effects through perceptual and attitudinal shifts.

That said, our intended area of focus does not include a number of tools and techniques that are often used in conjunction with such specifically information-based campaigns. Those can include direct support (financial or otherwise) for political parties or political figures, clandestine operations designed to harass or injure individuals or groups, economic or military assistance, economic sanctions, and many other forms of intervention into another state's society, economy, and politics. They fall under broader conceptual formulations, such as measures short of war or political warfare. This report focuses specifically on the informational component of such larger endeavors—the ways states broadcast, shape, invent, block, and otherwise manipulate information to achieve effects on other societies.

The analysis examines these issues through a detailed assessment of available evidence of Russian and Chinese social manipulation efforts, the doctrines and strategies behind such efforts, and evidence of their potential effectiveness. RAND Corporation analysts reviewed English-, Russian-, and Chinese-language sources; examined national security strategies and policies and military doctrines; surveyed existing public-source evidence of Russian and Chinese activities; and assessed multiple categories of evidence of effectiveness of Russian activities in Europe, including public opinion data, evidence on the trends in support of political parties and movements sympathetic to Russia, and data from national defense policies. Taken together, these multiple sources of data provide a comprehensive open-source portrait of the status of Russian and Chinese social manipulation efforts and their potential effects.

This report focuses on past and current practices and capabilities of Russia and China in this area and the emerging trends in the tactics and techniques of social manipulation. A forthcoming analysis looks to the future and evaluates the degree to which the synergy of a range of technologies—from social media platforms to artificial intelligence to voice-activated personal assistants to virtual reality—could create an even more perilous landscape for hostile social manipulation.

Our analysis comes with one important caveat: The degree of Russian influence on the 2016 U.S. election—and the fundamental issue of whether Russia determined its outcome with its multiple influence efforts—was never intended to be a focus of the analysis and is beyond the scope of this report. Existing evidence on the effectiveness of Russian manipulation activities is not sufficient to support anything like a definitive judgment of the impact of Russian efforts to shape electoral outcomes. Our analysis does conclude that whatever the truth about Russia's effect on the election, Moscow has developed an emerging suite of tools that give it the *potential* ability to have significant, perhaps even decisive impacts on electoral outcomes. This fact, we argue, should be of significant concern to the United States.

More broadly, our research into the character and evolving nature of hostile social manipulation supports several conclusions. Our first finding relates to the narrow issue of a conceptual foundation for

analysis. *The United States*, we find, *needs an updated framework for organizing its thinking about the manipulation of infospheres by foreign powers determined to gain competitive advantage.* Accounts of social manipulation today refer to a blizzard of related concepts and issues, from disinformation to social media marketing to "information warfare" and psychological operations to cyberattacks to blackmail and the use of stolen documents to discredit individuals or political parties (a tactic referred to as *doxfare*), without a clear sense of how they relate to one another or what, in fact, the core threat actually is. A coherent framework for organizing the various components of the challenge is the first step toward improved policy.

Second, the evidence surveyed for this analysis suggests that it is now undeniable that *leading autocratic states have begun to employ information channels for competitive advantage—plans that remain in their initial stages and that could unfold in several ways*. Russia and China believe themselves to be engaged in an information war with the West—one begun by the United States and its friends and allies—and have begun to invest significant resources in such tools. Both countries are dedicated to controlling their domestic information environment and using information tactics to gain increasing leverage over other countries. Both view such techniques as sources of competitive advantage over the United States and other democracies.

Third, this research suggests that *efforts at social manipulation are effective to the degree that vulnerabilities in a society allow them to be effective*. Such techniques can seldom create from whole cloth the situations that allow an aggressor to manipulate political life; they can only take advantage of realities being created by underlying trends. This has been the story of Russian and Chinese efforts to date—searching for seams and gaps in the social and information fabric of other countries.

Partly as a result, and despite the growing interest in such campaigns, our research suggests that they remain in their preliminary stages, have so far had relatively marginal effects, and may reflect far less coherent strategy in Moscow and Beijing than is typically assumed. A fourth broad finding is that *there is as yet no conclusive evidence about the actual impact of hostile social manipulation to date*. Significant gaps remain in our awareness of what has happened and how effective cur-

rent social manipulation campaigns have been. Indeed, their efforts appear to have been counterproductive in some ways: There is reason to believe that, at least so far, inflated claims of Russian and Chinese activities have provided more strategic value to Moscow and Beijing than the direct effects of the manipulation. Our research suggests, for example, that Russian officials measure the effectiveness of their efforts in part by the turmoil that emerges around the controversy itself, independent of any minds or votes changed. They may be willing to deal with the negative blowback to get these results.

In the process, a critical distinction emerged in our research between the *outputs* of these campaigns—numbers of posts, tweets, clicks, views, likes, and so on—and their *outcomes* in terms of the actual effect of that activity on attitudes or behavior. There is a tremendous amount of data on outputs, and almost no meaningful empirical evidence on outcomes. In fact, according to many metrics, the disinformation campaigns of one of the two actors examined in this study—Russia—have *not* been having significant success. Even in cases where outcomes have matched Russia's objectives, Moscow has not been inventing the grievances that produced a few recent electoral or referendum outcomes.

Yet the emphasis Russia and China have placed on these techniques—combined with ongoing research into the evolution of future technologies—suggests that this pattern may not persist. It may reflect a temporary reprieve rather than a permanent limit on the effectiveness of what could be termed *virtual societal aggression*. Our fifth finding is therefore that *despite the apparent limited effects to date, the marriage of the hostile intent of several leading powers and the evolution of several interrelated areas of information technology has the potential to vastly increase the effectiveness and reach of these techniques over time*. Such technologies as targeted marketing, including opt-in programs through which consumers share the most intimate details of their location, thought process, and emotional state; artificial intelligence and related fields such as machine learning; virtual and augmented reality; high-fidelity video and audio capture and impersonation; and the emergence of an "internet of things" in which data are being gathered from and shared among most things people interact with in daily life,

are creating the potential for much more sophisticated campaigns of social manipulation.

Leading democracies may therefore have a limited window of opportunity to develop resilience and active defenses against such measures before they become truly dangerous. Widespread, increasingly influential and damaging campaigns of hostile social manipulation attack the very essence of free societies—the relationship between facts, knowledge, belief, and political behavior. These techniques are not magic wands, and there are significant constraints on efforts to fine-tune the beliefs of any population. But the risks are significant enough to warrant continued close attention, and initial policy responses to bound the danger. The second report in this study will focus on the future risks of emerging technologies.

The sixth conclusion of this analysis is that *the United States and other democracies urgently need to undertake detailed, rigorous research on many aspects of this issue to provide themselves with a better understanding of many of the dynamics related to social manipulation*. Simply put, too many basic relationships are poorly understood, and more research is called for to better grasp the true level of risk, the most effective types of manipulation, and the most powerful responses.

This report catalogs a growing commitment to tools of social manipulation by leading U.S. competitors. As we argue, the threat as it exists today should not be blown out of proportion. So far, most of these campaigns appear to have had limited effects in terms of concrete geopolitical outcomes that either Russia or China is seeking. But there is abundant evidence that both of these governments view information competition as an integral part, perhaps the leading part, of an unending, intensive competition with the United States. Both are investing significant resources in building extensive capabilities in this realm and have begun to acquire extensive experience in their employment. If combined with emerging technologies that significantly enhance the impact of such campaigns—a possibility we assess in the next report—the results could pose one of the most significant dangers in history to open democracies. The findings in this report alone are sufficient to suggest that the U.S. government should take several immediate steps, including developing a more formal and concrete framework for

understanding the issue and funding additional research to understand the scope of the challenge.

About This Report

This research was sponsored by the Office of Net Assessment, Office of the Secretary of Defense, and conducted within the International Security and Defense Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

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

Acknowledgments

The authors would like to thank Ryan Bauer and Sarah Heintz for their assistance with research on some of the future technologies referenced in the scenarios in the report. We would like to thank Leah Hershey for her expertise in preparing the document for publication, and Rosa Maria Torres for her dedicated and timely assistance with the project. We are deeply indebted to our RAND colleague John Godges for his diligent work to enhance the tone and flow of the document. We extend our sincere thanks to the sponsor, the Office of Net Assessment in the Office of the Secretary of Defense, for support of the project.

Abbreviations

AI	artificial intelligence
AIDS	acquired immune deficiency syndrome
AP	Associated Press
API	Application Programming Interface
CAATSA	Countering America's Adversaries Through Sanctions Act
CAC	Cyber Administration of China
CCP	Chinese Communist Party
CCTV	China Central Television
CDU	Christian Democrats
CGTN	China Global Television Network
CIA	Central Intelligence Agency
CNKI	China National Knowledge Infrastructure
CPSU	Communist Party of the Soviet Union
DNI	Director of National Intelligence
EC	European Commission
EU	European Union
EW	electronic warfare
FARA	Foreign Agents Registration Act
FN	National Front
FNC	Framework Nation Concept

GDP	gross domestic product
HIV	human immunodeficiency virus
IIWAM	information/influence warfare and manipulation
IRA	Internet Research Agency
ISIS	Islamic State of Iraq and the Levant
KGB	Komitet Gosudarstvennoy Bezopasnosti
MPS	Ministry of Public Security
MSS	Ministry of State Security
NATO	North Atlantic Treaty Organization
OII	Oxford Internet Institute
PESCO	EU Permanent Structured Cooperation
PiS	Law and Justice Party
PLA	Peoples' Liberation Army
PLAAF	Peoples' Liberation Army Air Force
PRC	People's Republic of China
RT	[formerly] Russia Today
SAPPRFT	State Administration for Press, Publications, Radio, Film, and Television
SBU	Security Service of Ukraine
SCIO	State Council Information Office
SOE	state-owned enterprise
SPD	Social Democratic Party
TAR	Tibet Autonomous Region
USSR	Union of Soviet Socialist Republics
VK	VKontakte
XUAR	Xinjiang Uyghur Autonomous Region

CHAPTER ONE

Introduction: Information and Democracy—A Perilous Relationship

In the 1997 James Bond film *Tomorrow Never Dies*, the villain is Elliot Carver, head of a media conglomerate who has come to believe that information is a more powerful weapon than military force. He blackmails senior British leaders and ultimately tries to spark a war between China and Britain to bring his ally to power in Beijing. His plot is a combination of real-world actions—luring a British frigate into Chinese waters and then sinking it—with a global media blitz to "demonstrate" to the world that the action represents Chinese aggression and stoke the flames of British nationalism.

At one point in the film, Carver stands underneath massive television screens in the headquarters of his media empire, personally drafting the headlines—many of them referring to fabricated events—that will push the world toward war. "We're both men of action," he tells Bond, "but your era . . . is passing. Words are the new weapons, satellites the new artillery. . . . Caesar had his legions, Napoleon had his armies. I have my divisions—TV, news, magazines." Control of the global narrative, Carver suggests, will give him more power than any of those military leaders could ever wield.

The Bond plot offers one vision of a dystopian future: The idea that mass media in the electronic age has become so powerful, prevalent, and capable of manipulation that—with some "real" events thrown in for leavening—they could make whole populations believe the opposite of the truth. Elliot Carver represents a turbocharged version of the historical media figures who trafficked in rumor, innuendo,

and sometimes outright fabrication. Empowered by modern technology and spurred by a determination to exacerbate existing social divisions and fuel popular trust in their authorities and institutions, he brings the practice to its logical conclusion: the replacement of reality with invented fiction.

The Growing Danger of Social Manipulation

Fast-forward 20 years, and this scenario appears to be becoming reality. Using techniques far more advanced than those available to Bond villains in the 1990s, today's practitioners of what this report terms *hostile social manipulation* employ targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, distribution of rumors and conspiracy theories, and other tools and approaches to cause damage to the target state. This emerging practice reflects an updated and modified version of many long-established forms of influence, including propaganda, "active measures," disinformation, and political warfare. "Adversaries do not seek to attack their opponents physically but merely to destabilize them," one report on the trend concludes. "They favor assaults on the beliefs a population holds about its own government . . . and on a population's ability to distinguish fact from fiction."[1]

These informational tools are often part of larger campaigns that go by various names—political warfare, measures short of war, gray zone campaigns. Such campaigns can involve many tools beyond the realm of the manipulation of information. They can include economic aid or sanctions, direct political meddling through support of specific parties or movements, clandestine operations to foment protests or even coups, and more. In this research, however, we are focused on one aspect of these larger campaigns: the use of information to shape perceptions and attitudes in other societies and achieve harmful effects.

---

[1] Hannes Grassegger and Mikael Krogerus, "Weaken from Within," *New Republic*, November 2, 2017.

The subject has become a leading topic of debate in the West in the wake of reports of Russian election interference, not only in the United States but throughout Europe. As British Prime Minister Theresa May recently said of the leading practitioner of such techniques, Russia is "seeking to weaponize information. . . . in an attempt to sow discord in the West and undermine our institutions . . . threatening the international order on which we all depend."[2] Former U.S. Vice President Joe Biden and political analyst Michael Carpenter recently argued that the effort to "weaken and subvert Western democracies from the inside by weaponizing information, cyberspace, energy, and corruption" is part of a larger Russian program of "brazenly assaulting the foundations of Western democracy."[3]

In the last year, reports have laid bare several major campaigns by a range of actors to use information for aggressive purposes.

- Russia used a wide range of mechanisms to sow discord, exacerbate political divisions, reduce faith in public institutions generally and the political process especially, spark real-world political protests, and manipulate U.S. political and social outcomes. Those mechanisms have ranged from automated "bots" spewing thousands of tweets to political advertising on Facebook to direct propaganda broadcast through state-owned media channels to the targeted release of stolen documents to influence electoral outcomes. In the process, Russia is employing a confusing array of state-directed, state-supported, and state-encouraged actors to achieve its results.[4]
- The extremist group the Islamic State of Iraq and the Levant (ISIS) has continued to employ a sophisticated, multilevel social media outreach program to distribute its narrative, offer advice and motivation to potential radicals, and recruit actual followers.

---

2 Alexander Smith, "British PM Theresa May Says Russia Seeks to 'Weaponize' Information," NBC News, November 14, 2017.

3 Joe Biden and Michael Carpenter, "How to Stand Up to the Kremlin," *Foreign Affairs*, December 2017.

4 Scott Shane, "The Fake Americans Russia Created to Influence the Election," *New York Times*, September 7, 2017a.

- Several studies indicate that Russian and Venezuelan social media accounts flooded Spain with proindependence messages during the 2017 Catalan separatist crisis. One analysis of over 5 million messages dealing with the separatist debate claimed that 97 percent of them came from Russian and Venezuelan accounts. "Europe is at war," one account of this information campaign concluded. "Digital war . . . facing an attack meant to sow distrust, heighten divisions, and undermine established democratic processes."[5]
- China is reportedly becoming increasingly active in this space, including directly or indirectly supporting web and social media sites that promote China's official narratives and, increasingly, spread misinformation and outright fabrications designed to exacerbate social divisions in the United States.[6] Chinese state intelligence has used LinkedIn as a means of gathering information and establishing relationships with key individuals.[7] Writing in the *Washington Post*, the journalist Josh Rogin warned of the "huge scope and scale of Chinese Communist Party influence operations inside the United States, which permeate American institutions of all kinds. China's overriding goal is, at the least, to defend its authoritarian system from attack and at most to export it to the world at America's expense." He described Beijing's "combination of technology, coercion, pressure, exclusion and economic incentives" as being "beyond anything this country has faced before."[8]
- Forms of information aggression have already gone well beyond disinformation and targeting elections. Both in Eastern Europe and in the West, Russia and others have undertaken cyberharass-

---

5 Itxu Diaz, "Venezuela and Russia Teamed Up to Push Pro-Catalan Fake News," *Daily Beast*, November 28, 2017.

6 DFR Lab, "#FakeNews: Made in China," *Medium*, November 25, 2017.

7 "German Intelligence Unmasks Alleged Covert Chinese Social Media Profiles," Reuters, December 10, 2017.

8 Josh Rogin, "China's Foreign Influence Operations Are Causing Alarm in Washington," *Washington Post*, December 10, 2017. See also Ishaan Tahroor, "China's 'Long Arm' of Influence Stretches Ever Further," *Washington Post*, December 14, 2017.

ment, "trolling," stealing and then releasing personal information, and other techniques to intimidate or discredit specific individuals or activist groups.
- More broadly, Michael Abramowitz of Freedom House argued at the end of 2017 that "Online manipulation tactics played an important role in at least 17 other elections over the past year. From the Philippines and Ecuador to Turkey and Kenya, governing parties used paid commentators, trolls, bots, false news sites and propaganda outlets to inflate their popular support and essentially endorse themselves."[9]

These emerging tools and techniques represent a potentially significant threat to U.S. and allied national interests.[10] Yet democracies often have difficulty perceiving information as a possible weapon. The natural assumption of most democratic systems is that free flow of information is an unalloyed social good. The reality of hostile actors in the infosphere does not completely undermine this assumption, but it does mean that the United States and other democratic countries must begin to think more strategically about the information environment, their vulnerabilities, and also potential advantages.

Study Design, Methodology, and Scope

This report represents an effort to better define and understand the challenge by focusing on the activities of the two leading practitioners of such techniques—Russia and China. Our goal is to evaluate the

---

[9] Michael J. Abramowitz, "Stop the Manipulation of Democracy Online," *New York Times*, December 11, 2017.

[10] "Today, thanks to the Internet and social media," the RAND analyst and former senior Defense Advanced Projects Research Program Agency program manager Rand Waltzman has argued, "the manipulation of our perception of the world is taking place on previously unimaginable scales of time, space and intentionality. That, precisely, is the source of one of the greatest vulnerabilities we as individuals and as a society must learn to deal with" (Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," testimony before the Committee on Armed Services, Subcommittee on Cybersecurity, U.S. Senate, April 27, 2017, Santa Monica, Calif.: RAND Corporation, CT-473, 2017.

forms of hostile social manipulation both nations have employed and to conduct an initial assessment of how effective they have been. To do that, we examine three somewhat distinct issues:

- We first build an understanding of the essential idea of social manipulation by surveying the various terms and concepts in play and offering a framework for distinguishing them.
- We then review what we know about recent and ongoing efforts at hostile social manipulation strategies and activities of first Russia and then China in these areas.
- Finally, we examine evidence on the potential effectiveness of those techniques by evaluating the area where we have the best evidence—Russia's efforts to shape opinion and social dynamics in Europe and the United States.

The report begins with a proposal, outlined in Chapter Two, for a framework to define and understand the problem. Chapter Three offers a detailed survey of Russian social manipulation efforts; Chapter Four offers an analysis of Chinese activities. Those two chapters are intentionally somewhat different in structure and approach: The Russian and Chinese cases are very different—in the sorts of tools employed, the history behind them, the information available, the recent history—and an exactly parallel treatment of the two would be artificial. Each chapter covers the same four basic themes: the recent history of their efforts, their goals and purposes, the tools employed, and the organization of their governments for these tasks. The two chapters are structured to cover those themes in slightly different ways, as dictated by the differing nature of the two countries' programs. Chapter Five offers an initial assessment of the outcomes of social manipulation campaigns by focusing on Russian efforts in Europe and the United States—partly because their goals and character are better understood

An Overarching Concept: The Infosphere

Throughout this report, we will employ one term—*infosphere*—to refer to the broad social process of information production, dissemination, and perception.[11] A society's infosphere encompasses broadcast and print media, social media, government messaging and propaganda; the internet and all networks of communication and broadcasting that it carries; all the channels of information production that feed those outlets; and the ways in which individuals interact with information. The concept refers to the increasingly dense and interconnected connective tissue of information that provides the foundation for economic, social, and political activities. It is the terrain on which campaigns of hostile social manipulation unfold.

than Chinese initiatives, and partly because there is more open-source evidence to make these judgments. Finally, Chapter Six summarizes the main findings of the report and points to areas for further research.

To address these topics and, in particular, the activities of Russia and China in this space, we reviewed English-, Russian-, and Chinese-language sources; reviewed national security strategies and policies and military doctrines; surveyed existing public-source evidence of Russian and Chinese activities; conducted semistructured, anonymous interviews with a number of experts on, and former participants in, Russian disinformation activities; and assessed multiple categories of evidence of effectiveness of Russian activities in Europe, including public opinion data, evidence on the trends in support of political parties and movements sympathetic to Russia, and trends in national defense policies. Taken together, these multiple sources of data provide a comprehensive open-source portrait of the status of Russian and Chinese social manipulation efforts and their potential effects.

Our analysis comes with two important caveats. First, the degree of Russian influence on the 2016 U.S. election—and the fundamental issue of whether Russia determined its outcome with its multiple influence efforts—was never intended to be a focus of the analysis and is beyond the scope of this report. Existing evidence on the effective-

[11] For a similar definition, see John Arquilla and David Ronfeldt, *The Emergence of Noopolitik: Toward An American Information Strategy*, Santa Monica, Calif.: RAND Corporation, MR-1033-OSD, 1999, pp. 11–12, 16–17. For a U.S. Defense Department definition of the information environment, see U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, Washington, D.C., November 2010.

ness of Russian manipulation activities is not sufficient to support anything like a definitive judgment of the impact of Russian efforts to shape electoral outcomes. Indeed, given the multiple factors involved in determining election outcomes and the paucity of hard data on the basis for voting choices, it may never be possible to make such a clear judgment. Our analysis does conclude that whatever the truth about Russia's effect on the election, Moscow has developed an emerging suite of tools that give it the *potential* ability to have significant, perhaps even decisive impacts on electoral outcomes. This fact, we argue, should be of significant concern to the United States.

Second, this report focuses on understanding the problem rather than laying out a comprehensive strategy for dealing with it. Some initial research suggests that responding to social manipulation may be a complex task: Simply throwing "good" information against "bad" may not always work, for example, and in some limited circumstances can be counterproductive. Moreover, social manipulation frequently taps into well-established belief systems and social grievances for its effects—beliefs and grievances that must be addressed to truly reduce a nation's vulnerability to such efforts. A specific agenda for defending democracies against social manipulation must be based on deep and painstaking research.

The Broader Danger: A Corrupted Information Environment

While there is as yet no conclusive evidence about the effects of what has taken place so far, these tools and techniques are symptomatic of truly fundamental shifts in the character of the infosphere in open societies. Clearly, the United States needs to work to ensure that foreign powers cannot easily skew elections or cause large-scale social conflict. But this research points to a much bigger task: understanding whether current trends in the infosphere risk generating dynamics that can have dangerous long-term effects on the cohesion and stability of those societies.

This danger might be termed the *corruption of the infosphere*.[12] The goal of aggressors employing techniques of social manipulation will not typically be to change fundamental attitudes or "brainwash" large populations. Everything in what we know about attitudes, attitude change, and persuasion suggests that—unless a manipulator can exercise near-total control of an information space—such fine-tuning of beliefs across whole populations is extremely difficult. Instead, social manipulators will seek to cause havoc and to wage a systematic campaign of intimidation, sometimes including indirect or even direct physical violence against perceived opponents.

In the process, these trends may dramatically change our view of the effect of authoritarian regimes on world politics. Such states will continue to seek an iron grip on the information flows, beliefs, and behaviors of their own societies, a task now empowered by the vast droves of data available from state-controlled social media platforms and 21st-century surveillance technologies and techniques. But they will also increasingly seek to achieve global reach for some components of this autocratic program: not controlling information flows per se, but undermining the free world's faith in shared facts and reality; working hard to exacerbate social divisions within democracies; and, most of all, conducting an ongoing campaign of harassment, intimidation, and virtual and physical violence against groups or individuals perceived as hostile to their state control and objectives. They will try to incite the same hesitation, fear, and self-censorship among opponents globally as they do among their own citizens within their borders.

As multiple states undertake such campaigns, moreover, a related danger could be the gradual emergence of a new global alliance—informal but nonetheless significant—of autocratic states collaborating to subvert the open information sphere and destabilize democratic societies.[13] Already, evidence has emerged of Russian and Venezuelan

---

[12] See, for example, Rand Waltzman, "The Weaponization of the Information Environment," Defense Technology Program brief, American Foreign Policy Council, September 2015, pp. 4–6.

[13] On the potential for this outcome, see Christopher Walker, "A New Era of Competition," Konrad Adenauer Stiftung *International Reports*, No. 2, 2017.

coordination in intervening in Spain's Catalan-independence debate. Some Chinese social media sites have reposted Russian propaganda. Over time, states such as Russia, China, Venezuela, Iran, North Korea, and others could find ways to work together in creating alternative information systems, promoting counter-narratives, and achieving specific disruptive effects. One related outcome could be the deep fragmentation of global information networks, including the internet itself, into competing and mutually exclusive zones, with profound effects on world politics and international relations. This process is already well underway with the efforts on the part of several countries, most notably China, to build what amount to parallel internets.

It is too early to understand the full ramifications of these possibilities. Liberal democracies have long viewed the flow of knowledge and information as a competitive advantage. To inform public discussion on these issues, we have taken a two-phase approach to our analysis. This report provides findings of the first phase—an effort to define terms and understand the scope and effectiveness of Russian and Chinese activities to date. The forthcoming second report takes the story into the future, identifying a range of emerging technologies that could empower new versions of hostile social manipulation and defining an even more encompassing risk that it terms *virtual societal aggression*. Taken together, they point to an urgent need for the United States and other democracies to consider the information foundations of free societies and what must be done to shore up their resilience. The limited effects of such campaigns to date should not lead to complacency: Our research suggests not that the risks will remain low, but that the United States has been granted a window of opportunity to deal with this challenge before it becomes much more perilous.

CHAPTER TWO

Understanding Social Manipulation: Definitions and Typologies

The first step on this analytical path is to be clear about the subject of inquiry. This report is concerned with what we are calling *hostile social manipulation*. It is at once a very specific notion and one that overlaps with many other concepts. As a first step, therefore, we surveyed the terms and concepts that are part of the current debate.

Defining Key Categories

The recent discussion of these issues has featured a dozen or more terms—*misinformation*, *disinformation*, *fake news*, *propaganda*, and others. It often conflates two broad types of strategy: an all-encompassing effort to use measures short of war and the more targeted and specific approach of employing information to achieve disruptive effects. Table 2.1 lists several of the primary terms in circulation today for defining and understanding the distinctions among these various issues. (The list is not meant to indicate distinct categories; many of these terms and categories overlap with one another. Our intention here is to give a sense of the range of concepts in current discussion.) Scholars and other observers tend to use these categories somewhat interchangeably, and the dividing lines between them are ambiguous. We offer this list not to clarify precise distinctions among these categories as much as to convey the range of terms being used in the debate today.

Table 2.1
Categorizing Informational Behavior

Category	Intent	Definition	Examples
Misinformation	Often none; disseminators believe it to be true	• Inadvertent sharing of false or misleading information; "information that is initially presented as true but later found to be false"[a]	Inaccurate news stories that are corrected; spreading invalid facts about vaccines
"Fake news"	Boost traffic, drive clicks and shares, garner revenue or publicity	• Misleading or completely invented information generally spread online • Often generated by web publishers to generate views, profit; can be state-directed • Sometimes intentionally spread, can be inadvertent	Invented stories, hoaxes, satire, parody, intentionally deceptive angle or slant to news
Marketing, public affairs, public diplomacy, "strategic communications"	Affect beliefs, shape narratives with "truth" (often a form of propaganda)	• Spin on factual information to support case for product, issue, country • Provides context and slant but not intentionally deceptive • Can be employed by corporations, countries, nongovernmental organizations	Consumer marketing campaigns; U.S. government public diplomacy efforts
Propaganda	Affect beliefs, shape narratives with any techniques available	• "The deliberate and systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist"[b] • Can use falsehoods but typically packages factual information in narratives to achieve desired effect	Public service campaigns (antismoking); wartime patriotic drives; autocratic regimes' efforts to control thoughts of citizens

Table 2.1—Continued

Category	Intent	Definition	Examples
Computational propaganda	Affect beliefs, attitudes	• "The use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks"[c]	Various types of social media bots, autonomous agents combined with cognitive psychology insights
Information operations and warfare, PSYOPS	Shape information context for tactical, operational engagements	• Use of active deployment or denial of information to affect ongoing or prospective military operations • Information operations: "The integrated employment of electronic warfare (EW), computer network operations (CNO), [PSYOPS], military deception (MILDEC), and operations security (OPSEC) . . . to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own"[d]	Directing propaganda at enemy forces; efforts to undermine will of enemy forces through psychological operations (discrediting leaders); technical interference with communications (EW)
Cybersecurity/ cyberattacks	Protect/attack information systems	• The use of computer programs to ruin, degrade, or penetrate information systems in target country	Russian cyberattacks on Latvia, 2007; Stuxnet; Chinese espionage
Political warfare	Damage target society's will	• Efforts to coerce or weaken target state through intervention in domestic affairs • Discourage enemy troops from fighting	Propaganda to shape beliefs; actions to reinforce narrative
"Active measures"	Weaken Western societies; shape narratives	• Category of Soviet techniques of disinformation used during the Cold War • Political warfare to affect global trend of correlation of forces • Broader information channels; included support for proxy groups, sabotage, violence	Soviet campaign to inflame racial tensions by suggesting HIV was a U.S. government conspiracy against the African American community

Table 2.1—Continued

Category	Intent	Definition	Examples
Disinformation	Shape beliefs, narratives; counteract role of "truth"	• Purposeful spreading of combination of false and true information to create inaccurate impressions • "Deliberate use of misinformation to influence attitudes"[e] • Essentially equivalent to propaganda	Russian activities in Ukraine; spreading falsehoods during 2016 U.S. presidential election

NOTE: PSYOPS = psychological operations; HIV = human immunodeficiency virus. The definitions and concepts in the table are drawn from a number of sources, most notably National Endowment for Democracy, "Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News,'" October 17, 2017; Jennifer Kavanaugh and Michael 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; Claire Wardle, "Fake News: It's Complicated," *First Draft*, February 16, 2017; and D. J. Flynn, Brendan Nyhan, and Jason Reifler, "The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics," *Advances in Political Psychology*, Vol. 38, Supplement 1, 2017, pp. 128–129.

[a] John Cook, Ullrich Ecker, and Stephan Lewandowsky, "Misinformation and How to Correct It," in Robert Scott and Stephan Kosslyn, eds., *Emerging Trends in the Social and Behavioral Sciences*, New York: John Wiley and Sons, 2015.

[b] Garth Jowett and Victoria O'Donnell, *Propaganda and Persuasion*, Beverly Hills, Calif.: Sage Publications, 1986, p. 16. Edward Bernays (in *Propaganda*, New York: IG Publishing, 2005, originally published 1928) offers on p. 52 a related definition: "A consistent, enduring effort to create or shape events to influence the relations of the public to an enterprise, idea or group."

[c] Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," in Samuel Woolley and Philip N. Howard, eds., Working Paper 2017.11, Oxford, United Kingdom (UK): Project on Computational Propaganda, 2017, p. 3.

[d] U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, Washington, D.C., November 27, 2012, incorporating Change 1, November 20, 2014.

[e] Nathaniel Persily, "Can Democracy Survive the Internet?" *Journal of Democracy*, Vol. 28, No. 2, April 2017, p. 68.

This report's focus is a more encompassing concept. As an initial definition, we would propose the following:

Hostile social manipulation *is the purposeful, systematic generation and dissemination of information to produce harmful social, political, and economic outcomes in a target area by affecting beliefs, attitudes, and behavior.*

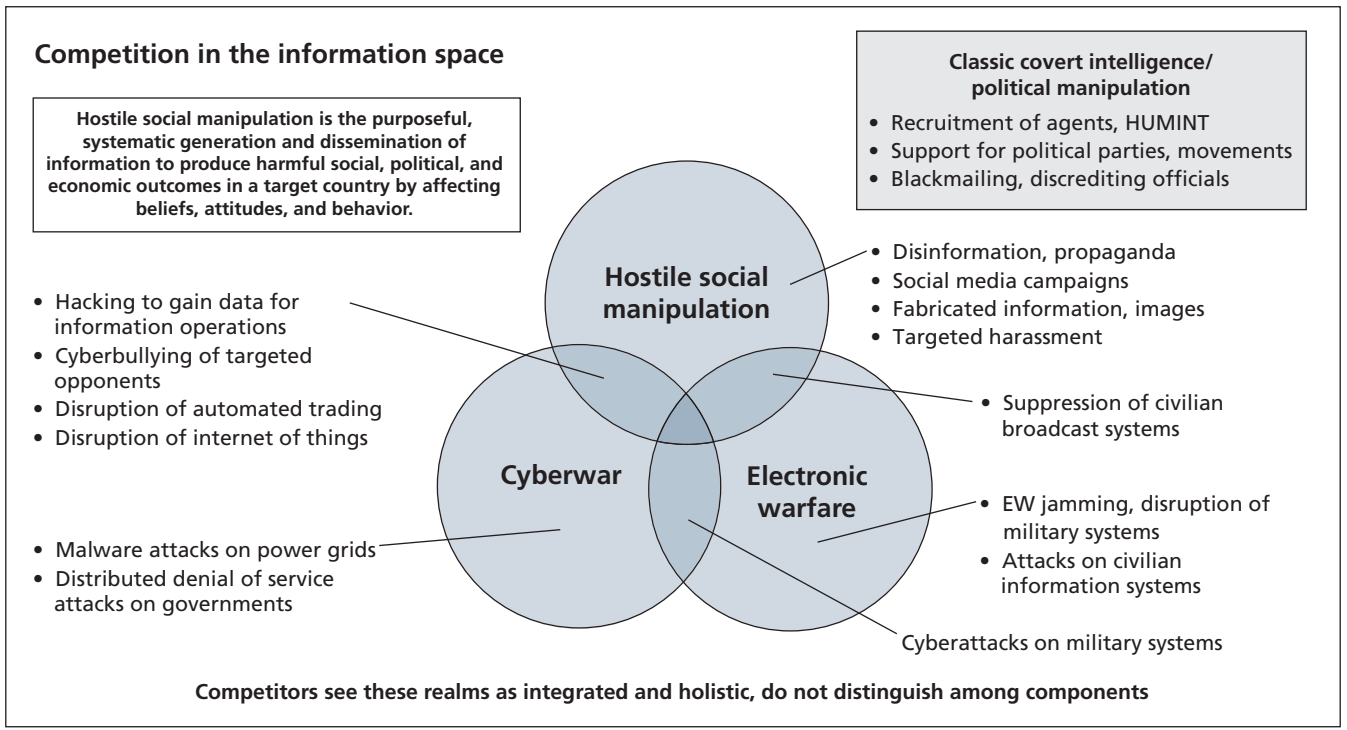
This definition stresses the role of information channels as the essential mechanism of these strategies. In all cases, the intent is aggressive: The user of hostile social manipulation seeks to do damage to the target state or use the information campaign to allow it to undertake aggressive, hostile actions. One critical distinguishing factor is that hostile social manipulation targets beliefs and attitudes, not physical assets or military forces.

This definition is very close in spirit to the concept of *information/influence warfare and manipulation* (IIWAM) offered by Herbert Lin and Jackie Kerr. They define this as "the deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes." It is thus a "hostile non-kinetic activity" whose targets are "the adversary's perceptions." Their concept of IIWAM is therefore distinct from classic cyberaggression because attacks in the IIWAM realm focus on "damaging knowledge, truth, and confidence, rather than physical or digital artifacts. . . . IIWAM seeks to inject fear, anxiety, uncertainty, and doubt into the adversary's decision making processes."[1]

Our concept of hostile social manipulation differs from two other types of information-related coercive activity. Figure 2.1 outlines this basic three-part typology, all of which falls under the encompassing category of *information warfare*. *Electronic warfare* typically refers to the use, manipulation, or degradation of information to support military operations. This concept is sometimes stretched to include more generalized attacks on societies, but the classic conception refers to activities

[1] Herbert Lin and Jackie Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation," in *Oxford Handbook of Cybersecurity*, August 14, 2017, pp. 5–7.

Figure 2.1
The Boundaries of Social Manipulation



NOTE: HUMINT = human intelligence.

in support of military operations.[2] A second related but distinct concept is *cyberwar* or *cyberattacks*, the use of malicious computer programs to achieve hostile intent, from malware that can damage civilian or military systems, to distributed denial of service attacks that compromise networks, to intrusions to steal information. We distinguish each of these from the focus of this analysis—hostile social manipulation—which refers to the broader use of information to affect other societies for strategic effect. Interestingly, neither Russia nor China has coined a single, encompassing term for this category of tools and techniques; the following chapters will discuss the terminology they employ.

As indicated in Figure 2.1, hostile social manipulation involves operations to affect attitudes, beliefs, and, ultimately, behavior and lies at the intersection of four established types of influence activities: Propaganda and disinformation, cyber aggression, active subversion of political processes, and harassment and intimidation. Of the various categories summarized in Table 2.1, the resulting combination is probably closest in spirit and practice to "political warfare." From the standpoint of Russian and Chinese activities, the focus concept of hostile social manipulation includes the use of social media campaigns, theft and targeted release of personal or secret documents, direct propaganda and efforts to shape narratives (including through broadcast venues and paid advertising), active use of disinformation, and political influence-seeking through media venues.

As Figure 2.1 also suggests, some activities reside at the boundaries between these three major categories. Direct cyberattacks on another state's military capabilities, or the civilian infrastructure that supports them, can count as a form of electronic warfare and also cyberwar. Of more interest to our focus is the boundary between cyberwar and hostile social manipulation: Campaigns of manipulation are often supported with cyberactivities, whether designed to steal information that

---

[2] John Arquilla and David Ronfeldt, "A New Epoch—and Spectrum—of Conflict," in Arquilla and Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND Corporation, MR-880-OSD/RC, 1997, p. 2. See also Bruce D. Berkowitz, "Warfare in the Information Age," in Arquilla and Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND Corporation, MR-880-OSD/RC, 1997, pp. 175, 177.

is then used in the information campaign or to conduct coercive or intimidating attacks on information networks.

It is important to keep in mind that states such as Russia, China, and North Korea tend to view these dividing lines as blurry rather than fixed and pursue campaigns that integrate all three major elements in this typology. This is one reason neither has a neat-and-clean term for hostile social manipulation: The general practice reflects a combination of concepts and mechanisms in all of their national strategies. This complicates efforts to deal with the problem, both because it can be difficult to draw neat lines around activities the United States hopes to curtail and because Russia and China see these techniques as a perfectly acceptable component of a much more encompassing vision of ongoing competition.

The concept of hostile social manipulation, therefore, encompasses Russian efforts to use propaganda, fabricated stories, appeals to Russian-language populations, and other information techniques to foment unrest among populations in Eastern European countries. It includes efforts of extremist groups to stimulate greater radicalization among target populations, as well as Russian intervention in U.S. social media platforms. It can involve efforts at intimidation, such as generating cyberbullying and using information channels to discredit, harm, or even bankrupt specific firms. It includes Chinese efforts to promote specific narratives among countries in Southeast Asia, and to shape the thinking of pro-Chinese subpopulations, including the region's ethnic Chinese diaspora.

The Goals of Social Manipulation

Campaigns of social manipulation are very flexible and tailorable tools. No two are exactly alike. Table 2.2 lists the primary objectives we have drawn from the current experience in social manipulation, but this set is not exhaustive.

One implication of this list is that, to be effective, social manipulation need not affect the most direct and, in a sense, crude measure of attitude change—the degree of favorability toward the social manipu-

Table 2.2
Goals and Objectives of Social Manipulation Campaigns

Objective	Examples
Improve attitudes toward aggressor/social manipulator	• General propaganda offering aggressor state narratives, views • Cultural information to promote positive feelings
Generate conflict and tension among components of target society	• Promoting both sides of an intense social debate with the goal of prompting clashes, protests • Spreading rumors, false information, exaggerated accounts to intensify grievances, anger
Intimidate, silence, or render ineffective groups or individuals in target society who are opposed to the goals of the manipulator	• Discredit, threaten, direct physical violence against social activists, groups • Target exiled political, social activists
Distract attention, cause confusion	• Cloud agreed understandings of key issues • Promote a wave of disinformation to undermine faith in shared truth
Discredit, destabilize, undermine or promote specific groups, institutions important to competitive strength of target country	• Attacks targeting U.S. military personnel to undermine morale, cohesion • Disinformation campaigns to undermine faith in national media outlets • Efforts to undermine profitability of key firms
Discredit specific popularly elected leaders in unfriendly or target countries	• Chinese efforts to undermine support for Taiwanese leaders who do not support China's policies and approaches • Russian efforts to support attacks against key European leaders
Delegitimize public institutions, especially governmental, in target nation (and/or delegitimize those institutions in the eyes of other countries)	• Efforts to influence elections to reduce perceived legitimacy of outcomes • Using disinformation to exacerbate public loss of faith in key institutions
Erode the basic distinction between truth and falsehood in democratic societies	• Spreading false reports on social trends, major political figures
Spark desired behavior among highly targeted populations or groups (voting, terrorism, protest)	• Seed extremist sites with information • Conjure specific protests, riots • Influence voting outcomes

lator. That is a possible goal but often not the predominant one. The tools of social manipulation may be best suited to sow chaos and to weaken a target state by influencing social, political, and economic outcomes. If Russia's social manipulation efforts were designed to ease Western confrontation, for example, they have manifestly failed. There is much contrary evidence, in fact, that these campaigns have been counterproductive at a geopolitical level, prompting a much more vigorous Western response than would have been the case without them. But the campaigns may have a more long-term purpose—to undermine social institutions, exacerbate social and political divisions, and intimidate political or ideological opponents in target countries in ways that weaken them as international actors over time.

The Range of Options: Examples of Hostile Social Manipulation

In pursuing this range of goals, social manipulation campaigns can make use of an impressive array of specific tools and mechanisms for influence. Table 2.3 offers examples of specific techniques and mechanisms. This is a broad and inclusive list, not a discrete set of precise categories. The techniques here are not mutually exclusive: Some of the approaches—trolling, for example, or microtargeting—can be a subset of another approach (such as computational propaganda). Our goal here is to convey a wide range of the distinct tools that can be used alone or in various combinations to achieve social manipulation.[3]

As the list makes clear, social media is only one part of this universe. Strategies for social manipulation typically employ a combination of traditional information channels, including print advertisements and broadcast television. This is likely to remain true for some

[3] A fine recent summary of such efforts is Samantha Bradshaw and Philip N. Howard, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation," Working Paper No. 2017.12, Oxford, UK: Project on Computational Propaganda, 2017.

time, because most people—including in the United States—still get their news mostly from broadcast sources.[4]

At the same time, the real innovations in this field are coming from the targeted, evolving, and data-based use of social media platforms. The outstanding recent example is computational propaganda, the use of automated accounts (known as *bots*) to grab information and send messages based on preset algorithmic principles, without human engagement. Twitter estimates that 8.5 percent of its user accounts may be bots; other estimates suggest the real number could be close to double that—meaning that between 25 and 50 million accounts on Twitter could be automated.[5] Neither Facebook nor Instagram has released official estimates of the proportion of bot accounts, but both periodically conduct "purges" that eliminate millions of accounts, suggesting that the number of automated or fake accounts could be quite high.

Because of their automation, relatively small numbers of bots can achieve significant effects, generating a sizable proportion of the social media traffic on any given issue. In a study of Twitter discourse in the lead-up to the Brexit referendum, the Computational Propaganda Project at the Oxford Internet Institute (OII) found that in its sample, less than 1 percent of the accounts generated almost *one-third* of all the Brexit-related traffic, signaling a high level of automation in the Twitter discourse on the referendum.[6] As noted above, recent studies suggest that the vast majority of social media messages dealing with the independence debate in Catalonia were generated by automated or fake accounts.

---

4 Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives*, Vol. 31, No. 2, Spring 2017; Levi Boxell, Matthew Gentzkow, and Jesse M. Shapiro, "Is Media Driving Americans Apart?" *New York Times*, December 6, 2017.

5 Zoey Chong, "Up to 48 Million Twitter Accounts Are Bots, Study Says," CNET, March 14, 2017.

6 Philip N. Howard and Bence Kollanyi, "Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum," Research Note 2016.1, Oxford, UK: Project on Computational Propaganda, 2016, p. 4.

Table 2.3
Techniques and Mechanisms for Social Manipulation

Type	Definition or Characteristics	Examples
Broadcast media	The use of cable television stations, online channels, or other means of broadcasting state-created or promoted content	RT's YouTube and cable presence; Chinese-language broadcasts in Asia
Public diplomacy and traditional propaganda	The use of state assets to promote narratives and content that serve purposes of social manipulation campaigns	Classic public diplomacy tools such as sponsored libraries, cultural events; government-sponsored websites; messages directed to diaspora populations
Content creation	Developing real or fake content for distribution through multiple channels with goal of broad uptake by web/social media universe; increasingly, artificial intelligence (AI)–generated content	Fabricated audio or video content, often by AI; use of AI to generate real stories from basic data (Associated Press [AP]); blog sites; promoting hoaxes
Disinformation	Spreading false reports, invented claims, hoaxes to create chaos, uncertainty, or to harass	2013 Twitter hack of AP account with hoax of White House attack; fake videos of killings to inflame sectarian hostility; 2014 fake Louisiana chemical spill report
Doxing	Searching for and publishing private or identifying information about a particular individual on the internet, usually with malicious intent	Russian theft of Democratic Party documents and release to Wikileaks in 2016; Russian harassment of individuals by releasing private information
Direct advertising	Buying paid ads on broadcast or print media, online, in social media	Pro-Russia and pro-China newspaper inserts; social media election ads
Computational propaganda	Use of automated accounts (bots and botnets) to generate large numbers of messages, obstruct hostile messages, or engage with audiences	Use of bots in recent elections in U.S., Eastern Europe, and Mexico to flood Twitter with selected messages
Social media commenting	Making positive, negative, or neutral/distracting comments in social media threads, increasingly with bots and AI	Saudi Arabia's strategy of "hashtag poisoning"; Chinese "50-Cent Army" mass commenting

Table 2.3—Continued

Type	Definition or Characteristics	Examples
Trolling	Posting inflammatory content; harassing or insulting targets online to generate attention, disrupt dialogue	Classic trolling community such as 4chan; specific accounts set up by Russian agencies; attacks on specific individuals
Use of "Dark Web," dark social networks	Manipulating social media spaces that are not fully public, either group or individual, such as closed Facebook groups, WeChat groups, private Instagram accounts, 4Chan sites	Russian creation of "honey pot" groups in 4Chan and elsewhere to attract motivated members
Astroturfing	Flooding a message space to create a sense of conventional wisdom, faked social proof	Enormous number of Brexit-oriented messages in days before vote
Behavioral redirection	Sensing expressed interests and redirecting people online or in social media platforms to content that modifies intent, behavior	Google redirects people searching for suicide information or extremist content to prevention videos
Social influencer campaigns	Identify and influence individuals known or believed to have disproportionate influence on others' attitudes, behavior	Identify social media network influencers; shape messages of opinion leaders
Identity theft, personal harassment, psychometric profiling	The use of available protected and open data on the internet to disrupt the lives of target groups or individuals (related to classic cybertechnique of social engineering)	Targeting of anti-Russian activists and journalists; South Korea National Intelligence Service attacks on opposition parties
Microtargeting	Using data to target small groups or even individuals by views, likes, desires	Focus on right- or left-wing advocacy groups in U.S.

The Past: Understanding the Context for Social Manipulation

Current efforts to manipulate public opinion and, potentially, behavior represent the most recent expression of a long tradition of propaganda, disinformation, and public diplomacy. An important question is whether the current version reflects a difference in degree or kind. There is, in fact, convincing evidence, as we will review below and in

the later chapters on future trends, that emerging technologies could empower not merely stronger versions of propaganda or disinformation, but an entirely new and more powerful kind of capability.

The initial modern phase of social manipulation was the propaganda campaigns of World War I, with efforts on all sides to formally and systematically influence public opinion in support of the war effort. One of the classic statements about the nature of propaganda came from Edward Bernays, a leading practitioner of the art. Bernays, writing in 1928 with experience in the World War I Creel Committee still fresh in his mind, viewed it as the "conscious and intelligent manipulation of the organized habits and opinions of the masses." The experts in this art constituted, for him, "an invisible government which is the true ruling power of the country."[7] It was too time-consuming for people to make their own decisions on a million issues, he argued; better for the propagandists to do it for them, through persuasion. His essential concept was that people are guided by unconscious motives, motives of which they are often unaware—and that the propagandists' task is to manipulate these unconscious preferences to shape behavior.

Bernays laid the groundwork for today's focus on specific social subgroups by emphasizing that propaganda targeted people not as individuals, but as members of "interlocking group formations." And he emphasized the importance of persuading the leaders of those social groups—people whose opinions carried disproportionate weight with their followers.[8]

---

7 Bernays, 2005, p. 37.

8 Bernays, 2005, pp. 55, 73. On the one hand, Bernays saw propaganda as the tool of an unseen governing class, instructing Americans how to behave. But such a vision presumed some degree of coordination and singular message, or else the result would be chaos; some of his language clearly has an authoritarian tone, implying that a select group of leading men and women were running society, working to "mold the mind of the masses that they will throw their newly gained strength in the desired direction." On the other hand, he had to recognize the obvious—that often the messages of propagandists contradict one another. In fact, he celebrated the art as contributing to a society based on "open competition" (Bernays, 2005, pp. 47, 39). See also Edward L. Bernays, *Crystallizing Public Opinion*, New York: IG Publishing, Reprint Edition 2011, in which Bernays expresses other aspects of his faith in an elite group of persuaders and the risks of the herd.

Another classic treatment of propaganda is the slim 1965 volume by the French intellectual Jacques Ellul, which offers several themes that have become common in assessing social manipulation efforts. One is the idea that propaganda was designed not to modify ideas but to use existing beliefs to provoke action—to make people militant and ready to act on existing views. It was very difficult, he wrote, to change "an individual's firmly established opinion."[9] Propaganda needed to make use of peoples' group membership to crystallize their opinion and generate action. It was all about partitioning, he suggested—finding small groups within society and prompting them to act.

During the Cold War, Soviet-bloc intelligence services placed a greater emphasis on deceptive operations, *dezinformatsiya*, to influence opinions or actions of individuals and governments. The Union of Soviet Socialist Republics (USSR)'s active measures included media control and manipulation, spread of written and oral disinformation, use of foreign communist parties and front organizations, clandestine radio broadcasting, manipulation of the economy, kidnappings, paramilitary operations, and support of guerrilla groups and terrorist organizations.[10] The basic goal of active measures was to weaken the USSR's enemies, primarily the United States, and to advance Soviet views and interests globally.

There are hundreds of examples of disinformation-style activities undertaken by the Soviet Union as part of its decades-long campaign of active measures. During the 1984 Summer Olympics, for example, the Komitet Gosudarstvennoy Bezopasnosti (KGB) sent forged racist letters threatening Olympic athletes from 20 Asian and African nations in the name of the Ku Klux Klan.[11] The Soviets forged a memorandum from the President of the United States to the Secretaries of State and Defense and the director of the CIA that ordered the establishment of a U.S. military force called the "Permanent Peace Forces" that would

---

[9] Jacques Ellul, *Propaganda*, New York: Vintage Books, 1965, p. 33; see also pp. 25–35.

[10] U.S. House of Representatives Permanent Select Committee on Intelligence, *Soviet Active Measures*, Washington, D.C.: Government Printing Office, 1982, p. 31.

[11] Fred Barbash, "U.S. Ties 'Klan' Olympic Hate Mail to KGB," *Washington Post*, August 7, 1984.

be used to intervene in Latin America. The Soviets also circulated false reports that the United States was bringing Latin American children to the United States to use their organs for organ transplants. Unsurprisingly, these disinformation attempts inflamed anti-American sentiment in Latin America.[12]

One of the most infamous of the Soviet operations was called Operation Infektion, a disinformation campaign carried out in the 1980s. The objective was to make people believe that the human immunodeficiency virus and acquired immunodeficiency syndrome (HIV/AIDS) was a result of American biological weapons experiments. It was a good example of pursuing disinformation by piggybacking on existing myths rather than creating them wholesale. Theories about the U.S. government creating the AIDS virus predated any KGB manipulation, which may have made the misinformation spread by the Soviets more effective. By 1988, the theory had been published in over 200 periodicals in 80 countries. A survey conducted in 1992 found that 15 percent of Americans considered it "probable" or "certain" that the AIDS virus was deliberately created in a government laboratory.[13] A study conducted by the RAND Corporation and the National Institute of Child Health and Human Development in 2005 found that some variant of this myth persisted almost two decades later in the African American community.[14] Almost half of the respondents said that HIV was man-made, 26 percent believed HIV/AIDS was pro-

---

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

[13] Thomas Boghardt, "Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence*, Vol. 53, No. 4, December 2009.

[14] The prevalence of this conspiracy theory could also stem from distrust within the African American community created by the Tuskegee syphilis experiment conducted by the U.S. government on African American men, or from other factors. While it is not possible to directly link the prevalence of this belief to the Soviet disinformation campaign, it is an interesting and relevant data point.

duced in a government laboratory, and 12 percent believed it was created and spread by the U.S. Central Intelligence Agency (CIA).[15]

One lesson of earlier phases of hostile social manipulation thus points to the limits of the ability to reach into other societies. Domestic propaganda can be highly effective, especially if undertaken by autocratic states that can control the information environment. So far, there are precious few examples of efforts to achieve significant strategic effects in other countries through such means that have achieved anything but marginal effects. Yet evolving technology may provide social manipulators with unprecedented capabilities to do just that.

A distinct form of history can be written about prior eras in which the shared truths in U.S. society came under particular strain. A major recent RAND study on the phenomenon of "Truth Decay" considered three such periods: "yellow journalism" in the 1880s and 1890s; the "jazz journalism" and sensationalism of the 1920s and 1930s; and the challenge to accepted understanding of events in the 1960s and 1970s.[16] Each period, the authors found, was in part a product of social and political turmoil that affected the treatment of public issues at that time. The most direct indicators of truth decay—the rise of misinformation and active disinformation in the public sphere—is typically a symptom of deeper problems with democracy.

This historical perspective on periods of especially powerful misinformation reinforces a central message of this report. Social manipulation is effective to the degree that vulnerabilities in a society allow it. Such techniques can seldom create from whole cloth the situations that allow an aggressor to manipulate political life; they can only take advantage of realities being created by underlying trends. This has been the story of Russian and Chinese efforts to date—searching for seams and gaps in the social and information fabric of other countries. We now turn to a detailed assessment of their strategies, concepts, and activities in this realm.

---

15 "Are HIV/AIDS Conspiracy Beliefs a Barrier to HIV Prevention Among African Americans?" *Journal of Acquired Immune Deficiency Syndromes*, Vol. 38, No. 2, February 1, 2005, pp. 213–218.

16 Kavanaugh and Rich, 2018, pp. 41–78.

CHAPTER THREE

Hostile Social Manipulation: Russian Activities

Much ink has been spilled over the Kremlin's attempts to influence foreign audiences in recent years. Although there is general agreement that these efforts exist, there is less agreement on exactly what Moscow seeks to accomplish with these efforts; how Russia exerts influence in the informational realm; and who orders, designs, and executes the efforts. Additionally, few recent studies address the effectiveness of Russian efforts. This chapter aims to assess what is understood and identify areas where additional inquiry is necessary.

One of the robust debates on this issue is a terminological one. Russian efforts to use information to influence target audiences have been called by many a name: *hybrid warfare*, *psychological warfare*, *gray zone activities*, *information operations*, *disinformation*, *active measures*, and so on. We use the term *social manipulation*. As defined earlier, *hostile social manipulation* is the purposeful, systematic generation and dissemination of information to produce harmful social, political, and economic outcomes in a target country by affecting beliefs, attitudes, and behavior.

It is important to acknowledge that s*ocial manipulation* is not a term Russia uses. Nor is there any Russian equivalent of the term in publicly available Russian doctrine or relevant literature. Instead, Russia uses the term *information warfare* (*informatsionnaya voyna*).[1]

[1] As Keir Giles notes, Russian sources use the terms *information warfare* (*informatsionnaya voyna*) and "information confrontation" (*informatsionnoye protivoborstvo*). The distinction between these terms is debated in the literature (Keir Giles, *Handbook of Russian Information Warfare*, Research Division, NATO Defense College, November 2016, p. 6).

Russia appears to conceive of and conduct information warfare and social manipulation as a perpetual activity, in war and peace, serving offensive and defensive ends. Therefore, for our purposes the term *social manipulation*, as outlined in this report, is an analogous way of understanding and thinking about the Russian construct and approach of the information space in a way that is, hopefully, understandable for the Western military and policy community.

In this chapter, we focus on Russian efforts conducted outside the scope of outright military conflict. Russia appears to have a number of objectives in these efforts—though, as will be made clear in the discussion of Russian goals below, these must largely be inferred from Russian activities and public statements about U.S. and Western threats to its security. There is no conclusive source of evidence, at least in open-source literature, that clarifies what precisely Russia is trying to do. Moreover, different senior leaders and bureaucratic entities may perceive somewhat distinct goals and objectives. Broadly speaking, though, Russia appears intent on weakening Western cohesion and governance, in part through undermining faith in public institutions, leaders, and political parties and intensifying partisan and ideological divides. More broadly, its goals seem to be to toxify the information environment and foster the transition to something closer to a "post-truth" world. This wider objective serves the dual Russian goal of undermining Western democracies and empowering actors with strong information operations capabilities.

In pursuing these goals, Russia appears to conceive of and conduct information warfare and social manipulation as a perpetual activity, during peace and war, which simultaneously serves both offensive and defensive ends. Likewise, social manipulation can be directed against either domestic or foreign audiences, but we examine only those Russian efforts to influence audiences outside of Russia. We do not look at Russia's extensive use of information to shape the opinions, attitudes, or behaviors of the country's domestic populace. The high preponderance of our references to Russian efforts targeted against the United States is indicative not of the scope of our research, but rather of the rigor of the evidence that exists for these cases. Our analysis

also excludes traditional clandestine and espionage activities targeted at individuals or organizations.

This chapter is divided into seven sections. The first describes our methodology, including caveats and limitations. The second covers the historical evolution of the Soviet and Russian approaches to social manipulation. The third outlines the doctrinal foundations guiding Russian thought behind social manipulation efforts. The fourth discusses Russia's current social manipulation strategies, including the actors, targets, target audiences, messages, and sources of narratives. The fifth itemizes recent Russian social manipulation actions. The sixth examines how effective these strategies and actions have been and discusses the wider debate on effectiveness in social manipulation. We close the chapter with our conclusions.

Methodology

For the analysis in this chapter, we used a mixed methods approach. This included a survey of relevant literature; examination of primary documents; and semistructured interviews with experts, scholars, and practitioners. The primary sources included documents accessible through official Russian government websites and declassified U.S. government documents available through archives and other sources. Secondary literature was drawn from academic and research papers, including relevant work from Russian think tanks and writers.

We conducted the semistructured interviews in person and by phone.[2] The interview subjects were selected using purposive sampling and therefore may not be a representative sample of the field. The subjects were chosen based on their firsthand experience working in Russia on this topic, working in or with Russia in a diplomatic capacity, or examining these issues as analysts or intelligence officers.

[2] For a discussion of interview types, see Margaret C. Harrell and Melissa A. Bradley, *Data Collection Methods: Semi-Structured Interviews and Focus Groups*, Santa Monica, Calif.: RAND Corporation, TR-718-USG, 2009, pp. 27, 29–46.

Efforts have been taken to preserve the anonymity of the interview subjects, as the interviews were conducted on a not-for-attribution basis. Throughout this report, the subjects are referred to using general monikers and have been assigned three-digit identification numbers so that the researchers could identify between those with similar monikers. The group of subjects was limited to those individuals who were accessible to the research team and those willing to engage. Lastly, we attempted to solicit interviews with, and gather literature from, individuals from various disciplines and backgrounds to understand these issues from various perspectives.

Caveats and Limitations

This analysis was conducted using only unclassified and publicly available material. Given the deliberately opaque nature of Russian social manipulation efforts, it is difficult to make definitive judgments about Russian efforts based on open-source material alone. Therefore, our approach limits the claims and conclusions we can put forth. We attempt to be transparent about the limitations of our conclusions and the availability of sources throughout the chapter. In many cases, available evidence indicates a link between observed efforts and Russian sponsorship; however, it is rare to be able to definitively prove a link or meet the highest standards of proof.

Given the breadth of the many disciplines this topic touches on, it is unlikely that our efforts represent a comprehensive survey of the subject, though we aimed to identify and include key scholarship and individuals. Given the rapidly evolving nature of this topic, some of the evidence or issues cited in this chapter may be deemed to be incorrect, obsolete, or perhaps substantiated by information made public by the time this study is published.

This analysis of Russian social manipulation activities does not attempt to answer whether Russian efforts tipped the 2016 U.S. presidential election (or any other specific election or referendum). That question was intentionally beyond the scope of our analysis. Our research, moreover, suggests that the evidence presently available, at least in the unclassified realm, is insufficient to render an analytically conclusive verdict on that sensitive question.

History: Soviet and Russian Approaches to Social Manipulation

Information has been used by states to influence and manipulate audiences for centuries.[3] The same is true in Russia, and current efforts at social manipulation fit into a long historical tradition of employing similar techniques. Tsarist police, or Okrhana, attempted to foment discord among émigré groups and to buy positive press abroad for the Russian empire by secretly paying journalists.[4] Perhaps the most notable example of Tsarist-era social manipulation is the Okrhana's production and dissemination of *The Protocols of the Elders of Zion*—fabricated minutes of an alleged meeting of the First Zionist Congress, describing a Jewish plot for global domination and suppression of Gentiles. After their initial publication in 1903, the *Protocols* were republished in several languages, and later used by the Nazi regime as anti-Semitic propaganda (having influenced Adolf Hitler, according to some scholars).[5]

With the overthrow of the Tsarist regime in 1917, the new Soviet ruling regime introduced its own internal and external social manipulation efforts, both during and after its ascent to power. Internally, Bolshevik leadership under Vladimir Lenin designed and executed propaganda campaigns to discredit domestic and foreign adversaries and to foster support for the Communist ideology. In an article directed at the new Soviet press (after confiscating its printing presses and imposing strict censorship measures), Lenin offered guidance on the parameters that journalists should follow:

---

[3] In his classic work *Art of War*, Sun Tzu wrote "all warfare is based on deception. [. . .] Thus one who is skillful at keeping the enemy on the move maintains deceitful appearances, according to which the enemy will act" (Sun Tzu, *Art of War*, military treatise, circa fifth century BCE).

[4] Dennis Kux, "Soviet Active Measures and Disinformation: Overview and Assessment," *Parameters*, Vol. 15, No. 4, 1985, p. 20; also see Wojciech Karpinski, "Agents and Exiles," *Survey*, Vol. 27, Autumn–Winter, 1983.

[5] CIA translation of S. Simoni, "Soviet Anti-Semitism and the Prague Trial," Yedioth Hayom, 1952; Randall L. Bytwerk, "Believing in 'Inner Truth': The *Protocols of the Elders of Zion* in Nazi Propaganda, 1933-1945," *Holocaust and Genocide Studies*, Vol. 29, No. 2, 2015.

> Instead of 200–400 lines, why don't we talk in 20–10 [sic] about matters such as the treachery of the Mensheviks, the lackeys of the bourgeoisie, or such as the Anglo-Japanese attack for the sake of reestablishing the sacred rule of capital, or such as how the American billionaires gnash their teeth about Germany. [. . .] Less political noise. Less intelligent-like discussions.[6]

Externally, the early Soviet leadership sponsored the dissemination of disinformation in Western Europe in the 1920s to malign émigré groups.[7]

In the 1950s, Russian social manipulation efforts "underwent an 'expansion, institutionalization, and professionalization.'"[8] Shortly after the establishment of the Soviet state security agency—the KGB—in 1954, the regime created an institution within the KGB—Department D—responsible for social manipulation efforts. Department D was located within the First Chief Directorate of the Soviet intelligence apparatus. Moscow began devoting more resources to social manipulation (*dezinformatsiya*) at this time.[9]

Department D underwent several organizational changes in the following decades. In the 1960s, its name was changed to the Active Measures Department, or Department A. It was then promoted to a service, which meant that it reported directly to KGB leadership, signaling the increased significance of these efforts to the Soviet government.

By the 1970s, the Soviets had established a global network to support their social manipulation efforts. The network included "agents,

---

6 Peter Kenez, *The Birth of the Propaganda State: Soviet Methods of Mass Mobilization, 1917–1929*, Cambridge, UK: Cambridge University Press, p. 49.

7 Kux, 1985, p. 19.

8 Max Holland, "The Propagation and Power of Communist Security Services Dezinformatsiya," *International Journal of Intelligence and Counterintelligence*, Vol. 19, No. 1, 2006, p. 5.

9 The terms *disinformation* and *active measures*, which have been used to describe recent Russian efforts to influence foreign audiences using information, descend from Soviet intelligence terminology. The former is a transliteration of the Russian term *dezinformatsiya*, and the latter a translation of the Russian phrase *aktivnyye meropriyatiya*. Though exact definitions of these terms differ, disinformation is generally agreed to mean the deliberate use of partially or wholly false information to mislead (Kux, 1985, p. 19).

organizations and technical facilities."[10] Established in 1978, the International Information Department of the Communist Party of the Soviet Union (CPSU) became the coordinating mechanism of Soviet social manipulation efforts. The creation of this organization further demonstrated the regime's desire to prioritize social manipulation, ensure its coordination, and allow it to respond nimbly to external developments in a timely fashion.[11] Additionally, intelligence services across the Soviet bloc (the Warsaw Pact) became important parts of the efforts to conceive of, produce, and disseminate propaganda.[12]

In the 1980s, Soviet social manipulation was directed, planned, produced, and executed by several institutions. Though still an important part of these efforts, the KGB was only one organization in a larger bureaucracy charged with social manipulation in this era.[13] The Politburo, the most senior policymaking organ in the Soviet government, oversaw social manipulation at a high level, approving "all major themes of Soviet propaganda."[14] Three organizations reported directly to the Politburo: the KGB, the International Department of the CPSU, and the aforementioned International Information Department of the CPSU. The system was restructured again in 1986–1987, with the reorganization of the International Department of the CPSU and the dissolution of the International Information Department of the CPSU.

Given its inherently secretive nature as an intelligence agency, the KGB's Service A acted as the covert complement to its overt counterparts. Service A coordinated with both the International and the International Information Departments of the CPSU and supported

---

[10] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, *Soviet Covert Action (The Forgery Offensive)*, Washington, D.C.: U.S. Government Printing Office, 1980, p. 7.

[11] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, pp. 6–7.

[12] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 7.

[13] Congressional Record, "Soviet Active Measures in the United States: An Updated Report by the FBI," December 9, 1987, p. E4717.

[14] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 6.

their overt efforts by creating, disseminating, and planting such nonattributable "devices of covert action as forgeries, planted press articles, planted rumors, and controlled information media."[15]

Soviet Approaches to Social Manipulation

Although the Cold War–era organizations referenced above are now relics of the past, they remain relevant today and are therefore worth examining. Even though the Soviet state apparatus that was once responsible for social manipulation efforts dissolved with the collapse of the Soviet Union, its vestiges remain in the form of both institutional knowledge and writings.

As many scholars, analysts, and policymakers have aptly noted, Russian President Vladimir Putin and many in his inner circle, as former Soviet intelligence agents, were trained to view information (whether incoming or outgoing) through a specific lens. Putin and his cohort spent their early years in the KGB in the midst of Yuri Andropov's reforms of the agency. As its chief, Andropov sought to repress dissent in the Soviet Union, and his leadership of the KGB shaped its institutional culture into one that was highly suspicious and "ideologically drilled."[16] Major General Oleg Kalugin recalled the agency and its approach toward information during the Andropov era: "the KGB penetrated practically all pores of our social organism, all spheres of life . . . and destinies of millions of people depended on information which the KGB manipulated at its own discretion."[17] Some have argued that the experience of training and working as a KGB agent has left an indelible mark on the mindset of Putin and his colleagues and has molded their perceptions of information as both a tool and a threat:

---

[15] "CIA Study: Soviet Covert Action and Propaganda," in U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 61; Kux, 1985, p. 21.

[16] Robert W. Pringle, "Andropov's Counterintelligence State," *International Journal of Intelligence and Counterintelligence*, Vol. 13, No. 2, 2000, p. 199.

[17] Oleg Kalugin, *Vechernyaya Moskva*, November 3, 1990, as referenced in Pringle, 2000, p. 199; Giles, 2016, p. 36; in-person interview with former CIA analyst 024, November 20, 2017.

> Putin's formative lessons came from a career in the KGB, devoted to protecting the Communist Party's monopoly on power. He joined in 1975, at a time when veterans of Stalin's secret services were still serving. . . . They strongly believed that access to information and to means of communication should be under control of the state. . . . He was in the KGB when it crushed dissidents, hunted for samizdat publications, and sought to cut back the international phone lines after the 1980 Olympic Games in Moscow. This was the organization that shaped Putin's view of the world. Long after he left the KGB and after he was promoted to prime minister, Putin still retained a deep suspicion of journalists, a legacy of his years in the security service.[18]

Putin and his associates have been at Russia's helm for nearly two decades. This continuity in leadership indicates a continuity in thought.[19] Even in the interim years following the Soviet collapse, journalists accepted bribes in exchange for publishing false information about government officials or other public figures, and the security services collected compromising information, or *kompromat,* which was revealed to the public at opportune times.[20] Thus, the influence of Soviet social manipulation practices has likely endured despite internal institutional and external geopolitical changes.

A former CIA analyst responsible for covert action directed against the Soviet Union in the 1970s and 1980s also noted the similarities between Soviet-era social manipulation that he experienced and Russian efforts today, in terms of their conception, principles, and desired outcomes. The analyst said the only differences they observed are the mechanisms used to disseminate Russian messages—mechanisms brought about by advances in technology.[21] Though Soviet intelligence practices are likely an important influence on current Russian social manipulation, these appear to be but one driver shaping the Rus-

---

[18] Andrei Soldatov and Irina Borogan, *The Red Web*, New York: Public Affairs, 2015, p. 90.

[19] Giles, 2016, p. 36.

[20] Soldatov and Borogan, 2015, pp. 61–62.

[21] In-person interview with former CIA analyst 024, November 20, 2017.

sian government's conception and execution of information for influence efforts.

Soviet Targets, Target Audiences, Objectives, and Messages

Externally, the United States was the principal—though certainly not the only—target of Soviet social manipulation.[22] Soviet efforts were designed to undermine U.S. influence, credibility, and policymaking power, and, in doing so, to enhance the favorability of Soviet policies.[23] To achieve this objective, the Soviet government undertook efforts to shape the opinions of chosen individuals, groups, and mass publics globally. By tarnishing the U.S. image in the minds of these target audiences, Moscow believed it could frustrate U.S. interests and isolate Washington from its allies and the broader international community.[24]

At the highest level, Soviet messaging focused on several recurring themes: portraying the United States as an "aggressive, colonialist and imperialist power . . . demonstrat[ing] that the policies and goals of the United States are incompatible with the ambitions of the underdeveloped world," and portraying Soviet activities as positive and defensive in nature.[25] More narrowly, the Soviets designed messages to discredit or support specific policies. Soviet messaging was not exclusive in its support of a specific U.S. political ideology, and disseminated messages were consistent with views of both the political right and the left.[26]

Moscow also gained access to reputable foreign news outlets. Some Soviet intelligence agents worked at foreign news outlets as journalists. Though most of their time was spent reporting on legitimate news, they were instructed by their agency to print one or two false or mis-

---

[22] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 7.

[23] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 8.

[24] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 60.

[25] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 8.

[26] In-person interview with former CIA analyst 024, November 20, 2017.

leading stories a year.[27] In other cases, Soviet agents attempted to cultivate relationships with editors of Western media outlets to earn their trust over time. Once developed, the relationship would be used as a conduit to pass propaganda for print in the reputable outlet, thereby masking the hand of the Soviet Union as the originator of the stories.[28]

Reflexive control was another factor in Soviet thinking on the use of information to influence. As a form of deception, or *maskirovka*, *reflexive control* refers to the communication of specific information to an adversary such that the adversary willingly pursues actions that are favorable to the perpetrator, yet the adversary is unaware of having been influenced.[29] In other words, *reflexive control tactics* are "systematic methods of shaping an adversary's perceptions, thereby decisions, and latently forcing him to act voluntarily in a way that would be favorable to [Soviet] strategic interests."[30]

This concept has evolved in the decades since its inception and has been applied in both the military and civilian spheres. Though the term for this concept appears to have changed to something roughly translated to *perception management*, the concept continues to influence thinking on social manipulation activities in Russia.[31]

Categories of Soviet Social Manipulation

Soviet efforts to influence foreign policy outcomes can be categorized as *white*, *gray*, or *black*. *White* efforts are those that were overt, meaning operations that were publicly attributed to and acknowledged by the Soviet Union. These include political discourse and public diplomacy efforts. In other cases, the Soviets used unaffiliated media outlets

---

27 "Soviet Forgeries and Disinformation," statement of Ladislav Bittman, in U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, pp. 37, 46.

28 In-person interview with former CIA analyst 024, November 20, 2017.

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

30 Can Kasapoglu, "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control," NATO Research Division, Research Paper No. 121, November 2015, p. 2.

31 Giles, 2016, pp. 19–20.

or Communist fronts as proxies to disseminate information. Though Soviet sponsorship of these efforts was suspected, it was not formally acknowledged. These were considered *gray* activities. *Black* operations were those in which the identity of Soviet involvement was deliberately concealed through false attribution, clandestine methods, or the coercion of foreign media outlets.[32] Though these categories offer a useful taxonomy by which to classify Soviet social manipulation practices, in reality, Soviet operations were often a mosaic of white, gray, and black practices.[33]

Like Russian efforts today, Soviet social manipulation is difficult to characterize because of the volume, secrecy, and mutually reinforcing nature of these operations. Soviet social manipulation used true, partially true, and/or false content in its efforts to influence. Some content was entirely manufactured by Soviet actors. In these cases, the Soviets fabricated false stories based on existing issues or grievances.[34]

To lend legitimacy and credibility to their contrived content, the Soviets produced and disseminated forgeries. Many forgeries were falsified U.S. government documents or fictitious statements by U.S. officials. In the 1950s and 1960s, Soviet forgeries were low-quality and frequently included rudimentary errors that were observable to journalists and other audiences. In some cases, as with the falsified statements attributed to then–Secretary of State John Foster Dulles in the late 1950s, the translations were poor.[35] Other forgeries demonstrated a lack of understanding of U.S. institutional practices and the official formats of government documents.[36]

---

[32] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 6.

[33] Kux, 1985, p. 19.

[34] Lawrence Britt, (pseudonym for Ladislav Bittman), testimony before U.S. Senate Subcommittee on Internal Security, Washington, D.C., May 5, 1971, p. 4, as referenced in Holland, 2006, p. 24.

[35] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, pp. 14–15.

[36] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980.

By 1980, the quality of forgeries improved, and they were "realistic enough to allow Soviets to plant them in the western non-communist media with a reasonable expectation that they will be considered genuine by all but the most skeptical of recipients."[37] In the 1970s, for instance, the Soviets produced a counterfeit top secret U.S. Army field manual, FM 30-31B, which was used as "proof" in the attempt to reinforce an existing Soviet allegation claiming the CIA was behind the assassination of Italian statesman Aldo Moro. The manual was used as evidence to deflect blame from a communist group, the Red Brigades, who had ties to the Soviet Union. An article surfacing this "evidence" was originally penned by an outlet with ties to the Soviets and was then picked up by the European press.[38]

In other cases, the content of Soviet social manipulation was truthful but was still used for propaganda purposes.[39] The Soviets leaked classified U.S. documents or sensitive information that they obtained through covert channels (as long as it no longer had intelligence value). The Soviets monitored the declassification of U.S. documents closely and used information from these documents as the genesis for new anti-American messaging. Declassified documents often revealed information that did not portray the United States in a positive light, which was particularly useful to the Soviets.[40]

Channels of Soviet Social Manipulation

Soviet social manipulation efforts relied on several dissemination avenues, including print media, radio programming, and books. The multichannel news outlet TASS was directly controlled by the government. TASS was believed to be under the policy control of three agencies—

---

[37] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 9.

[38] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, pp. 15–16, 66–67.

[39] U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, pp. 39–45.

[40] "Soviet Use of Declassified Documents," memorandum from A. Denis Clift to Secretary of State Henry Kissinger, National Security Council Files, President Gerald R. Ford Library, October 8, 1975.

the Agitation and Propaganda Section of the Party Control Committee, the Soviet Foreign Ministry, and the Main Administration for Affairs of Literature and Publishing. TASS operated both inside the Soviet Union and abroad.[41] As of 1986, TASS had offices in 126 countries.[42] TASS did not merely collect and report on the news, but performed other functions; it served as a cover for KGB agents abroad, as the conduit for directives from Moscow to local Soviet-affiliated organizations, and as a platform to disseminate Soviet propaganda.[43] While other Soviet state-owned newspapers—such as *Pravda, Izvestia, Novosti,* and *New Times*—were also circulated in the Soviet Union, their content was frequently published by TASS abroad.[44]

Soviet print content was also disseminated through proxies, such as affiliated Communist or friendly press organizations. However, the real objective of Soviet print efforts was often to gain circulation in the non-Communist press, as it offered greater legitimacy and credibility.[45] In some instances, the Soviets spent months or years courting foreign journalists at nonaffiliated press organizations. If these efforts were fruitful and the Soviets were successful in getting their stories printed in mainstream outlets, the Soviets would then reprint the stories in their own media in an effort to increase their exposure.[46] The Soviets also relied on repetition and misquoting Western sources as a means to bolster the authenticity of their messaging.[47]

Much like comment trolls today, Soviets used "letter brigades" to write fictitious letters to reputable newspapers expressing anger at anti-Communist stories and praise of stories that put Moscow in a

---

41 CIA, "TASS: Its Role, Structure, and Operations," June 1959, pp. 3–4.

42 CIA, "The Soviet Foreign Propaganda Apparatus: A Research Paper," 1986a, pp. iii.

43 CIA, *Political Information: The Role of TASS in Soviet Propaganda Activities, Shanghai*, Information Report, December 13, 1948; CIA, 1959, p. 6.

44 CIA, 1959, pp. 17–18.

45 Kux, 1985, p. 23.

46 Congressional Record, 1987, p. E4717; Holland, 2006, p. 4.

47 Kux, 1985, p. 25.

positive light.[48] The hope was that this would affect the policies of the newspaper editors who thought they should "keep in tune with their readers."[49]

Soviet-sponsored radio programming included overt and clandestine transmissions. Moscow ran two overt stations: Radio Moscow's International Service, which was openly affiliated with the government, and Radio Peace and Progress, which was considered an unofficial station. Radio Moscow's programming was broadcast in the local language of the target audience. A CIA memorandum describes Radio Moscow's foreign-language broadcasts as follows:

> The basic contents of Radio Moscow's international service programming to the Middle East and South Asia, as to any other region, consist of news, commentary and features dealing with a variety of Soviet domestic and international developments. Subjects range from political economic and trade affairs to science, culture, education, sports, and so forth. The primary purpose of Soviet media is to publicize Soviet achievements and convey the Soviet position on current international issues. . . . Broadcasts to specific target audiences may touch on topics which are not mentioned, or are selectively discussed in other foreign-language beams.[50]

Soviet-sponsored clandestine radio stations included National Voice of Iran and Radio Ba Yi in China.[51] Programming on clandestine stations tended to be more inflammatory than on Radio Moscow and served to agitate existing grievances, such as those against the People's Republic of China (on Radio Ba Yi).[52] Soviet newspapers, such as *Izvestia*, echoed and amplified the positions that were broadcast on the

---

[48] Suzanne Labin, "The Technique of Soviet Propaganda," presented to the Subcommittee to Investigate the Administration of the Internal Security Act and other Internal Security Laws, 86th U.S. Congress, 2nd Session, 1965.

[49] Labin, 1965.

[50] CIA, "Soviet Broadcasts to Middle East–South Asian Countries," February 4, 1980, p. 2.

[51] CIA, 1980.

[52] CIA, 1986a, p. 7.

clandestine radio programs.[53] This allowed "the radio to pose as the voice of the Soviet public opinion rather than of the government."[54]

Though government-sponsored books were exported in high volume, they were primarily used for internal political and cultural communication. Television played only a marginal role in external Soviet social manipulation efforts, even toward the end of the Cold War. While Soviet leadership recognized the virtues of television in reaching mass audiences and undertook efforts to improve the quality of Soviet broadcasting, it nevertheless suffered from several flaws: All its programming was in Russian, its quality remained lower than Western television content, and its reach was limited by technical issues.[55]

Historical Effectiveness of Soviet Social Manipulation

Measuring the effectiveness of these historical Soviet efforts is a complex task. During the Cold War, U.S. policymakers expressed their frustration at their inability to assess the success of Soviet efforts. As noted by Ohio Congressman John M. Ashbrook on the committee hearing discussing Soviet active measures: "We talk about all this covert activity, forgeries, etc., but then we get to the place where we say how successful they are, who they are influencing, where they are coming from, but when we get to this country, we draw a blank."[56] A 1986 CIA study concurred:

> We have no objective means for measuring the overall effectiveness of Soviet propaganda in influencing public thinking and policies abroad, but the huge investment the Soviet Union has made in its propaganda effort—in radio broadcasting, news agencies, publications, and cultural and information activities—

---

53 CIA, "Moscow Drops Clandestine Radio, Sustains Criticism of Tehran," *FBIS Trends* newsletter, December 10, 1986b.

54 CIA, 1980.

55 CIA, 1986a, pp. 9–10.

56 U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980.

attests to Moscow's high regard for propaganda instruments as political tools.[57]

The Soviet social manipulation apparatus had worldwide reach and was supported with significant resources. Rough estimates of Soviet expenditures on these efforts offer some insight into their magnitude.[58] A 1952 hearing before the subcommittee of the Committee on Foreign Relations in the United States indicated that "the Communists" were believed to be spending "in the neighborhood of $2 billion on their worldwide propaganda efforts."[59] In 1980, the CIA estimated that the Soviet Union spent approximately $3 billion on such programs.[60] That estimate was over $4 billion by 1987.[61] However, budget size may not always be a useful measure of effectiveness.

Some assert that Soviet social manipulation efforts were more effective in Third World states than in Western democracies, due to the West's stricter journalistic standards that rely on fact checking.[62] In a congressional hearing, a CIA representative noted that the most successful Soviet forgery was the falsified U.S. Army Field Manual 10-31B because the Soviets had "replayed it in many different countries, in fact in practically every continent in the world, and it was played in the press."[63] This suggests that success was in part construed as the

---

57 CIA, 1986a, pp. vi–vii.

58 It is important to note that these figures may include the active measures budget, which falls outside the scope of this report. Financial support to communist parties and fronts may have made up a larger portion of these budget expenditures. U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 7.

59 Overseas Information Programs of the United States, "Hearings Before a Subcommittee of the Committee on Foreign Relations of the United States," 82nd Congress, November 20–21, 1953, p. 777.

60 U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 7.

61 Congressional Record, 1987, p. E4716.

62 Kux, 1985, pp. 25–26; Oleg Kalugin, *Spymaster: My Thirty-Two Years in Intelligence and Espionage Against the West*, New York: Basic Books, 2009, p. 104.

63 U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, 1980, p. 21.

amount of press a story received. Others have argued that while Soviet social manipulation efforts did not change the tide of opinion against the United States, they were a distraction.[64] Still others have cited the mediocre quality of Soviet propaganda, issues with its timeliness due to internal bureaucratic and parochial hang-ups, and its lack of credibility as potential detractors from Soviet success.[65]

But the difficulty of measuring effectiveness goes both ways. A former CIA analyst responsible for U.S. covert action against the Soviet Union in the 1970s and 1980s told us that, when asked during budget discussions to justify *their* program's expenditures on such efforts, they were unable to provide a definitive answer. Whereas certain indicators showed that some in their target audience were reading stories planted by U.S. social manipulation efforts, there was ultimately no way to prove that their efforts were achieving the desired impact.[66]

Ultimately, the tide of opinion did not appear to shift largely in favor of the Soviet Union or its interests during the Cold War. Whether this is due to a lack of success of Soviet social manipulation efforts or to other factors is difficult to definitively assess.

Post-Soviet Approaches to Social Manipulation

Our research suggests that other factors may have shaped Russian social manipulation efforts since the collapse of the Soviet Union. One factor is U.S. political strategy, though the extent to which this has been an influence is debated.[67] A former Russian media editor told us that American political consultants and public relations experts have worked in Russia since the early 1990s, offering services to potential clients and exchanging ideas with Russian counterparts.[68] In 1995, Russians tied to President Boris Yeltsin secretly sought out the help of

---

64 Kalugin, 2009, p. 104.

65 CIA, 1986a, pp. v–vi.

66 In-person interview with former CIA analyst 024, November 20, 2017.

67 Phone interview with former journalist in Russian media, November 28, 2017; Andrew Wilson, *Virtual Politics: Faking Democracy in the Post-Soviet World*, New Haven, Conn.: Yale University Press, 2005, p. 50.

68 Phone interview with former Russian journalist 026, November 28, 2017.

U.S. consulting strategists Joe Shumate (an expert in political data), George Gorton (a strategist), and Richard Dresner (a political consultant) to advise the 1996 Yeltsin reelection campaign.[69] Before the election, Yeltsin's prospects of winning the campaign were uncertain, given that his ratings in the polls were "abysmal."[70]

The group of Americans worked in secrecy for several months. After overcoming initial opposition to their recommendations, the team reportedly helped Yeltsin execute an American-style campaign strategy, using focus groups to test narratives and likeability, using a "perception analyzer" to measure audience approval of certain topics by asking them to turn a dial, floating false poll predictions to drive voters to the polls, and placing negative attack ads on television.[71] Ultimately, Yeltsin won.

There have been competing assessments about the degree to which U.S. political strategists have influenced Russian conceptions of, and execution of, social manipulation—if any. Although one expert we spoke with cited their influence, other scholars have argued that U.S. involvement in Yeltsin's election was not as influential as some claim.

Andrew Wilson, who has closely examined the world of Russian political technologists—a group that specializes in "fixing," "black PR," *kompromat* gathering, and other dark arts—argues that this group was already well established by the 1996 Yeltsin campaign.[72] He suggests that the technologists have influenced current Russian social manipulation efforts in their own right.

The most well-known of this group, Gleb Pavlovsky, served as a technologist-for-hire in Russia and as an adviser to Putin for nearly two decades.[73] Pavlovsky appears to have been one of the first to demon-

---

[69] A former political strategist with whom we had discussions confirmed this, noting that the consultants recruited by Yeltsin's team were former colleagues (phone interview with former political consultant 028, December 5, 2017).

[70] Michael Kramer, "Rescuing Boris," *TIME*, July 15, 1996, pp. 29–37.

[71] Kramer, 1996, p. 36.

[72] Wilson, 2005, p. 50. *Kompromat* refers to information that is collected with the intent that it may be used to blackmail or embarrass its subjects.

[73] Wilson, 2005, pp. 54–55.

strate the virtues of the internet as a tool for manipulation and achieving political ends.[74] As Wilson notes, Pavlovsky was one among many such technologists operating in the post–Cold War era. Though he appears to have left the field, many others remain.

Another expert we spoke with offered an alternative view of the role of the American team aiding Yeltsin in 1996. The expert noted that this effort may have shaped Russian perceptions of U.S. intentions and methods; that while the American consultants likely viewed their efforts as the implementation of a typical campaign strategy, the view from Moscow was likely very different; and that the Russian intelligence services likely saw this effort as secret U.S. interference in a Russian election to engineer an outcome that was preferable to Washington.[75]

Others told us that Russian technology experts in the early post–Cold War years may have also influenced Russian thinking on social manipulation. Russian tech personalities, such as Igor Ashmanov, warned of the potential dangers posed by the internet, given its rise in the West.[76] Ashmanov appears to have had some influence with the Russian government; in 2010, the Kremlin consulted with his firm, Ashmanov and Partners, regarding the Kremlin's plans to build a Russian national search engine.[77]

When asked about the relationship between search engines and the state in 2010, Ashmanov noted, "U.S. authorities often say that Google is advancing the causes of democracy in China. How should the Chinese government view this? As an intervention in their affairs. That's exactly what they are doing. The U.S. government would be silly not to use it for America's own good."[78] In response to questions about Google's growing popularity in Russia, Ashmanov remarked that "a search engine is a means of influencing public opinion, and second, it's

---

74 Soldatov and Borogan, 2015, pp. 92–99; Wilson, 2005, pp. 54–55.

75 Phone interview with expert 030, January 15, 2018.

76 Phone interview with former Russian journalist and editor 026, November 28, 2017.

77 Evgeny Morozov, "Is Russia Google's Next Weak spot?" *Foreign Policy*, March 26, 2010.

78 Morozov, 2010.

a source of unique information about what people think and what kind of information they want."[79]

Lessons from the Second Chechen War also appear to have reinforced Russian suspicions of Western attempts to interfere in Russian domestic affairs using information, information technologies, or other mechanisms by which information is disseminated. Andrei Soldatov, a Russian investigative journalist, spoke of these suspicions in a recent interview:

> People in the Kremlin sincerely believed that we lost the First Chechen War because of journalists. They spoke of this very clearly and very openly that it was because of journalists and foreign media; and they actually, they forced us to lose and to stop the war . . . they believed that the biggest challenge, the biggest threat to the Kremlin, was supposedly by the [National Security Administration] trying to penetrate Russian government communications.[80]

Doctrine: Russia's Conceptualization of Social Manipulation

Many of the tactics and techniques of the Soviet era have flowed directly into Russian practices today. These include an embrace of the general practice of propaganda and efforts to control narratives, manufacturing partly true material or outright falsehoods; efforts to reach into other societies with targeted appeals; and conscious attempts to shape political outcomes abroad. The way Russia is able to undertake these campaigns, however, has evolved significantly under the influence of new technologies.

---

[79] Morozov, 2010.

[80] Michael Kirk, interview of Andrei Soldatov, "The Putin Files," *Frontline*, PBS, July 25, 2017b; this point was reinforced in our discussion with a Russian expert 030, January 15, 2017.

This section will discuss the Russian conceptualization of social manipulation, drawing on publicly available doctrine, academic literature and statements, and expert assessments. Russian government documents detailing offensive information warfare or social manipulation are likely classified. The publicly available documents largely speak of social manipulation in the context of broader national security and refer to social manipulation efforts in a defensive context. Nevertheless, these documents can offer relevant insight into Russian thought on these issues and into Russian perceptions of external social manipulation as a threat. Though this chapter focuses on Russian social manipulation efforts outside of outright military conflict, Russian military documents are nevertheless relevant as the Russian approach to social manipulation appears to be less partitioned than that of the West. From an assessment of publicly available sources since 2000, three key themes emerge.

1. Russia Sees Information Warfare as a Critical Threat to Its National Security

Russia has long viewed the information space as a threat. In 2000, the "National Security Concept of the Russian Federation" described the threat to Russia from the information sphere:

> There is an increasing threat to national security in the information sphere. The striving of a number of countries to dominate the global information space and oust Russia from the external and internal information market poses a serious danger, as [does] the elaboration by a number of states of a concept of information wars that envisages creation of means of dangerous influence on the information spheres of other countries of the world; disruption of the normal functioning of information and telecommunication systems and of storage reliability for information resources; and gaining of unsanctioned access to them. [81]

[81] Ministry of Foreign Affairs of the Russian Federation, "National Security Concept of the Russian Federation," January 10, 2000.

Russia appears to have believed that it was lagging behind other states in its capabilities in the information space and was therefore under threat. The 2000 doctrine calls out the practice of information warfare by other unnamed countries and specifies the following tasks for the Russian state as necessary to ensure its information security:

- "realization of the constitutional rights and freedoms of the citizens of the Russian Federation in the sphere of information activities"
- "improvement and protection of the national information infrastructure and the integration of Russia into the world information space"
- "counteraction against the threat of rivalry in the information sphere."[82]

As reflected in the Information Security Doctrine, also published in 2000, the public focus of national security and strategy documents with regard to the information space was on securing Russia from attack and influence from the outside. The emphasis in this document was on protecting technical means and physical hardware and infrastructure, with only an occasional reference to information warfare, and the document barely makes reference to the internet.

Russia's 2014 Military Doctrine document continues in this vein, describing growing global competition and tension: "There is a tendency towards shifting the military risks and military threats to the information space and the internal sphere of the Russian Federation."[83] The document distinguishes between external and internal military risks. It declares one of the main external military risks to be the "use of information and communication technologies for the military-political purposes to take actions which run counter to international law, being aimed against sovereignty, political independence, territorial integrity of states and posing threat to the international peace, security, global

[82] Ministry of Foreign Affairs of the Russian Federation, 2000.

[83] Russian Federation, "Military Doctrine of the Russian Federation," December 26, 2014.

and regional stability."[84] The document declares one of the main internal military risks to be "subversive information activities against the population, especially young citizens of the State, aimed at undermining historical, spiritual and patriotic traditions related to the defense of the Motherland."[85]

In 2016, the "Doctrine of Information Security" continued to stress the threat from the outside:

> The possibilities of transboundary information circulation are increasingly used for geopolitical goals, goals of a military-political nature contravening international law or for terrorist, extremist, criminal and other unlawful ends detrimental for international security and strategic stability. . . . One of the key negative factors affecting the state of information security is the fact that a number of foreign countries are building up their information technology capacities to influence the information infrastructure in pursuing military purposes.[86]

It goes on to say,

> Information security in the sphere of national defense is characterized by the growing use by certain States and organizations of information technologies for military and political purposes, including for actions inconsistent with international law and seek to undermine the sovereignty, political and social stability and territorial integrity of the Russian Federation and its allies, and pose a threat to international peace, global and regional security.[87]

The 2016 doctrine formalized the idea of "protecting the information sovereignty of the Russian Federation," a key part of Russian

---

84 Russian Federation, 2014.

85 Russian Federation, 2014.

86 Ministry of Foreign Affairs of the Russian Federation, "Doctrine of Information Security of the Russian Federation," December 5, 2016.

87 Ministry of Foreign Affairs of the Russian Federation, 2016.

national security strategy.[88] However, from this self-described position of lagging behind others in the early 2000s, Russian thinking, doctrine, and practice have rapidly evolved. Russia has begun to reinvest in its offensive information capabilities and has deployed and refined them operationally in conflict, first in Chechnya and then in Georgia and Ukraine.

2. The Russian Concept of Information Warfare Is Holistic and Integrated

As we have noted, there is no Russian equivalent of the term *social manipulation* in publicly available Russian doctrine or relevant literature; instead, Russia uses the term *information warfare* (*informatsionnaya voyna*).[89] As Keir Giles notes, *information war* is a "broad and inclusive concept covering a wide range of different activities. It covers hostile activities using information as a tool, or a target, or a domain of operations."[90]

The Russian concept of information warfare is far broader than any equivalent concept found in Western military or national security literature.[91] From the Russian perspective, information warfare is all-encompassing; covers the widest range of activities; crosses organizational, technical, and personnel boundaries; and is conducted at the tactical, operational, and strategic levels.[92] This integrated and holistic view is reflected in Russian national security documents, which all conceptualize the information space in concert with the other tools of state power.[93] Journalists and analysts Alexey Kovalev and Matthew

---

88 Ministry of Foreign Affairs of the Russian Federation, 2016.

89 Giles, 2016, p. 6. This publication offers one of the most comprehensive and authoritative accounts of Russian information warfare.

90 Giles, 2016, p. 6.

91 Dimitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," Proliferation Papers No. 54, Security Studies Center, Institut Francais des Relations Internationales, November 2015, p. 29.

92 Giles, 2016, p. 6.

93 Though Russian thinking conceives of information warfare (social manipulation) as an all-encompassing coordinated range of activities, this does not necessarily mean this is how

Bodner contrast the Western and Russian approaches: "Things we tend to compartmentalize (and label with weasel expressions such as 'strategic communications') are to the Russians all part of one seamless domain relating to the human, morale-and-will side of warfare."[94]

Importantly, in contrast with the West, Russia does not appear to separate or differentiate cyberspace from information warfare. To Russia, cyberspace is integral to information operations and is viewed as a means of transmission, rather than a separate sphere.[95]

By 2011, Russian thinking and doctrine on information warfare had developed significantly. The 2011 Russian Federation Armed Forces' Information Space Activities Concept defined information warfare as follows:

> the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force.[96]

While this is a military concept, it demonstrates the breadth of the Russian definition of information warfare, encompassing the "massive psychological manipulation of the population to destabilize the state and society."[97] This definition goes well beyond what the Russian military alone could be expected to deliver and demonstrates how the military is seen as fitting into a much wider range of actions and agencies of the Russian state. The 2011 doctrine defines the information

---

these efforts operate in practice.

[94] Alexy Kovalev and Matthew Bodner, "The Secrets of Russia's Propaganda War, Revealed," *Moscow Times*, March 1, 2017.

[95] Giles, 2016, p. 9.

[96] Ministry of Defense of the Russian Federation, "Russian Federation Armed Forces' Information Space Activities Concept, 2011," January 2012.

[97] Ministry of Defense of the Russian Federation, 2012.

space as including "a scope of activities associated with the formation, creation, transformation, transmission, usage, storage of information which influences the individual and community awareness, information infrastructure and information itself."[98] Though mostly defensive, the doctrine sets few parameters on the reach of the information space: "Hundreds of millions of people (whole countries and continents) are involved in a single global information space formed by the Internet, electronic mass media and mobile communication systems."[99]

Similarly, the 2014 "Military Doctrine" characterizes current military conflicts as the "integrated employment of military force and political, economic, informational or other non-military measures implemented with a wide use of the protest potential of the population and of special operations forces."[100] Polina Sinovets and Bettina Renz highlight the fact that the 2014 doctrine includes a list of domestic threats to Russia as well as singling out the information space in a way that had not been done before.[101]

The 2016 "Doctrine of Information Security" brings the concepts up to date with the growing importance of the internet. The doctrine revises the definition of the *information sphere*:

> a combination of information, informatization [sic] objects, information systems and websites within the information and telecommunications network of the Internet (hereinafter referred to as the "Internet"), communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere.[102]

---

98 Ministry of Defense of the Russian Federation, 2012.

99 Ministry of Defense of the Russian Federation, 2012.

100 Russian Federation, 2014.

101 Polina Sinovets and Bettina Renz, "Russia's 2014 Military Doctrine and Beyond, Threat Perceptions, Capabilities and Ambitions," Research Paper No. 117, Research Division, NATO Defense College, July 2015, p. 2.

102 Ministry of Foreign Affairs of the Russian Federation, 2016.

Once again, the 2016 doctrine is largely domestic and defensive in nature. Nonetheless, it also recognizes the free flow of information across boundaries and notes that information technologies "are now an integral part of all areas of activity of the individual, society and the State."[103] Interestingly, the document conceptualizes the use of information technologies for the "preservation of cultural, historical, spiritual, and moral values" and warns of the "growing information pressure on the population of Russia, primarily on the Russian youth, with the aim to erode Russian traditional spiritual and moral values."[104]

In Russian doctrine, information warfare (social manipulation) is conceived of as being integrated into the other tools of power. When speaking of the new information forces established in 2017, Vladimir Shamanov, head of the State Duma's defense committee, said simply: "Information conflict is part of general conflict."[105]

3. The Information Struggle Is Perpetual, Conducted in Both War and Peace

For Russia, information warfare appears to be perpetual, part of the ongoing contest between nations and societies, which Russia rationalizes is a natural part of the international system. Published in 2009, the "National Security Strategy of the Russian Federation to 2020" warns that "the global information struggle will intensify."[106] Throughout the document, *information* and its synonyms are referenced as part of a range of potential threats and possible responses. This conceptualization demonstrates how Russia has, from an early stage, thought of information, both offensively and defensively, as a broad and integral part of security strategy. The 2015 "National Security Strategy" and 2016 "Foreign Policy Concept" reiterate the theme of the international system as a struggle between countries and the somewhat pessimistic

---

[103] Ministry of Foreign Affairs of the Russian Federation, 2016.

[104] Ministry of Foreign Affairs of the Russian Federation, 2016.

[105] Kovalev and Bodner, 2017.

[106] Russian Federation, "National Security Strategy of the Russian Federation to 2020," Publication No. 537, May 12, 2009.

assessment of rising tensions. Recent Russian military thinking further reinforces this point:

> In peacetime, information operations must be maintained to achieve objectives set by the country's political leaders in an effort to enhance the effectiveness of political, diplomatic, economic, judiciary, and military measures to maintain the security of the Russian Federation.[107]

These documents suggest that information warfare is to be conducted continuously in war and peace—the only difference being the tools employed.[108] Russian military literature outlines two types of information warfare: *information-psychological warfare*, focused on the armed forces and the population of an adversary; and *information-technology warfare*, focused on adversary technical systems.[109] The former is conducted consistently, and the latter is conducted during conflict and is one of the core missions of Russian special forces.

These three elements of the Russian conceptualization of information warfare—the belief in information warfare as a critical external threat, the holistic and integrated nature of information warfare, and the necessity for perpetual information warfare to fight an ongoing international battle—guide Russian actions in pursuit of social manipulation. Rightly or wrongly, Russia appears to believe it is permanently under threat from external social manipulation efforts.[110]

It is important to underscore the incongruities in the conceptualization of social manipulation between Russia and the West, as they

---

[107] Kh. I. Sayfetdinov, "Information Operations on the Battlefield," *Military Thought*, Vol. 3, 2014, p. 74.

[108] Phone interview with expert 030, January 15, 2017. For a discussion of the "uninterrupted" nature of information warfare in Russian military thinking, see Adamsky, 2015, p. 29.

[109] Giles, 2016, p. 9; Adamsky, 2015, p. 27.

[110] Interviews with Department of State official 101, October 4, 2017; phone interview with expert 030, January 15, 2018; phone interview with former military information activities specialist 022, November 2, 2017; in-person interview with former CIA analyst 024, November 20, 2017.

could affect attempts to understand and counter Russian efforts. Viewing Russian efforts through a Western lens could lead to erroneous conclusions.

Objectives of Russian Social Manipulation

A discussion of Soviet objectives, excerpted from a 1980 U.S. congressional report on Soviet active measures in the United States, could easily apply to Russian social manipulation efforts targeting the United States and others today:

> The Soviet leadership in Moscow takes a long-term view of its active measures operations directed at the United States. Through these operations the Soviets attempt to: directly influence the policies and actions of the U.S. government; undermine public confidence in U.S. leaders and institutions; influence public opinion against certain U.S. military, economic, and political programs; disrupt relations between the United States and its allies; and demonstrate that the policies and goals of the United States are incompatible with the growth of developing nations.[111]

The exact policy ends to which Russian social manipulation efforts are directed are difficult to know with any certainty. As one former intelligence officer said to us, one can only speculate as to what Russia is trying to achieve unless a defector or source who is privy to Russian government decisions and directions can provide the information or documentation.[112] That said, a number of useful deductions can be made from Russian actions and statements.

Because Russia appears to believe it is the target of offensive social manipulation at the hands of the West, Moscow views its use of social manipulation externally as defensive in nature. Consequently, one possible strategic objective is simply to counter the perceived offensive efforts.

A second possible objective is to use social manipulation to pursue discrete policy objectives at specific moments in time, such as influ-

---

[111] Congressional Record, 1987, p. E4717.

[112] In-person interview with former CIA analyst 024, November 20, 2017.

encing a vote, a policy debate, or a policy outcome in a target state, in ways that advance Russian interests. This could translate to efforts intended to engender support for policymakers or policies that endorse the removal of sanctions on Russia, or are supportive of Russian economic projects or political aspirations.

Russia analyst Andrew Monaghan describes Russia's strategic thinking as a "dialogue" between the current context and the immediate future.[113] This could be a useful way of understanding this possible objective of Russian social manipulation: to adapt easily and iteratively, responding to events as they unfold and to failures or successes on the ground. There is also an experimental quality to social manipulation, and so this second possible objective could complement any others. Given how much modern technology has transformed what is possible, Russian efforts are likely evolving and changing rapidly in response to events, to new tactics and techniques, and to lessons learned about what works.

A third possible objective is more opaque. Several interviewees suggested that some Russian efforts are not intended to influence the outcome of any discrete end, but rather to discredit its target or to agitate the target's existing domestic anxieties more broadly.[114] Neither Russian doctrinal nor policymaking documents state this as an explicit objective. Yet organizations reportedly affiliated with the Russian government—such as St. Petersburg's now notorious internet troll factory, the Internet Research Agency (IRA)—have articulated this as an objective.[115]

The 2018 indictment filed by the U.S. government against the IRA cites "spread[ing] distrust towards the candidates and political

---

[113] Andrew Monaghan, *The New Politics of Russia*, Manchester, UK: Manchester University Press, 2016.

[114] Phone interview with expert 030, January 15, 2018; phone interview with former military information activities specialist 022, November 2, 2017.

[115] "An Ex St. Petersburg 'Troll' Speaks Out: Russian Independent TV Network Interviews Former Troll at the Internet Research Agency," *Meduza*, October 15, 2017.

system in general" as a declared goal of the organization.[116] Some IRA behavior appears to confirm this goal. Several days after the U.S. election, IRA-sponsored groups organized rallies both supporting and denouncing President Trump's victory.[117] These efforts to reinforce both sides of the political debate suggest the organization was attempting to magnify conflicting views over the election outcome rather than to support a specific policy aim.

Accounts from a former employee of the IRA appear to verify this impression. He claimed to work for the organization's "foreign desk." He said his role was to "set Americans against their own government: to provoke unrest and discontent [and] . . . to rock the boat ."[118] Nevertheless, this is but one example. As will be discussed below, other campaigns associated with the IRA appear to be directed at supporting discrete ends such as supporting a specific candidate or one side of a policy debate.

Social manipulation may also serve a grander strategic goal related to Russia's power, position, and prestige on the world stage—that of being considered a world power and having a role in decisionmaking on global issues. Some have noted that sowing discord and undermining trust and faith in institutions and alliances externally serve to weaken those outside institutions and alliances so that Russia can deal with countries on a bilateral basis, thereby bolstering its own position.[119] Again, history is instructive. According to Max Holland, who has written about Communist disinformation, "The purpose of such measures was unitary: to weaken the military, economic, and psychological cli-

---

[116] U.S. District Court for the District of Columbia, "United States of America v. Internet Research Agency LLC, [et. al]," filed February 16, 2018, pp. 4, 17l; Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community assessment, January 6, 2017, p. 6. The IRA has been registered under many names since its inception (refer to p. 7 of the 2018 indictment for a full list). This chapter will refer to the organization as the IRA, given that this is the moniker most commonly used in public discourse.

[117] "United States of America v. Internet Research Agency LLC, [et. al]," p. 23.

[118] "An Ex St. Petersburg 'Troll' Speaks Out: Russian Independent TV Network Interviews Former Troll at the Internet Research Agency," 2017.

[119] In-person interview with European Defense Official 020, October 26, 2017.

mate in the West, and by doing so, to strengthen the Soviet Union in what was perceived as a zero-sum game on a global scale."[120] However, because this objective is not known to be explicitly stated in doctrine, it remains, at least for now, to be an inferred hypothesis of an objective.

Some analysts studying this issue argue that another of Moscow's ambitions is to drive society toward a "posttruth" environment—one in which the distinction between fact and falsehood is immaterial, objectivity is unattainable, and reality is malleable. Others question whether this is an end in itself for the Kremlin, or whether it is instead a potential means to other ends.

Journalist and Russia hand Peter Pomerantsev asserts that the dizzying array of explanations for the downing of MH-17 propagated by Kremlin-linked actors was not intended to "convince viewers of any one version of events, but rather to leave [audiences] confused, paranoid, and passive—living in a Kremlin-controlled virtual reality that can no longer be mediated or debated by any appeal to 'truth.'"[121] If, in this case, Russia had intended to perplex and pacify audiences, the question remains whether this was the ultimate objective of these efforts.

While Russia may not have tried to *convince* its target audience of the legitimacy of any *one* narrative, as Pomerantsev argues, it is plausible that the Kremlin sought to *avert* audiences from *one* specific narrative: its involvement in the MH-17 incident and the Ukraine crisis more broadly. Thus, its efforts to saturate public discourse with competing and often contradictory explanations for the tragedy may have been a means to more specific foreign policy ends. It may have sought to obscure its connection to the incident to prevent further tarnishing to its image in the eyes of eastern Ukrainian, regional, and global audiences, and to preserve its influence in the region.

This is to say that it is possible that Russia seeks a postfactual reality and uses social manipulation efforts in an effort to achieve this end. It is also possible that Russian social manipulation efforts employ this instrument to achieve other, specific objectives.

---

[120] Holland, 2006, p. 3.

[121] Peter Pomerantsev, "Russia and the Menace of Unreality," *The Atlantic*, September 9, 2014.

Strategies: How Russia Conducts Social Manipulation Today

Most likely, the identities of those who plan and execute Russia's social manipulation efforts are deliberately concealed and are therefore hard to reveal using entirely open-source material. Those who are visible, or who have become visible, such as the troll farms, are not necessarily the most important of the Russian state-sponsored entities engaged in social manipulation. Some have argued that troll farms serve a secondary function as a distraction for Western journalists and analysts.[122] The farms could divert attention from other entities and activities that are harder to uncover.[123] These organizations still matter. In the view of one Moscow journalist we interviewed, the IRA is likely part of a much larger system, much of which may be unknown in the unclassified setting.[124]

While this chapter examines Russian social manipulation efforts overseas, the domestic Russian information landscape matters, as the two are inextricably linked.[125] This is also the case with the perception of domestic and foreign threats more broadly in the eyes of the Kremlin leadership.[126] Just as Russia conceives of information warfare holistically, according to one interviewee, disinformation and social manipulation strategies outside and inside Russia cannot be separated.[127] The Russian government seeks to protect itself and the survival of the regime through the domestic information space, as it has

---

[122] Phone interview with expert 030, January 15, 2018; Adrian Chen, "The Agency," *New York Times Magazine*, June 2, 2015.

[123] Keir Giles, "Indicators and Warnings for Detecting Information Threats," YouTube video of remarks at the Riga StratCom Dialogue: Perception Matters, NATO Stratcom Center of Excellence, Riga, Latvia, August 20–21, 2015; phone interview with expert 030, January 15, 2018.

[124] Phone interview with Moscow correspondent 014, October 4, 2017.

[125] Nearly every one of our interview subjects reinforced the interconnected nature of this system.

[126] Andrew Radin and Clint Reach, *Russian Views of the International Order*, Santa Monica, Calif.: RAND Corporation, RR-1826-OSD, 2017, p. 9.

[127] Phone interview with Moscow correspondent 014, October 4, 2017.

felt under threat from information from abroad.[128] The Russian government describes this priority as "securing of the national information space against breaches."[129] The Russian defense appears to consist of a well-established network of state and private entities engaging in a wide range of activities.

Actors: Centralized Direction Versus Freedom of Action

Although Russian social manipulation strategies are often described as the decisions and outputs of a monolithic and hierarchical structure, evidence suggests that strategies instead appear to be designed and executed by a complex web of state and nonstate actors. These seem to include Kremlin officials, members of the state security services, private entities, individuals unaffiliated with but distantly tied to the Russian state, and others. It is, therefore, unlikely that all strategic decisions are determined by a central authority. Some decisions may originate from the highest levels at the Kremlin, whereas others may be motivated by parochial interests and even competition among Russian state actors vying for control or prestige.[130]

Other self-motivated actors could be inspired to pursue social manipulation strategies in the hopes of financial gain, or for love of country. Still others may be unaware they are pursuing strategies on behalf of Moscow. Not all of the actors operate within Russia. Some external organizations—such as WikiLeaks, which has been called a "tool of Russian intelligence" and a "hostile intelligence service" by U.S. officials—serve as proxies.[131]

The centralized yet entrepreneurial nature of the system affords plausible deniability and a buffer between government officials and more unorthodox activities or entrepreneurial types. One interviewee

---

[128] Phone interview with expert 030, January 15, 2018.

[129] Giles, 2015.

[130] In-person interview with Department of State official 010, October 4, 2017; Angela Charlton and Matthew Bodner, "Russian Meddling Abroad: Does Putin Pull All the Strings?" Associated Press, September 15, 2018.

[131] Kathryn Watson, "How Did WikiLeaks Become Associated with Russia?" CBS News, November 15, 2017; Office of the Director of National Intelligence, 2017.

suggested that this hybrid system of public and private, and of directed and entrepreneurial efforts, has evolved organically over time rather than by design.[132]

The exact balance between centralized direction and freedom of action is very difficult to determine, and neither the literature nor interviewees agreed on the matter. According to one interviewee, Russian actors conducting influence efforts and information operations are highly entrepreneurial and decentralized, while others suggested that a greater degree of control and direction exists.[133]

Putin's role is also debated. It is common in Western literature to assign direction and control of Russian social manipulation strategies to him personally. The 2017 U.S. intelligence community report on Russian interference in the 2016 U.S. elections explicitly identifies Putin as the deciding authority in this case: "We assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election."[134] We assume the U.S. intelligence community has come to this conclusion based on concrete evidence demonstrating Putin's role—evidence that is unavailable to the public. In other cases of alleged Russian social manipulation, Putin's role is largely a mystery.

Putin may decide on certain strategic actions, but excessive personalization can occlude the wider network of government officials, decisionmakers, and entrepreneurs potentially operating in the social manipulation space.[135] It can also underestimate the amount of competition for attention, funding, and perceived success among both state agencies and private entities.

According to interviewees, the competition among state and private entities is intense and leads to freelancing and entrepreneurship, which has not been centrally directed.[136] These actors may float a nar-

---

[132] Phone interview with Moscow correspondent 014, October 7, 2017.

[133] In-person interview with Department of State official 010, October 4, 2017.

[134] Office of the Director of National Intelligence, 2017, p. 1.

[135] In-person interview with Department of State official 010, October 4, 2017.

[136] In-person interview with Department of State official 010, October 4, 2017.

rative, in line with broader Kremlin messaging, and then ask their government contacts whether to promote this narrative further.[137] In an interview, Pavlovsky underscored the self-motivated nature of some Russian social manipulation efforts.[138] One Moscow correspondent we spoke with noted that, given the disaggregated nature of the system, it is possible that the Russian state may not have the ability to rein in certain elements.[139] Thus, it is difficult to definitively characterize Putin's role in the Russian social manipulation system based on the publicly available evidence.

Several of those we spoke with, particularly those who had worked in Russian media and interacted with individuals working for parts of the state apparatus like RT, said that many of those who pursue social manipulation strategies are not "true believers" in the narratives they produce and disseminate, while others are.[140]

Targets and Target Audiences

Without access to classified documents or senior officials, it is difficult to identify which actors the Russian government seeks to discredit (its targets) and which audiences it seeks to influence (its target audiences).[141] That said, one can draw limited inferences about the targets and target audiences based on the languages efforts are conducted in, the locations these efforts target, and the narratives they use. Given the attribution challenges discussed, it is important to note that this approach has limitations.

Analyses of the predominant narratives and messages of Russian social manipulation efforts suggest that Western states, institutions,

---

[137] In-person interview with Department of State official 010, October 4, 2017.

[138] Michael Kirk, interview of Gleb Pavlovsky, former adviser to Vladimir Putin, "The Putin Files," *Frontline*, PBS, July 13, 2017a.

[139] Phone interview with Moscow correspondent 014.

[140] In-person interview with Department of State official 010, October 4, 2017; phone interview with Russian journalist 027, December 4, 2017.

[141] The Russian government's targets and target audiences may not be one and the same.

and officials are Moscow's principal targets.[142] These include the European Union (EU), North Atlantic Treaty Organization (NATO), Western European states, the United States, and the individuals who represent these bodies. Ukraine has also been the target of Russian efforts; the authorities in Kyiv who came to power following the 2014 Ukrainian Revolution have been accused of supporting fascist elements, and Ukrainian soldiers have been accused of barbaric crimes.[143] However, even in these instances, the West is often indirectly implicated.

Of the known actors believed to be responsible for Russian social manipulation strategies, two are overtly affiliated with the Russian government: RT (formerly Russia Today) and Sputnik News. Given their acknowledged relationship with the government, analysis of their target audiences is instructive. RT is a news organization comprising eight television channels, digital platforms in six languages, and a robust social media presence. Its television programming is available in over 100 countries in English, Arabic, Spanish, and French. Its documentary channel is available in English and Russian, and its digital platforms are available in German, French, English, Arabic, Spanish, and Russian.[144] Sputnik News operates a news agency, websites, and a

---

[142] Martin Kragh and Sebastian Asberg, "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies*, Vol. 40, No. 6, 2017, pp. 782–784; Stephen Hutchings and Joanna Szostek, "Dominant Narratives in Russian Political and Media Discourse During the Ukraine Crisis," in Agnieska Pikulicksa-Wilczewska and Richard Sakwa, eds., *Ukraine and Russia: People, Politics, Propaganda, and Perspectives*, Bristol, UK: E-International Relations Publishing, 2015, pp. 174–178; Maria Hellman and Charlotte Wagnsson, "How Can European States Respond to Russian Information Warfare? An Analytical Framework," *European Security*, Vol. 26, No. 2, 2017, pp. 156–157.

[143] Mark Galeotti, "'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't," in Agnieska Pikulicksa-Wilczewska and Richard Sakwa, eds., *Ukraine and Russia: People, Politics, Propaganda, and Perspectives*, Bristol, UK: E-International Relations Publishing, 2015, pp. 153–154; Anton Shekhovtsov, "Pro-Russian Network Behind the Anti-Ukrainian Defamation Campaign," blog post, Anton Skekhovtsov's Blog, February 3, 2014; Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, New York: The Interpreter, Institute of Modern Russia, 2014, pp. 10–11; Alina Polyakova, "Russia Can't Decide If Ukrainian Jews Are Victims or Villains," *New Republic*, April 28, 2014.

[144] RT, *About RT*, webpage, undated(a).

radio broadcast service.[145] With its headquarters in Moscow, the agency has offices in the United States, China, France, Germany, Egypt, and the United Kingdom. At least some of its content is available in over 30 languages.[146] The office locations and chosen languages indicate that the corresponding populations are likely Russia's target audiences. At the same time, Russian social manipulation strategies likely extend well beyond RT and Sputnik target audiences.

The Russian government has been associated with many social manipulation strategies throughout Western, Central, Eastern, Northern, and Southern Europe, as well as North America and South America. However, confirming the Kremlin's direct sponsorship of these efforts is challenging, given the purposeful concealment of sponsorship in many cases.

Russian messaging also appears to target specific populations within states; populations that exhibit frustrations with economic, political, social, or cultural grievances. The Facebook and Instagram ads purchased by the IRA during the 2016 U.S. presidential election demonstrate this type of targeting.[147] The ads focus on gun control, border security, racial tensions, anti-Islamic sentiment, immigration, and the candidates—all polarizing issues at the time. A former employee of the IRA substantiated this targeted approach: "People in his department . . . were even trained and educated to know the nuances of American social polemics on tax issues, LGBT rights, the gun debate, and more."[148] The advertising metadata released by the U.S. House Permanent Select Committee on Intelligence show that those purchasing

---

[145] Sputnik, *About Us*, webpage, undated.

[146] These languages include Abkhazian, Arabic, Armenian, Azerbaijani, Belarusian, Brazilian Portuguese, Chinese, Czech, Danish, Dari, English, Estonian, Finnish, French, Georgian, German, Hindi, Italian, Japanese, Korean, Kurdish, Kyrgyz, Latvian, Lithuanian, Moldavian, Norwegian, Ossetian, Pashto, Persian, Polish, Russian, Serbian, Spanish, Swedish, Tajik, Turkish, Urdu, Uzbek and Vietnamese (Wikipedia, "Sputnik [news agency]," article, 2018).

[147] Scott Shane, "These Are the Ads Russia Bought on Facebook in 2016," *New York Times*, November 1, 2017b.

[148] "An Ex St. Petersburg 'Troll' Speaks Out: Russian Independent TV Network Interviews Former Troll at the Internet Research Agency," 2017.

the ads selected specific audience criteria for each ad—criteria such as age, gender, language(s), interests, and behaviors.[149] This is to say that the IRA targeted audiences with specific beliefs about issues relevant to the campaign by crafting messaging that appealed to their existing views, and by using the platform's tools to direct messaging at niche populations.

For instance, one of these ads, which was allegedly sponsored by the organization called "Secured Borders," prompts users to join the group with an image of a yellow sign reading "no invaders allowed" placed against the backdrop of a high fence.[150] The text, "Every man should stand for our borders! Join!" sits atop the image. The corresponding metadata show that its sponsors selected ad criteria to target users between the ages of 18 and 85, in the United States, who had "Conservatism," "Confederate States of America," "Donald Trump," "Republican Party (United States), or "Dixie" listed as interests on their Facebook accounts.[151]

Other ads targeted audiences in specific U.S. geographic locations.[152] According to the 2018 U.S. indictment of Russian players in these strategies, IRA employees traveled to specific U.S. states to collect intelligence prior to the organization's campaign. Advice provided by an unwitting, legitimate, Texas-based grassroots organization sug-

---

[149] The Facebook advertisements and corresponding metadata represent only a small sample (30 ads) of the overall corpus of ads reportedly purchased by Russia (3,300 ads). It is unclear whether the content of the ads and metadata of the sample that were released is representative of the full corpus. The metadata can be found here: U.S. House of Representatives Permanent Select Committee on Intelligence, "HSPCI Minority Open Hearing Exhibits," webpage, undated. Note that the ability to target specific audiences using demographic criteria is an option available to all who advertise through Facebook.

[150] "Secured Borders Ad_Cultural _Metadata 1," U.S. House of Representatives Permanent Select Committee on Intelligence, 2017; Taylor Hatmaker, "Here's How Russia Targeted Its Fake Facebook Ads and How Those Ads Performed," *Tech Crunch*, November 1, 2017.

[151] "Secured Borders Ad_Cultural _Metadata 1," 2017.

[152] "BM Not My President Rally," Twitter post, U.S. House of Representatives Permanent Select Committee on Intelligence, 2017; Hatmaker, 2017.

gested that the IRA focus its efforts on "purple states like Colorado, Virginia & [sic] Florida."[153]

Likewise, an analysis of 36,000 tweets promulgated by the 2,752 Russian-affiliated Twitter accounts during the 2016 U.S. presidential election found that the accounts appear to have focused on amplifying stories published by local U.S. news outlets, such as Cleveland Live and KSN Topeka.[154] Some names of the Russian-affiliated accounts—DailyNewsDenver, DallasTopNews, TodayMiami, StLouisOnline, Seattle_Post—suggest they were intended to impersonate local news outlets.[155] The falsified news accounts also "showed a pattern of systematically re-broadcasting local news outlets' stories," reinforcing the assertion that Russian efforts during the election campaign were likely focused on geographic target audiences.[156]

RT's programming on YouTube offers another example of targeting. RT draws viewers with human interest stories and offers content on local issues by region. For instance, RT Arabic's YouTube channel

> focuses on regional news on some channels to build credibility. In order to get viewers to believe their extremely biased coverage of issues like Ukraine, RT must build credibility and provide a legitimate "second opinion," at least some of the time. Accordingly, the vast majority of the coverage in the RT Arabic channel is devoted to Middle East issues.[157]

---

153 "United States of America v. Internet Research Agency LLC, [et. al]," p. 13.

154 Jonathan Albright, "Trolls on Twitter: How Mainstream and Local News Outlets Were Used to Drive a Polarized News Agenda," Berkman Klein Center for Internet and Society at Harvard University, February 15, 2018. The U.S. Congress released the full list of Twitter accounts linked to Russia (according to Twitter) that were reportedly actively targeting the U.S. audience during the 2016 presidential election; it can be found on the U.S. House of Representatives Permanent Select Committee on Intelligence–Democrats website.

155 "Exhibit B," U.S. House of Representatives Permanent Select Committee on Intelligence, 2017.

156 Albright, 2018.

157 Elizabeth Nelson, Robert Orttung, and Anthony Livshen, "Measuring RT's Impact on YouTube," *Russian Analytical Digest*, December 2016, pp. 5–6.

Not only does RT report pro-Russian narratives of political content, but it also covers issues that other outlets downplay, such as Venezuela or the Occupy Wall Street movement.[158] According to a 2015 study analyzing the content of RTs YouTube videos over time, RT covers some events objectively and others that highlight Russia's political views or distort reality in some way.[159]

A major focus of these efforts is to reach specific politically active groups in the United States, such as extremist groups (including white supremacist organizations), groups organized around conspiracy theories, misogynistic and hate speech–oriented trolls in corners of the "dark web," and other gatherings of radicalized individuals. There is significant evidence in the pattern of Russian social media activities that Russia aimed to distribute material that would appeal to and energize such groups, and that it aimed to deliver its messages directly to them, in part by merging with the extremist networks online. In some cases, as part of wider politically oriented campaigns, it made direct contact with specific American political activists.[160]

At the same time, Russia targeted specific groups—or sometimes invented such groups, gathering members from among like-minded social media participants—likely to engage in overt political activity as a result of the information. These groups were on both sides of the political spectrum: One example was an anti-Trump protest by the supposed group BlackMattersUS, which attracted 16,000 people to a rally in New York.[161] These activities suggest that Russian information campaigns have only begun to scratch the surface of a highly targeted, issue-specific, sometimes even individualized campaign to make use of existing groups in target societies to affect political outcomes.

These examples of Russian social manipulation strategies may not be representative of all such efforts, but they do indicate that, in some

---

[158] Nelson, Orttung, and Livshen, 2016, pp. 8–9.

[159] Nelson, Orttung, and Livshen, 2016, pp. 8–9.

[160] Tricia Jenkins, "What Did Russian Trolls Want in 2016?" *War on the Rocks*, May 22, 2018.

[161] Ali Breland, "Thousands Attended Rally Organized by Russia on Facebook," *The Hill*, October 31, 2017.

cases, Russia does target specific audiences. Moreover, these examples bolster the theory that Russian targeting strategies do not attempt to incite wholly new tensions but rather foment existing discord in Russia's target audiences.

Messages

The narratives associated with alleged Russian social manipulation strategies vary depending on their intended audiences and objectives. Given the multitude of suspected Russian targets discussed above, capturing the range of messages of the alleged Russian efforts would be lengthy. That said, there are some overarching trends in narratives across efforts.

When targeting audiences that share cultural, linguistic, or historical ties with Russia, Moscow appears to underscore these commonalities. The legacy of the Second World War (or the Great Patriotic War, as it is often referred to in the region) is a common trope used in social manipulation targeting former Soviet states. This important shared experience affected most of the population in the region, transcends national boundaries, and is associated with both painful memories and pride. Some in the region feel the West has not been sufficiently grateful for their sacrifices. Consequently, Russian messaging underscores both the joint sacrifice and the West's lack of adequate gratitude.[162]

Russia also appears to use pronationalist narratives and to incorporate historical memories, such as those of lost territory, into its messaging in Central, Eastern, and Southern Europe.[163] Russian messaging in these states often also focuses on the alleged moral corruption and opulence of the Western liberal order, the failed promises made by Western institutions, the threats posed by Western institutions, and

[162] Kirk, 2017b.

[163] Lóránt Győri, Peter Krekó, Jakub Janda, and Bernhard Weidinger, *Does Russia Interfere in Czech, Austrian, and Hungarian Elections?* Political Capital, European Values, in cooperation with Dokumentations Archiv des österreichischen Widerstandes, 2017, p. 4; phone interview with Hungarian Academic 012, October 6, 2017.

the negative aspects of globalized societies.[164] These messages are often designed to play off of existing local sentiment.

Messages targeting Western European audiences often portray U.S. policies, efforts, or leaders negatively. In other instances, messaging focuses on issues controversial among some populations, such as the backlash against Muslim immigrants and refugees. Likewise, if Russia is, in fact, the sponsor of many recent social manipulation efforts in which it has been implicated, this would indicate that Russian messages are also tailored to support or discredit specific policy ends like the election of a candidate or the passage or defeat of specific legislation.

Again, this trend is evident in the case of the 2016 U.S. presidential election. Information released about Russian efforts targeting the U.S. public during the campaign demonstrates that Moscow's messaging appeared to discredit then-candidates Hillary Clinton, Ted Cruz, and Marco Rubio and to positively portray then-candidates Bernie Sanders and Donald Trump.[165] At a more granular level, Russian messaging incorporated existing narratives in U.S. discourse and existing sentiments held by the U.S. population on the hot-button issues of religion, immigration, and racial tensions, as well as geographic-specific regional or local issues.[166] For instance, some Russian-linked accounts disseminated anti-Muslim and anti-immigrant messages.[167]

This focus on polarizing issues was also the case for messaging propagated by allegedly Russian-linked accounts targeting U.S. audiences outside of the 2016 election. Following the 2018 Parkland, Florida, Marjorie Stoneman Douglas High School shooting, accounts with suspected links to Russia posted messages on the divisive issue of gun

---

[164] Győri et al., 2017, p. 4.

[165] "United States of America v. Internet Research Agency LLC, [et. al]," pp. 4, 17; Office of the Director of National Intelligence, 2017, p. 9.

[166] "United States of America v. Internet Research Agency LLC, [et. al]"; Albright, 2018.

[167] U.S. House of Representatives Permanent Select Committee on Intelligence, *Report on Russian Active Measures*, March 22, 2018, p. 33.

control, using the hashtags #guncontrolnow and #gunreformnow and promoting conspiracy theories about the perpetrator.[168]

This discussion of Russian messaging may give the impression that Russian messaging is all carefully composed and highly coordinated. This does not appear to be the case. While this may be true of some strategies, in other cases the messaging is inconsistent and even contradictory.[169]

Lastly, the messages that Russia disseminates abroad are complex to characterize in that they vary along two axes. Firstly, the level of sophistication varies, from clumsy or crude messages to sophisticated arguments.[170] Secondly, the accuracy of the information varies. It can be either entirely truthful, partially false, purposely misconstrued, or false. This is to say that there are various permutations of Russian information efforts, which make them all the more difficult to counter.

Sources of Narratives

Given the apparent lack of structure among the loosely connected group of actors described above, we were curious to understand where they get their narratives. Several of those with whom we spoke offered the same answer: Putin and his officials' public remarks offer general guidance on the Kremlin's stance toward various policies and actors.[171] A Moscow journalist noted the existence of invisible red lines and the expectation that those in the system know what these are.[172] Remarks from Pavlovsky in a recent interview appear to substantiate this point, even though he might have been referring more specifically to the domestic political context:

---

[168] Sheera Frenkel and Daisuke Wakabayashi, "After Florida School Shooting, Russian 'Bot' Army Pounced," *New York Times*, February 19, 2018.

[169] Christopher Paul and Miriam Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016, pp. 7–9.

[170] Phone interview with expert 030, January 15, 2017.

[171] In-person interview with Department of State official 010, October 4, 2017; in-person interview with European defense official 020, October 26, 2017.

[172] Phone interview with Russian journalist 027, October 31, 2017.

> Today, today the mass media is—the central power as FSB or investigation committee, they are not getting directives from Putin. They are not told what to say. They make up their plans, but they know in which direction to move. They know they have multiple meetings with members of the presidential administration. They have weekly meetings, and sometimes, they meet more often than that. Hence, all TV channels get general political instructions for the coming week.[173]

One potential indicator of the network's reliance on guidance is its behavior when the Kremlin is silent.[174] In the hours after the killing of an Armenian family at the hand of a Russian soldier who had wandered off base, the Kremlin was notably absent from public discourse. Coverage of the massacre by Russian state-sponsored news outlets (domestic and foreign-facing) was equally quiet in the first days after the massacre.[175] The few articles that were published tended to focus on the violence of the Armenian protests that, in response to the killing, called for the Russian ambassador to be ejected and the Russian base in Armenia to be closed.[176]

Senior editors of state-sponsored news outlets reportedly receive broad guidance from the Kremlin in the form of *temniki*.[177] *Temnik*, derived from the Russian word for *theme*, refers to guidance from the government communicating which stories should be covered, which should be ignored, and whether those covered should be portrayed positively or negatively.[178] Most often, this guidance is reportedly relayed

---

[173] Kirk, 2017a.

[174] Phone interview with Russian journalist (interview 27), October 31, 2017.

[175] Former Russian journalist and editor 027, October 31, 2017; additionally, no announcement was made by Russia's Foreign Ministry, nor by the president's press office in the days following the massacre.

[176] "Protesters Demand Russian Soldier's Trial in Armenia, Clash with Police," RT, January 15, 2015.

[177] Former Russian journalist 027, October 31, 2017.

[178] *Temniki* first appeared in autumn 2001 in Ukraine in the prelude to the March 2002 Ukrainian parliamentary elections, according to a Human Rights Watch investigation on state censorship in the Ukrainian media. According to senior editors, journalists, and media

orally to senior station editors of Kremlin-sponsored outlets in weekly meetings. The temniki reportedly influence editorial policy, which station editors communicate to their subordinates, and so on.[179] Though these directives primarily affect domestic Russian media, RT's editor-in-chief is reportedly in attendance at the meetings where the guidance is delivered.[180] Based on accounts from some employees of RT, the outlet's staff has some independence in deciding how RT conveys its message; however, there are "untouchable" stories that are mandated "from above."[181] While editors have the ability to "debate" which content is disseminated, managers have full approval authority.[182]

Leaked and publicly released documents, as well as interviews with former employees of the IRA, offer further insight into where potential Russian proxies get their narratives. An alleged former employee of the IRA explained that when assigned to the "foreign desk," he received

---

analysts interviewed, temniki are eight- to ten-page documents sent to television stations and selected newspapers with directions on what and how to report during that week. These appeared to be drafted and sent by the presidential administration of Leonid Kuchma, though they were not signed or stamped to maintain plausible deniability. These directives were initially sent to selected television stations, but their distribution was later expanded to include all stations and some newspapers. Editors, journalists, and media analysts reported feeling pressure to comply, concerned that failure to do so would result in negative repercussions such as job loss, salary cuts, or decreased budgets for their outlet ("Negotiating the News: Informal State Censorship of Ukrainian Television," *Human Rights Watch,* Vol. 3, No. 2, March 2003, pp. 13–24.

[179] "Temnik—The Kremlin's Route to Media Control," *EU vs Disinfo*, March 29, 2017; Dmitry Skorobutov, "Ispoved' Propagandista. Chast' I. Kak Delajut Novosti na Gosudarstvennom TV," *The Insider*, June 9, 2017. The use of temniki was brought up in two of our discussions, both with former journalists at Russian state news agencies. Both recalled hearing about such meetings from their editors. Phone interview with Russian journalist former desk chief (interview 27, October 31, 2017), and Moscow journalist (interview 26), November 28, 2017. A former RT journalist noted that in her time with the organization, she did not receive direct orders from above on what to report on, but rather some stories she put forth were declined by the Russian news director ("Russian Propaganda Broadcast into Canadian Homes," CBC News, *The Weekly*, January 21, 2018).

[180] Office of the Director of National Intelligence, 2017, p. 9.

[181] Matthew Bodner, Matthew Kupfer, and Bradley Jardine, "Welcome to the Machine: Inside the Secretive World of RT," *Moscow Times*, June 1, 2017.

[182] Bodner, Kupfer, and Jardine, 2017.

Excel files from the organization's "analytics desk" containing links to stories he was directed to comment on, and brief instructions on how to comment on these.[183] This suggests that the organization's messages are directed and somewhat coordinated, although the origins of its directives remain uncertain. While the organization is suspected to have ties to the Kremlin through the Russian businessman and financier of the factory Yevgeniy Prigozhin and several of his associates, there is little definitive evidence linking the IRA's messaging instructions with the authorities in Moscow.[184] According to the independent Russian station that interviewed him, the former employee provided records confirming his employment at the IRA.[185]

Russian social manipulation also appears to recycle, repackage, and amplify messages published by nonaffiliated news outlets or other channels. One Moscow correspondent with whom we spoke noted that

---

[183] The original interview can be found here in Russian: Evgenia Kotlyar, "U Nas Byla Cel' . . . Vyzvat Besporjadki': Interv'ju s Jeks-Sotrudnikom 'Fabriki Trollej' v Sankt-Peterburge," *Dozhd*, October 14, 2017. A summary of the interview in English can be found in "An Ex St. Petersburg 'Troll' Speaks Out: Russian Independent TV Network Interviews Former Troll at the Internet Research Agency," 2017. The "foreign desk" is allegedly the department within the IRA responsible for the 2016 U.S. election social manipulation efforts.

[184] The 2018 U.S. indictment of the IRA filed by U.S. authorities accuses the organization of "engag[ing] in operations to interfere with elections and political processes" and confirms Prigozhin as its financier ("United States of America v. Internet Research Agency LLC, [et. al]." pp. 2–3). However, it is important to note that while the indictment acknowledges that Prigozhin's company Concord has other Russian government contracts, nowhere in the document does it explicitly link the 2016 U.S. campaign with the Kremlin. Additionally, documents leaked by the group Anonymous International demonstrate the IRA's financial ties to Concord and to other individuals working at or connected to the agency. The leaked documents were originally posted with "Chast' pervaja. Zoloto trollej" ["Part One. Troll Gold"], Anonymous International, May 26, 2014, but have since been removed. For a description and analysis of the documents, see Max Seddon, "Documents Show How Russia's Troll Army Hit America," BuzzFeed News, June 2, 2014. Other analyses detailing the personal connections can be found in Russian; see Aleksandra Garmazhapova, "Gde Zhivut Trolli. I Kto ih Kormit" ["Where Trolls Live. And Who Feeds Them"], *Novaya Gazeta*, September 9, 2013.

[185] "An Ex St. Petersburg 'Troll' Speaks Out: Russian Independent TV Network Interviews Former Troll at the Internet Research Agency," 2017.

sites like Alternet, Breitbart, and blogs of European fringe movements are some of the sources from which Russia harvests its messaging.[186]

Likewise, a recent analysis of Russian efforts during the 2016 U.S. election, which examined a sampling of tweets produced by 388 of the 2,752 troll accounts, concluded that a significant portion of the tweets amplified authentic national, regional, and local news. In doing so, many of the tweets produced by the IRA trolls linked to legitimate nonaffiliated news sites. The *Washington Post,* Fox News, Reuters, and the *New York Times* were all among the top 15 most linked-to sources.[187] Thus, in some cases, it is possible that Russian social manipulation strategies appropriate and propagate legitimate news messages.

Much like Soviet-era actors, Russian-affiliated actors may have linked to these legitimate nonaffiliated sites in an effort to legitimize themselves or their own messages. Unlike in Soviet times, however, the Russian actors may not need to spend significant amounts of time and resources to cultivate relationships with the gatekeepers to these legitimate outlets.

Actions: What Russia Is Doing and How

It is challenging to neatly catalog, map, and characterize Russian social manipulation actions. There are several reasons for this. First, the actions are often designed to conceal the perpetrators' identities and to confuse the target audiences (and inquisitive minds) through mass and complexity. Such actions can involve a tangled web of mutually reinforcing or completely contradictory messages. The opaque nature of these actions complicates attribution; in many cases, the evidence can imply Russian involvement but not definitively link individual actions with the Russian government. As mentioned earlier, individuals or groups whose beliefs genuinely reflect Russian social manipulation narratives either create new or recycle existing content that reinforces

[186] Phone interview with Moscow correspondent 014.

[187] Albright, 2018.

Russia's narratives, further blurring the lines between Russian-sponsored and Russian-inspired messages and actions.

To assess this complex topic, in this section we will first address the most direct form of social manipulation: the physical control of the means of communication. Next, we describe the known instruments of Russian social manipulation. By *instruments*, we mean the content and how it is packaged (e.g., a forgery of a letter, image, video, etc.). We then explain the various conduits by which these instruments are delivered to the target audiences (e.g., television programming, social media platforms). Lastly, we discuss techniques that Russian-affiliated groups are suspected of using to maximize the effects of their efforts (e.g., bot campaigns, use of "sockpuppets," clickbait). In the notional example of a campaign to discredit a candidate by using a forgery of a document to "prove" the candidate's purportedly corrupt practices, the forgery is the instrument, the social media platform is the channel of communication, and trolling is the technique to maximize the effects of the campaign.

Controlling the Means of Communication

In some cases, Moscow has taken command of the very mechanisms by which information is communicated to its target audiences. The most extreme example is the monopoly Russia established over information in the early stages of the Ukraine crisis. One of the first actions by the Russian troops in Crimea and eastern Ukraine was to seize the Ukrainian communications infrastructure, primarily the television towers in Crimea and eastern Ukraine, which allowed Russia to control the content communicated to local audiences.[188] In Slavyansk, for instance, "well-equipped gunmen accompanied by specialized technicians disarmed the guards, allowing the technicians to connect sophisticated satellite equipment and replace Ukrainian channels with the

[188] Jill Dougherty, "Everyone Lies: The Ukraine Conflict and Russia's Media Transformation," Discussion Paper Series, Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School, July 2014, pp. 3–7.

pro-Kremlin Russian broadcasts."[189] According to Ukrainian counterintelligence authorities, these men were suspected of being Russian intelligence operatives.

Once Russian forces had established control over many sources of information, Russian television channels, which were available in Crimea and eastern Ukraine and already viewed by these audiences, reported false accounts of Ukrainian fascists hunting Russians and Russian-speaking Ukrainians. Additional false accounts recounted the development of a humanitarian crisis and a mass exodus of asylum-seekers from eastern Ukraine.[190]

In other central, eastern, and southern European states, many analysts, scholars, and officials have voiced concerns over suspected attempts by Russia to exert indirect and subtle control over the communication channels in their European countries. Russian-affiliated actors have been accused of seeking majority control over television networks or other media companies.[191] However, given the inherently obfuscated nature of these actions, little evidence exists to validate the assertions. It is also difficult to discern whether certain outlets promoting a pro-Russian stance are self-motivated or externally induced.

Appropriating and Manipulating Content

Though much of the public discourse on this topic is devoted to Russia's use of disinformation, the Kremlin also appropriates and manipulates factual information as content in its social manipulation efforts.

---

[189] Phillip Shishkin and James Marson, "Ukraine Accuses Kremlin Agents of Coordinating Separatist Unrest," *Wall Street Journal*, April 20, 2014.

[190] Dougherty, 2014, pp. 4–5.

[191] For a discussion of potential Russian interference in the Bulgarian media landscape, see Dimitar Bechev, *Russia's Influence in Bulgaria*, Brussels: New Direction: The Foundation for European Reform, May 12, 2015, pp. 22–23; for a discussion of potential Russian interference in the Serbian media landscape, see "Eyes Wide Shut: Strengthening of Russian Soft Power in Serbia: Goals, Instruments, and Effects," Center for Euro-Atlantic Studies, May 2016, pp. 56–64; for a discussion of potential Russian interference in the Hungarian media landscape, see Attila Juhász et al., "'I Am Eurasian': The Kremlin Connections of the Hungarian Far-Right," Political Capital and Social Development Institute, March 2015, pp. 32–51; phone interview with Hungarian academic 012, October 6, 2017.

As in the Cold War, the Russian government is believed to leak private or classified information to discredit its targets. The Russian security services are suspected of intercepting, recording, and leaking private telephone conversations of several prominent U.S. and European officials.[192]

One such leak was a damning conversation in 2014 between U.S. Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland and U.S. Ambassador to Ukraine Geoffrey Pyatt. Nuland conveyed her annoyance with the European Union by using a less-than-diplomatic choice of words—"Fuck the EU"—and expressed partiality toward two potential members of Ukraine's government.[193] A video containing the audio recording of the call was anonymously posted to YouTube and then reposted by Lev Mishkin, a *sockpuppet*—a fictitious online identity created by a person or group to promote particular opinions or views—with alleged links to Russia.[194]

Though the genesis of the intercept is unknown, some U.S. officials and experts suspect it was the work of Russian security services, while others believe the Security Service of Ukraine (SBU) was responsible.[195] Regardless of its origin, the intercept, which could have provoked a rift between the United States and the European Union or offered proof that the Maidan revolution was engineered by Western officials, provided Russia with damaging content to leverage against the United States.[196]

An RT article published two days after the leak quoted a foreign policy expert chastising Nuland: "What she hasn't apologized for is the plans to midwife a new government in Ukraine . . . she is not apologizing for trying to overthrow the government in Kiev, calling it a popu-

---

[192] Eli Lake, "Putin's Latest Dirty Trick: Leaking Private Phone Calls," *Daily Beast*, March 26, 2014.

[193] Lake, 2014; Soldatov and Borogan, 2015, pp. 285–288.

[194] Soldatov and Borogan, 2015, pp. 285–287.

[195] Soldatov and Borogan, 2015, pp. 285–288.

[196] Soldatov and Borogan, 2015, p. 287.

lar democracy."[197] A Voice of Russia (now Sputnik) headline screamed: "Nuland/Pyatt Dialogue Prove US-Backed Coup."[198] Nuland was portrayed as sympathizing with the Maidan protesters. Russian-affiliated outlets such as Sputnik continued to cover this story long after its initial surfacing in the years afterward—a tactic harkening back to Soviet-era information efforts.[199] This is only one of several such conversations that have been intercepted and publicized.

The Kremlin is suspected of having a hand in hacking and subsequently leaking the private emails of U.S. presidential candidate Hillary Clinton, other members of the U.S. Democratic Party, and French presidential candidate Emanuel Macron, among others. An investigation by the U.S. intelligence community determined that the U.S. leaks were likely an operation by Russia's General Staff Main Intelligence Directorate, which used WikiLeaks to publish the leaked material.[200] None of the documents posted on WikiLeaks was determined to be forged.[201]

In the Macron case, a trove of leaked emails that were posted on the site 4chan included authentic as well as falsified emails, according to Macron's political party En Marche.[202] Though some of the files' forensic evidence implied Russian involvement, it was inconclusive and conspicuous enough that some experts argued it could have been planted with the intention of framing Russia.[203] As with the intercepted phone conversations, Russia appears to leak private emails at

---

[197] "'F**k the EU': Snr US State Dept. Official Caught in Alleged Phone Chat on Ukraine," RT, February 6, 2014.

[198] "Anonymous Ukraine Klitschko E-mails and Nuland/Pyatt Dialogue Prove US-Backed Coup," Sputnik (then Voice of Russia), February 25, 2014.

[199] "Victoria 'F*ck the EU' Nuland Leaves Her Post at the US State Department," Sputnik, January 27, 2017.

[200] Office of the Director of National Intelligence, 2017, pp. 2–3.

[201] Office of the Director of National Intelligence, 2017, p. 3.

[202] Andy Greenberg, "Hackers Hit Macron with Huge Email Leak Ahead of French Election," *Wired*, May 5, 2017a.

[203] Andy Greenberg, "Don't Pin the Macron Email Hack on Russia Just Yet," *Wired*, May 8, 2017b.

opportune times in an attempt to influence audiences by portraying individuals or issues in a negative light, by distracting or confusing audiences, and by provoking controversies.

Russian social manipulation efforts have also appropriated unaltered images and videos from unrelated (and likely unwitting) sources and then used that content to substantiate their messages. In 2014, RT lifted an image from a 2012 opposition rally in Poland for a story on an alleged demonstration in western Ukraine calling for the region's annexation by Poland.[204] In another case, Zvezda (a Russian television network run by the country's Ministry of Defense) and several other stations posted a video allegedly demonstrating the Ukrainian military's use of phosphorous bombs against civilians. The video was footage from fighting in Fallujah, Iraq, in 2004.[205] There are countless examples of these kinds of misattributed images and videos.

Producing Falsified Content

Much like the Soviets before it, Russia relies on falsified information, such as forgeries, to validate its messaging and tarnish its targets. In some cases, these are falsified documents; in others, edited or manufactured still images or video footage. As with leaks of authentic documents, counterfeit documents believed to be produced by the Russian government or its proxies surface anonymously and are then amplified by other means.

Several forgeries targeting Swedish officials and policymakers have surfaced. Some evidence suggests that these may have been planted by Russia-linked actors.[206] One is a falsified letter from Tora Holst, chief prosecutor at Stockholm's International Public Prosecution Office, to Oleksiy Pokotylo, an alleged representative from the Ukrainian "Head Department for National Security and Defence [sic]

---

[204] "Russia's Top Lies About Ukraine. Part 1," blog post, *StopFake*, July 10, 2014a.

[205] "Russia's Top Lies About Ukraine. Part 2," blog post, *StopFake*, July 10, 2014b. The video and corresponding story were originally posted on Zvezda's Russian-language site, but the footage has since been removed ("Nacgvardija Obstreljala Semenovku Fosfornymi Bombami," Zvezda, June 6, 2014).

[206] Kragh and Asberg, 2017, pp. 773–816.

Affairs." The letter appears to be a response to a request by the Ukrainian government to dismiss an investigation into war crimes perpetrated by a Ukrainian citizen in Sweden. In the letter, Holst appears to turn down Pokotylo's request. Though Holst confirmed that her office is investigating a person residing in Sweden and the person's connection to war crimes, she denied penning the letter and noted the incorrect letterhead used by its author.[207]

The forgery initially surfaced in September 2015 on CNN's iReport site—a site that allows users to self-publish content—and was later broadcast on Russian state television and on government affiliated outlets.[208] It is important to note that, although the letter has appeared on Russian television, there is little concrete evidence tying its production to Russia. That said, it is one of 26 forgeries targeting Sweden that appeared between December 2014 and July 2016. Several, like the letter above, attempt to reveal secret dealings between the Swedish government and the authorities in Kyiv. Though it is difficult to prove any correlation, some have said the link between the timing of the uptick in forgeries and the implementation of the NATO host agreement with Sweden is too close to be coincidental.[209]

Russia has publicized doctored and manufactured images and videos to lend legitimacy to its messaging.[210] It is difficult to identify whether Russia, its associates, or independent actors are the original editors or manufacturers. Nevertheless, Russian-owned or -affiliated actors have incorporated such images into their social manipulation efforts, as was the case with a doctored image of the MH-17 incident; Russian television claimed the airliner was shot down by a Ukrainian

---

[207] "Fake Swedish Letter in Russian Media," blog post, *StopFake*, September 15, 2015; "Fake 'Swedish' Letter Spread in Russian Media," Radio Sweden, September 13, 2015.

[208] Kragh and Asberg, 2017, pp. 793–795.

[209] Kragh and Asberg, 2017, p. 806. For another example of a suspected Russian forgery, see John R. Haines, "Distinguishing the True from the False: Fakes and Forgeries in Russia's Information War Against Ukraine," Foreign Policy Research Institute, September 28, 2016.

[210] Soldatov and Borogan, 2015, pp. 284–285.

fighter jet.[211] Russian television stations that broadcast in Russia and Ukraine have also been accused of using an actress to masquerade as very different personas—an Odessa resident fearful of pro-fascist authorities in Kyiv, a protestor in Crimea, and a concerned mother of a Ukrainian soldier—to create the appearance that Ukrainians supported the Russian position, not the new Ukrainian government.[212] In fairness, the Ukrainian government has also been accused of circulating falsified images to engender sympathy for its cause against Russian aggression.[213]

Russia's Facebook and Instagram ads that were published during the U.S. election can also be characterized as forgeries, in that they masqueraded as legitimate organizations. Although such forgeries, leaked documents, and doctored images are useful for establishing credibility, they are more powerful when communicated as part of a broader message. As such, Russian efforts appear to incorporate and frame these actions and artifacts within broader messages. Additionally, Russian efforts appear to be opportunistic, such that they will appropriate existing forgeries, etc., and weave these into their narratives.

Disseminating the Content

Russia and its affiliates use various channels to publish their content and connect with their target audiences. These range from traditional media—such as television programming, radio broadcasts, and print articles—to nontraditional media, such as social media platforms, comment sections of online articles, and others.

Many of the actions discussed above are reminiscent of Soviet actions during the Cold War era. One of the variables that have changed in the intervening years is the mechanisms of dissemination.

---

[211] Max Seddon, "Russian TV Airs Clearly Fake Image to Claim Ukraine Shot Down MH17," BuzzFeed News, November 15, 2014b.

[212] Lucy Crossley, "The 'Aggrieved Housewife', the 'Soldier's Mother' and the 'Kiev Resident': Did Russian Television 'Use Actress to Portray FIVE Different Women' As It Reported Normal Ukrainians Backed Kremlin," *Daily Mail*, March 5, 2014.

[213] Amos Chapple, "War of Words over Ukraine 'Combat' Photo," Radio Free Europe Radio Liberty, August 25, 2016.

Advances in technology have facilitated the increased scope and reach of such campaigns. Cultivating relationships to gain coveted access to journalists or television editors in order to disseminate messaging is less important, given the proliferation of mechanisms that allow for self-publication. Meanwhile, the democratization of tools and platforms for communication has made attribution more difficult. The Russian government and its potential proxies appear to leverage many of these new mechanisms and their convenient anonymities while continuing to rely on time-tested practices.

Despite the proliferation of new media, Russia continues to use television and radio programming in its social manipulation efforts. RT, the Russian government–sponsored international television network, has positioned itself as an alternative to the "monopoly of Anglo-Saxon global information streams."[214] The channel offers 24/7 coverage of its interpretation of the news. RT's counterpart Sputnik, the international radio and podcasting service, claims to "tell the untold."[215] Both agencies operate news websites, video content sharing channels, and other social media properties. Additionally, Russia has access to many other websites, television and radio broadcasts, online networks, and social media properties that it can use to disseminate content for social manipulation. The Kremlin or its proxies are also suspected of using billboards to communicate with target audiences.[216]

Maximizing the Effects

The automation and the anonymity afforded by new fora for online political discourse have endowed Russia with techniques to maximize the reach, visibility, and credibility of its social manipulation efforts while maintaining plausible deniability. These techniques include the

---

[214] Vladimir Putin reportedly made this statement on a 2013 visit to RT's Moscow headquarters (Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *New York Times*, September 13, 2017).

[215] "Products and Services," webpage, Sputnik, undated; "Telling the Untold," webpage, Sputnik, undated.

[216] "Crimean 'Nazi' Billboard Highlights Propaganda Problem: U.S.," CBS News, March 10, 2014; Alan Yuhas, "Russian Propaganda over Crimea and the Ukraine: How Does It Work?" *The Guardian*, March 17, 2014.

use of social bots, political sockpuppets, search engine optimization strategies, clickbait, technologies to clone websites, and others.[217] We offer details about just the first few of these.[218]

Deploying Automated and Anonymous Agents (Bots)

Though the definition of *bots* has evolved since their inception in the 1990s, they are broadly defined as "automated agents that function on an online platform."[219] Within this broader taxonomy of bots, those used by the Russian government in the context of social manipulation are typically social bots, or programs "that automatically produce content and interact with humans on social media," sometimes mimicking the behavior of humans.[220] Social bots can be deployed on any number of social media platforms to post or share content, masquerading as real human users. Thanks to their automation, social bots allow those who deploy them to generate and disseminate significantly more content than would be possible by humans. As such, social bots allow their operators to promote certain messages through volume and repetition and to suppress alternative messages by overwhelming them.

The Russian government first employed social bots at home to influence domestic political discourse and to subdue opposing views.[221]

---

[217] Though Garth S. Jowett and Victoria O'Donnell use the nomenclature "techniques to maximize effect" to categorize the use of certain propaganda techniques in their book *Propaganda and Persuasion*, the techniques described are different from those in this discussion (Jowett and O'Donnell, 2012). For a brief discussion of some of these techniques employed in a real-world campaign, see Chen, 2015.

[218] It is important to acknowledge that there is little agreement on specific definitions for the terms used to describe human- and computer-driven online accounts. In an effort to be consistent, in this chapter we use terms as they are defined by Robert Gorwa and Douglas Guilbeault in their typology, based on a survey of the recent relevant literature. Robert Gorwa and Douglas Guilbeault, "Understanding Bots for Policy and Research: Challenges, Methods, and Solutions," Prague: Conference of the International Communication Association, May 2018.

[219] Gorwa and Guilbeault, 2018, pp. 8–9.

[220] Gorwa and Guilbeault, 2018, p. 8.

[221] Sergey Sanovich, *Computational Propaganda in Russia: The Origins of Digital Misinformation*, Working Paper No. 2017.3, Computational Propaganda Research Project, University of Oxford, Oxford, UK, 2017.

Moscow has since used this tool to target external audiences, evidence suggests.

Investigations jointly conducted by the U.S. Congress and technology firms have identified a bot campaign that operated during the 2016 U.S. presidential campaign that evidence suggests may have been sponsored by the Russian government. As of January 2018, Twitter identified over 50,000 bots linked to Russia that were operational during the 2016 U.S. presidential campaign.[222] Analyses of the social bot traffic during the campaign found that the number of bot-generated tweets classified as pro-Trump was significantly higher than pro-Clinton tweets during the campaign, and that bots "strategically colonized pro-Clinton hashtags, and then disabled activities after Election Day." However, this analysis includes bots sponsored by U.S. political entities.[223] Still, evidence suggests that pro-Trump bot traffic may have been engineered by the Russian government.[224] Russia has also been accused of deploying bot campaigns against several other target states.

Employing Sockpuppets (Trolls)

Politically driven sockpuppets, or what are now commonly referred to as *trolls* in public discourse, are manually controlled (i.e., human-controlled) "accounts that impersonate humans for political purposes."[225] In other words, these are accounts that pose as legitimate

---

[222] April Glaser, "Twitter Admits There Were More Than 50,000 Russian Bots Trying to Confuse American Voters Before the Election Campaign," *Slate*, January 19, 2018.

[223] Bence Kollanyi, Phillip N. Howard, and Samuel C. Woolley, "Bots and Automation over Twitter During the U.S. Election," Comprop Data Memo 2016.4, Computational Propaganda Research Project, University of Oxford, Oxford, UK, November 17, 2016.

[224] Alice Marwick and Rebecca Lewis, "Media Manipulation and Disinformation Online," Data and Society Research Institute, undated, p. 38.

[225] Gorwa and Guilbeault, 2018, p. 10. As with *bots*, the meaning of the term *troll* has metamorphosed over time. Even now there is little consistency in the use of this term within the computer science community, among policymakers, or in the media. Internet trolling has existed since people have been able to interact online. For much of the 2000s, the term *trolls* referred to humans who generated and/or communicated inflammatory material online, with the intent to offend, irritate, or provoke. The ultimate objectives of these trolls are varied: "They do this for many reasons, from boredom, to making people think, but

individuals or groups and are operated by humans, just not those the accounts claim to be. Sockpuppets can post comments on articles, share content, and "like" content while cloaked behind the anonymity of the internet, engendering false impressions about public discourse or sentiment. They can create the illusion that many (or few) "people" support certain messages. This provides sponsors of these activities with both credibility and mass.

The Russian government is suspected of employing sockpuppets to influence audiences and drive political outcomes. In 2012, leaked emails from the leader of the Kremlin-funded youth group *Nashi* offered evidence that the Russian government had paid bloggers and commenters to post pro-Putin content.[226] Sockpuppet campaigns have been identified in Ukraine, Poland, and Finland, but it is unclear whether these were sponsored by Russia or were the work of pro-Kremlin enthusiasts.[227] More recently, evidence has come to light that helps to further substantiate Russia's use of sockpuppet campaigns for political ends.

The IRA employs hundreds of individuals to generate content, operate accounts, and use these to post content. Information made public by the U.S. Congress and tech companies demonstrates the IRA's use of sockpuppets to generate and post content related to the 2016 U.S. presidential campaign.[228] Over 2,500 Twitter handles were operated by employees of the IRA during the campaign, and 3,300

---

most do it for the lulz. . . . Lulz is laughter at someone else's expense" (Encyclopedia Dramatica, "Troll" and "Lulz," referenced in E. Gabriella Coleman, "Phreaks, Hackers, and Trolls: The Politics of Transgression and Spectacle," in Michael Mandiberg, ed., *The Social Media Reader*, New York: New York University Press, 2012, p. 111. The online image forum 4chan.org, founded in 2003, is often considered a birthplace of this early provocative trolling behavior. Since then, the concept of trolling has evolved. Given the public's recent focus on Russian social manipulation efforts, the term *troll* is now often used in public discourse with the assumption that the trolling always has political ends.

[226] Miriam Elder, "Polishing Putin: Hacked Emails Suggest Dirty Tricks by Russian Youth Groups," *The Guardian*, February 7, 2012 .

[227] NATO StratCom Center of Excellence, *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia*, undated.

[228] David S. Cloud, "Facebook Tells Congress That 126 Million Americans May Have Seen Russia-Linked Ads," *Los Angeles Times*, October 31, 2017.

advertisements were designed and promoted by the proxy group.[229] Accounts from former IRA employees and leaked documents indicate that the quality of the IRA-generated content has improved since its inception, and that employees assigned to the "foreign desk" are considered to be the most creative and qualified.[230] Some evidence indicates that the IRA is only one of several outfits working as sockpuppets on behalf of the Russian government.

In fairness, social bot and sockpuppet campaigns are not exclusive to Russia. Rather, they are employed by other governments, for commercial use, and by political campaigns.[231]

Optimizing Traffic and Brandishing Clickbait

Another tool that Russian-linked accounts are suspected of using is the strategic manipulation of search engine results pages, the nefarious side of search engine optimization.[232] This practice is the deliberate attempt to tamper with search engine algorithms such that the results returned present the perpetrator's content first, above results that would have appeared organically had the algorithm not been manipulated.[233] This technique can increase the visibility of content, ensuring more eyeballs see it, and can depress audience exposure to alternative narratives. Likewise, it bestows a false sense of credibility on the content visible first in the responses.

Russia is suspected of using these techniques as a means of conducting social manipulation. For instance, stories from Russian state-sponsored news outlets RT and Sputnik appeared high in the list of results in response to queries made about the poisoning of former Rus-

---

[229] Ben Collins et al., "House Drops Motherlode of Russian Propaganda," *Daily Beast*, November 1, 2017.

[230] RBC, "Rassledovanie RBK: Kak 'Fabrika Trollej' Porabotala Na Vyborah v SShA," Vol. 11, No. 35, October 17, 2017; "An Ex St. Petersburg 'Troll' Speaks Out: Russian Independent TV Network Interviews Former Troll at the Internet Research Agency," 2017.

[231] Gorwa and Guilbeault, 2018, pp. 9–10.

[232] Dipayan Ghosh and Ben Scott, "#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet," New America, Public Interest Technology Program, January 2018, p. 17.

[233] Ghosh and Scott, 2018, p. 18.

sian spy Sergei Skripal.[234] Some suspect that it is unlikely these results were organically derived. The same was true for searches conducted using the query "ODNI hacking report" in reference to the 2017 Intelligence Community Assessment on Russia's activities targeting the U.S. election.[235]

Bots and sockpuppets can drive visibility for Kremlin messages by affecting search engine algorithms.[236] Search engine optimization techniques are driven by bot and sockpuppet campaigns, as well as through the use of clickbait. RT uses clickbait and viral videos, such as those of natural disasters, to increase the time spent watching RT videos and to generate more likes. Longer watch times and higher numbers of likes result in more favorable placement in YouTube's search results and recommendations.[237]

Tangled Web of Techniques

None of the aforementioned techniques are typically used in a vacuum. Rather, they are often employed as one part of broader efforts. The various elements of Russia's social manipulation efforts can be used to mutually reinforce one another, creating a complex, tangled web.[238]

The Digital Research Forensics Lab's deconstruction of a specific campaign, one in which the IRA attempted to malign actor Morgan Freeman's critique of Russian disinformation efforts, demonstrates this in practice.[239] On September 18, 2017, a nonprofit organization, the Committee to Investigate Russia, released a video featuring Free-

---

[234] Chris Meserole and Alina Polakova, "Disinformation Wars," *Foreign Policy*, May 25, 2018.

[235] Kaveh Waddell, "Kremlin-Sponsored News Does Really Well on Google," *The Atlantic*, January 25, 2017.

[236] In-person interview with Department of State official.

[237] Daisuke Wakabayashi and Nicholas Confessore, "Russia's Favored Outlet Is an Online News Giant. YouTube Helped," *New York Times*, October 23, 2017.

[238] Digital Forensics Research Lab, "Russia's Full Spectrum Propaganda: A Case Study in How Russia's Propaganda Machine Works," The Atlantic Council, January 23, 2018; Defense Intelligence Agency, "Russia Military Power: Building a Military to Support Great Power Aspirations," 2017.

[239] Digital Forensics Research Lab, 2018.

man. In it, the actor addresses Russia's efforts to interfere in the 2016 presidential election and cautions, "we have been attacked. We are at war."[240] Two days later, an online group that has since been revealed as an IRA account by the U.S. Congress, AgitPolk, initiated a campaign in response to Freeman's video under the slogan "#StopMorganLie."[241] The group accused Freeman of "manipulat[ing] the facts of modern Russian history and openly [slandering their] country," and announced the launch of a campaign in response to his video.[242]

The Digital Research Forensics Lab's analysis reveals how the campaign employed a labyrinth of actors and platforms to propagate the desired narratives and to potentially suppress alternative narratives. First, bot and sockpuppet accounts were used to amplify the hashtag on social media platforms Twitter and VKontakte (VK). Only hours later, official Russian government Twitter accounts such as that of the consulate general weighed in, posting memes that attempted to denigrate Freeman's credibility. This activity was followed by an RT article, which featured the same hashtag as the social media posts. The RT article was picked up by several other niche outlets.[243] While this analysis examines a single campaign believed to be sponsored by Russia, it nevertheless illustrates how various actors masquerading as independent from one another and from the Kremlin are used in concert.[244]

---

[240] Committee to Investigate Russia, "Morgan Freeman Warns Russia Is Waging War on the U.S.," September 18, 2017.

[241] Digital Forensics Research Lab, 2018.

[242] Digital Forensics Research Lab, "Putin's Online Cheerleaders: The 'Patriots' Behind Pro-Kremlin, Anti–Morgan Freeman Memes," The Atlantic Council, October 17, 2017.

[243] Digital Forensics Research Lab, 2018. For the RT article referenced, see RT, "#StopMorganLie: Twitterati Disappointed in Freeman After His 'War with Russia' Video," September 20, 2017.

[244] Digital Forensics Research Lab, 2018.

Effectiveness of Russia's Efforts

Much public debate and scholarship has been devoted to identifying and characterizing Russian social manipulation efforts. These discussions draw conclusions about the Russian threat, yet few address the issue of effectiveness and ask, what, if anything, have alleged Russian efforts accomplished; and how successful has Russia been in achieving its objectives? Those that do discuss effectiveness often focus on the number of rubles spent, or the sums of tweets produced, but these criteria may not be the most illustrative when seeking to understand whether Russian efforts worked. This section offers an initial discussion of effectiveness. In Chapter Five, we will assess detailed outcome evidence for Russian social manipulation efforts in the United States and Europe.

How Russia Measures Effectiveness

First, it is important to understand how Russia measures the effectiveness of its social manipulation efforts. Though it is impossible to definitively know, publicly available information may offer some clues. Leaked documents allegedly tied to the IRA suggest that, at least initially, the organization may have focused on the output rather than the outcome of its efforts:

> The documents show instructions provided to the commenters that detail the workload expected of them. On an average working day, the Russians are to post on news articles 50 times. Each blogger is to maintain six Facebook accounts publishing at least three posts a day and discussing the news in groups at least twice a day. By the end of the first month, they are expected to have won 500 subscribers and get at least five posts on each item a day. On Twitter, the bloggers are expected to manage 10 accounts with up to 2,000 followers and tweet 50 times a day.[245]

A former employee's account of her time at the IRA offers additional insight into the criteria possibly used to measure success:

---

[245] Seddon, 2014a.

> Management was obsessed with statistics—page views, number of posts, a blog's place on LiveJournal's traffic charts—and team leaders compelled hard work through a system of bonuses and fines. . . . Over [her] two shifts she had to meet a quota of five political posts, 10 nonpolitical posts and 50–200 comments on other workers' posts.[246]

Though this appears to validate the IRA's focus on internally generated output, it indicates that its management also valued performance based on external benchmarks, such as the number of times its work was viewed by users. That said, other evidence suggests that IRA managers may have different expectations for the organization's different departments.

An IRA defector assigned to the foreign desk—viewed as an elite group in the organization—recounted that his initial goal was not to attain a specific number of posts, but rather to influence opinions. He noted that his department valued the reaction to the content it produced and disseminated and measured this reaction by counting the number of likes the content received and assessing the conversations it provoked.[247] However, over time, he noted that IRA management began "focusing more on the quantity than the quality of their output."[248]

The tranche of leaked documents associated with the IRA also describes efforts by freelance sockpuppets, whose managers gave "them ratings based on the efficiency and 'authenticity,' as well as the number of domains they post from."[249] The 2018 U.S. indictment against the IRA confirms that IRA management regularly evaluated the "authenticity" of its employees' content and provided feedback on it.[250]

---

[246] Chen, 2015.

[247] Kotlyar, 2017.

[248] "An Ex St. Petersburg 'Troll' Speaks Out: Russian Independent TV Network Interviews Former Troll at the Internet Research Agency," 2017.

[249] Seddon, 2014a.

[250] "United States of America v. Internet Research Agency LLC, [et. al]," p. 15.

Similarly, a Department of State official told us that entrepreneurs trolling on behalf of the Russian government are likely paid based on the amount of content they produce and disseminate (e.g., by the message, blog post, etc.).[251] Thus, entrepreneurs may be incentivized to maximize output in an effort to procure larger contracts later.[252]

Russia's other instruments of social manipulation may use different metrics to measure effectiveness. A Russian journalist informed us that RT leadership appeared to judge its performance by the volume of articles in the West citing or covering its work. The leadership reportedly collected press clippings of stories in Western news outlets featuring or mentioning RT and Sputnik.[253] The journalist mentioned that they were frequently required to translate articles mentioning RT into Russian when they worked for a different news agency under the same roof.[254] Likewise, RT leadership allegedly used its increased press in the West as a justification for preserving its funding when faced with sizeable budget cuts in late 2015 and early 2016.[255]

Thus, based on an assessment of the publicly available information—which is admittedly very slim—in some cases, Russia and its proxies appear to focus on the outputs of its social manipulation efforts rather than their outcomes. Granted, they could use other metrics that are not apparent from information that is publicly available. This approach is understandable, given the challenges in accurately measuring the impact of such efforts on opinions, attitudes, and behaviors.

The effectiveness of Russian social manipulation efforts is tied to the government's objectives, and whether these objectives have been met. Earlier in the chapter, we drew inferences about Russia's goals based on its public statements and other evidence, but these are both broad and imperfect. Therefore, we examine Russian efforts through different lenses based on different criteria below.

---

[251] In-person interview with Department of State official 010, October 4, 2017.

[252] In-person interview with Department of State official 010, October 4, 2017.

[253] Phone interview with Russian journalist 27, October 31, 2017.

[254] Phone interview with Russian journalist 27, October 31, 2017.

[255] Phone interview with Russian journalist 27, October 31, 2017.

Outputs and Budgets

Much of the public discourse on Russian social manipulation efforts discusses the magnitude of output or amount of funding devoted to social manipulation efforts.[256] According to recent figures released by Twitter, over 50,000 automated accounts linked to Russia were operating during the 2016 U.S. election.[257] Facebook has said that Russia likely sponsored over 3,000 paid advertisements on its platform during the same period.[258] From the Russian perspective, incentives were aligned to drive maximum output at the IRA. The number of languages Sputnik operates in is also cited as indicators of the threat it poses. Though these figures are significant, the existence of content does not guarantee its viewing by or interaction with the target audience.

RT's budget has reportedly grown from approximately $30 million at its founding in 2005 to $300 million in 2010 and $323 million in 2017.[259] The alleged IRA documents leaked by Anonymous International in 2014 indicate the organization's budget was over $10 million in 2014.[260] The organization's funding appears to have increased by fall 2016, according to the 2018 U.S. indictment, though the figures listed are part of a broader effort that includes domestic social manipulation projects.[261] Additionally, according to U.S. congressional testimony given by Facebook's general counsel, the IRA spent approximately $100,000 on Facebook and Instagram ads targeting the U.S.

---

256 Josh Halliday, "BBC World Service Fears Losing Information War As Russia Today Ramps Up Pressure," *The Guardian*, December 21, 2014.

257 Glaser, 2018.

258 Colin Lecher, "Here Are the Russia-Linked Facebook Ads Released by Congress," *The Verge*, November 1, 2017.

259 For the first two budget figures, see Simon Shuster, "Inside Putin's On-Air Machine," *TIME*, March 5, 2015. For the third figure, see Steven Erlanger, "What is RT?" *New York Times*, March 8, 2017.

260 Seddon, 2014a. This figure is based on the assumption that spending continued at the rate of spending between December 2013 and April 2014.

261 "United States of America v. Internet Research Agency LLC [et al.]," pp. 5–6.

electorate between June 2015 and August 2017.[262] It is important to note that, while it is implied that the IRA is sponsored by the Russian government, neither the 2018 indictment nor the 2017 U.S. intelligence report explicitly validates this connection. The 2018 House Permanent Select Committee on Intelligence report on Russian Active Measures does acknowledge that the IRA has "ties to the Kremlin."[263]

When compared with Soviet spending on social manipulation efforts, which amounted to several billion dollars annually, today's figures appear somewhat modest. Granted, publicly available figures may represent only a sliver of total Russian spending on such efforts, the remainder of which could be obscured through shell organizations, such as Prigozhin's Concord. In contrast with the Soviet era, today's technologies might facilitate more nuanced and narrow targeting of specific audiences and may be more cost effective, allowing Russia to do more with less. That said, as in the Soviet era, the amount of funding spent on Russian social manipulation efforts may not necessarily be correlated with their effectiveness.

Audience Exposure

Some discourse on Russian efforts cites the number of people that have been exposed to social manipulation as evidence of its effectiveness. RT alleges that a survey conducted in 2015 found that its television network was viewed by 70 million people every week.[264] Yet, according to 2015 ratings by Nielsen Media Research, RT was not in the top 94 channels in the United States. Likewise, Britain's Broadcast Audience Research Group found that RT captured only 0.04 percent of British viewers in December 2016.[265]

---

[262] Colin Stretch, General Counsel, Facebook, "Hearing Before the United States Senate Select Committee on Intelligence," testimony, November 1, 2017, p. 4.

[263] U.S. Congress, "Report on Russian Active Measures," House Permanent Select Committee on Intelligence, March 22, 2018, p. 32.

[264] RT, "RT Watched by 70mn Viewers Weekly, Half of Them Daily—Ipsos Survey," March 10, 2016.

[265] "RT's Propaganda Is Far Less Influential Than Westerners Fear," *The Economist*, January 19, 2017.

Facebook estimates that 11.4 million people in the United States viewed at least one of the IRA-sponsored ads between 2015 and 2017, and that 126 million Facebook users may have viewed content propagated by the IRA on this platform at some point during this period.[266] Other independent analyses have identified "2.5 million recorded interactions with posts from [Instagram] accounts, as well as 145 million likely interactions with people who had passively viewed them."[267] That said, other researchers questioned these figures, noting that user views "could have been created by illegitimate and automated accounts and that there was no way of telling how many of the 'impressions' were from actual Americans."[268] It is also possible that others who may not have come in contact with the content directly heard about the content or the campaign through secondary sources, such as news reporting.

Impressions, which are Facebook's measure of the number of times that content appears on a user's screen, may not be reliable indicators of audience exposure to a message, let alone its influence. The same is true for any platform; users can passively click through content without actively engaging with it, yet this "interaction" is counted nonetheless. Behaviors such as following, retweeting, and liking require more user agency and might therefore be more useful barometers of audience internalization of messages. Yet this may not be the case, as discussed below.

As scholars studying public opinion have found, exposure to a message is often insufficient when attempting to affect opinion; the target audience must also understand it. Recipients must interpret the message as its sender intended.[269] Even then, another hurdle remains. The message is likely to be filtered through audiences' existing biases. Thus, while Russian messages may have reached large audiences, the audiences may not have been influenced.

---

[266] Stretch, 2017, p. 5.

[267] Sheera Frenkel, "'Troll Farms' Are Relentless at Sharing on Instagram," *New York Times*, December 18, 2017.

[268] Frenkel, 2017; Gorwa and Guilbeault, 2018, p. 17.

[269] George C. Edwards III, *On Deaf Ears: The Limits of the Bully Pulpit*, New Haven, Conn.: Yale University Press, 2003, p. 187.

Audience Engagement and Popularity

In the social media or online context, popularity is most often measured using easily quantifiable metrics indicating user consumption (the number of page views, video views, shares, likes, content garners, or the length of time a video is viewed) and user popularity (number of followers or friends a user has, number of likes or shares the content has generated). "Higher numbers" of social media metrics "are widely taken to imply more legitimacy, popularity, visibility, and influence."[270] Data on these metrics are readily accessible to operators through a platform's application programming interface (API), making them easy to study.

Figures released by Twitter from the 2016 U.S. presidential election project that over 65,000 users in the United States followed or retweeted a tweet from one of the Russia-linked accounts during the election.[271] An independent analysis found that tweets from IRA accounts earned 2.1 million retweets and almost 1.9 million favorites.[272]

Yet several potential issues arise when using these criteria as indicators of effectiveness. First, popularity online may not equate to favorability in the eyes of the target audience. Scholars in the market research discipline found that "'liking' a brand has no positive direct effect on consumer attitudes or purchases; if anything, its effect is detrimental."[273] This finding was reinforced by a series of studies examining the effects of "likes" on social media, which found little evidence to suggest that liking a brand on social media affects users' purchasing behavior related to that brand.[274] Though audience approaches to con-

---

[270] Nancy K. Baym, "Data Not Seen: The Uses and Shortcomings of Social Media Metrics," *First Monday*, Vol. 18, No. 10, October 7, 2013.

[271] Glaser, 2018.

[272] Ben Popken, "Russian Trolls Went on Attack During Key Election Moments," NBC News, February 13, 2018.

[273] Leslie K. John, Oliver Emrich, Sunil Gupta, and Michael I. Norton, "Does 'Liking' Lead to Loving: The Impact of Joining a Brand's Social Network on Marketing Outcomes," *Journal of Marketing Research*, Vol. 54, No. 1, 2017a, p. 4.

[274] Leslie K. John, Daniel Mochon, Oliver Emrich, and Janet Schwartz, "What's the Value of a Like?" *Harvard Business Review*, March–April, 2017b.

sumer goods may be different from audience approaches to political or social beliefs, this research may offer some insight into an area currently absent of applicable research. Additionally, social media metrics measuring popularity or audience engagement also may not capture a representative sample of the target audience.[275]

Second, assessments of popularity can be misleading. RT claims it is one of the most popular news outlets on YouTube. While it may garner the most "views, subscribers, and 'engagement' such as comments or likes," much of its most popular content does not appear to convey the government's messaging.[276] For instance, RT's most viewed video is a human-interest story featuring a former radio host turned homeless man.[277] In an investigation conducted by the *Daily Beast* of RT's 100 most watched videos between 2010 and 2015, those featuring extreme weather, accidents, and crime received 81 percent of the channel's views. Much of this content was purchased from a third party.[278] According to a study measuring RT's impact on YouTube viewers, the authors conclude

> It remains difficult to assess, however, whether or not RT's anti-Western messaging is actually having an effect. [. . .] Further efforts to more concretely measure viewer attitude change are therefore essential to understanding the impact of RT's news coverage. Though we have examined RT's channel-dependent strategy and corresponding success in gaining viewership, it remains to be seen what the effect actually is on viewers once they watch RT's coverage of events."[279]

---

[275] Baym, 2013.

[276] Daisuke Wakabayashi and Nicholas Confessore, "Russia's Favored Outlet Is an Online News Giant. YouTube Helped," *New York Times*, October 23, 2017.

[277] Wakabayashi and Confessore, 2017.

[278] Bodner, Kupfer, and Jardine, 2017.

[279] Nelson, Orttung, and Livshen, 2016, p. 9.

Legitimization of Contrived Messages

One aim of both U.S. and Soviet social manipulation efforts during the Cold War was the legitimization of their messages through either opinion makers or legitimate media outlets. The former CIA analyst with whom we spoke noted that in some cases the United States measured the effectiveness of its information efforts during the Cold War by observing where its narratives were echoed.[280] In other words, if his department wrote a pamphlet or article communicating a specific message, and a prominent leader of a group reiterated the same message in an unrelated forum, this was seen as a success. The analyst also acknowledged, however, that this approach did not provide a true measure of effectiveness in influencing attitudes or behaviors.[281]

In this area, expert Keir Giles asserts that Russia has indeed been effective. He explains that in the early stages of the Ukraine conflict, the reports of journalists identifying Russian troops in eastern Ukraine were questioned and often silenced because editors believed, and repeated, the Russian leadership's public denials.[282] Giles argues:

> This led at first to striking success in penetration of narratives, which contributed powerfully to Russia's ability to prosecute operations against Ukraine in the early stages of the conflict with little coordinated opposition from the West. The fact that the EU continued to find itself unable to refer publicly to the presence of Russian troops in Ukraine for almost a year denoted a broader inability to challenge the Russian version of events—without which a meaningful response was impossible. Early media coverage of the conflict made it "apparent, in short, that some interlocutors had swallowed whole some of the cruder falsifications of Russian propaganda."[283]

---

[280] In-person interview with former CIA analyst 024, November 20, 2017.

[281] In-person interview with former CIA analyst 024, November 20, 2017.

[282] Keir Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, London: Chatham House, March 2016a, p. 31.

[283] Giles, 2016a, p. 31, quoting John Besemeres, "Russian Disinformation and Western Misconceptions," in Besemeres, *A Difficult Neighbourhood: Essays on Russia and East-Central Europe Since World War II*, Canberra: Australian National University Press, 2016.

Policy Changes

Russian social manipulation efforts, or the perceived threat of such efforts, have spurred policy changes across Europe and in the United States in attempts to shield or inoculate populations from Moscow's influence. In 2014, the Ukrainian government banned 14 Russian television channels from its cable networks, citing their "broadcasting propaganda of war and violence" as the motivation for its action.[284] Three years later, Kyiv announced that it would block Russian-owned internet sites and social media platforms, including VK, Odnoklassniki, Mail.ru, and Yandex.[285] Finland sponsors classes educating "border guards, child protection agencies, educators, and civil servants how to respond to propaganda."[286] The U.S. government has pressured RT America to register as a foreign agent under the Foreign Agents Registration Act (FARA).[287] Individuals believed to be involved in Russian social manipulation efforts, such as Dmitry Kiselev, have been placed on the European Union's individual sanctions list.[288]

These describe only some of the offensive and defensive policy actions taken by the West in response to Russian social manipulation efforts. Although Moscow can claim to have motivated such policy actions, it is questionable whether these are positive developments for Russia.

Expenditures of Western Resources

Some have argued that the alleged Russian efforts have been effective in that they have distracted policymakers and forced governments to

---

[284] "Ukraine Bans Russian TV Channels for Airing War 'Propaganda,'" Reuters, August 19, 2014.

[285] "RT's Propaganda Is Far Less Influential Than Westerners Fear," 2017.

[286] Linda Kinstler, "How to Survive a Russian Hack: Lessons from Eastern Europe and the Baltics," *The Atlantic*, February 2, 2017.

[287] Aron Mate, "RT Was Forced to Register as a Foreign Agent," *The Nation*, November 16, 2017.

[288] Natalka Pisnia, "Why Has RT Registered As a Foreign Agent in the US?" BBC News, November 15, 2017.

expend precious time and resources (financial and labor) to countering the threat.[289]

Changes in Audience Opinions, Attitudes, Beliefs, and Behaviors

If, as we suspect, at least one of Russia's objectives is to engender support for its own interests and discredit its targets in the eyes of its target audiences, success would involve a change in opinions, attitudes, beliefs, and behaviors in some audiences, and the confirmation thereof in others. For those whose existing opinions and attitudes are consistent with Russian messaging, success likely means sustaining or deepening these opinions and attitudes. For those whose existing opinions and attitudes are inconsistent with Russian messaging, success likely means influencing or altering these attitudes and opinions.

This does not necessarily mean attitude, opinion, belief, or behavior change in mass audiences. If Russia seeks to influence attitudes, opinions, beliefs, and behaviors to engender specific policy outcomes—like the United Kingdom's departure from the European Union or the popular votes in the U.S. swing states of Wisconsin, Michigan, and Pennsylvania—Russia may only have to persuade narrow audiences on the margins to accomplish this objective.[290]

Still, determining whether social manipulation efforts have resulted in attitude, opinion, belief, or behavior change is an incredibly complex task, particularly outside of a controlled setting. The audiences Russia likely seeks to influence live in the real world and are constantly bombarded by influences from various sources. Isolating the effect of any one of these inputs in this setting is difficult. Even a basic examination of this requires a baseline assessment measuring attitudes of the target audience on the specific issues that Russia seeks to influence before the Russian efforts, and a posttest on the same issues. It is very difficult to mitigate the effects of intervening variables and to identify causation or even correlation in this setting. What is

---

[289] Dalibor Rohac, "Cranks, Trolls and Useful Idiots," *Foreign Policy*, March 12, 2015.

[290] Kragh and Asberg, 2017, p. 807.

more, social science scholarship has debated whether attitudes are reliable indicators of behavior.[291]

Given the information available, we cannot determine whether Russian social manipulation efforts have been effective in influencing attitude, opinion, belief, or behavior change in their target audiences. Humans are inclined toward attitude preservation, particularly with attitudes that are deeply held, like those in the political realm. If Russia has been successful in such efforts, it is because it navigated our own internal gatekeepers.

Conclusions

Our examination of Soviet-era social manipulation efforts reaffirmed the oft-stated assertion that today's efforts draw inspiration from their Cold War forerunners. We observed similarities in the core principles of both Soviet and Russian social manipulation—e.g., the use of information to discredit adversaries and/or further interests—and in the practices used by both. Yet despite decades of Soviet attempts to effect change through social manipulation efforts, it is not clear they were ever successful at achieving this objective.

We learned that the Russian social manipulation system may not be a system at all, but perhaps an assortment of official organizations, proxies, patriots, and "useful idiots." Likewise, it appears that not all efforts are directed by the highest levels of government. In some cases, the efforts may be directly affiliated with the Kremlin or under its direct control. RT and other actors executing such efforts appear to be given broad guidance on messaging. In other cases, there appears to be a mélange of contracts with semiaffiliated actors and self-directed efforts motivated by gold, glory, or parochial interests. It seems these

[291] Phone interview with former military information activities expert 022, November 2, 2017; Alice H. Eagly and Shelly Chaiken, "Attitude Structure and Function," in D. T. Gilbert, S. T. Fiske, and G. Lindzey, eds., *The Handbook of Social Psychology* (4th ed.), New York: Oxford University Press, 1998, pp. 269–322; Richard T. LaPiere, "Attitudes vs. Actions," Social Forces, Vol. 13, No. 2, 1934, pp. 230–237.

actors take their cues from the Kremlin's publicly stated positions on various issues and operate based on these signals.

Many mysteries remain. Our work has demonstrated how little the policymaking, scholarly, and analytical fields know about Russian social manipulation. More may be known in the classified setting. Yet with the centrality of this issue in today's public discourse, it is important that those being targeted by such efforts have access to evidence-based insights about the efforts.

Perhaps the most important missing piece of information pertains to Russia's effectiveness. Understanding whether and how Russian target audiences have been influenced is as important as identifying the perpetrators and their means. Our questioning of success should not be interpreted as a determination that Russian attempts have been ineffective in influencing opinions, attitudes, beliefs, or behavior. Instead, we believe that this issue merits further inquiry.

If Russia does, in fact, use reaction as a measure of its success, as some suggested to us, it could reasonably interpret its recent efforts in the West as victories. Western reactions could incentivize future Russian social manipulation efforts, further underscoring the need for additional examinations of the effectiveness of its efforts.

CHAPTER FOUR

Hostile Social Manipulation: Chinese Activities

Under the Chinese Communist Party (CCP), the People's Republic of China (PRC) has a long-standing and continually evolving approach to using information to achieve political goals. Yet in contrast with Russia's clear use of social media for harmful effects outlined in the preceding chapter, there is limited evidence that China has so far engaged in similar hostile social manipulation of Western social media. The strongest evidence of malign Chinese activities on social media has concerned those targeted at Taiwan on non-Western platforms, which are covered in this chapter. To better anticipate potential future hostile social manipulation by China, this chapter presents a broader overview of China's manipulation of public opinion on social media abroad, which is mostly accomplished through propaganda (宣传). The chapter will also cover China's approach to social media at home, since many of China's foreign operations are extensions of domestic activities.[1]

[1] For academic studies of Chinese ideology and propaganda, see, for example, Anne-Marie Brady, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China*, Lanham, Md.: Rowman and Littlefield Publishers, 2008; Anne-Marie Brady, ed., *China's Thought Management*, New York: Routledge, 2012; Daniel C. Lynch, *After the Propaganda State: Media, Politics, and 'Thought Work' in Reformed China*, Stanford, Calif.: Stanford University Press, 1999. In conducting this study, RAND leveraged open-source primary and secondary source information in Chinese and English and conducted a small number of face-to-face interviews with subject-matter experts knowledgeable about China's propaganda and social media operations.

This chapter also draws on Nathan Beauchamp-Mustafaga and Michael Chase, *The Chinese Military and Social Media: A New Tool for Peacetime and Wartime Propaganda at Home and Abroad*, Washington, D.C.: John Hopkins SAIS, forthcoming.

In recent years, China's efforts to spread propaganda, shape foreign views of China, and extend Beijing's influence have included using internet-based social media platforms. While many of China's efforts to influence foreign audiences via social media have to do with ensuring regime security at home, some focus on developing the capacity to achieve Chinese foreign policy goals abroad. According to the 2017 U.S. National Security Strategy:

> America's competitors weaponize information to attack the values and institutions that underpin free societies, while shielding themselves from outside information. They exploit marketing techniques to target individuals based upon their activities, interests, opinions, and values . . . [and] disseminate misinformation and propaganda.[2]

More recently, in September 2018, President Trump stated that the Chinese government was interfering in the 2018 midterm elections.[3] This statement was supported by a briefing by a senior National Security Council official and in a speech by Director of National Intelligence Dan Coats.[4] However, the core focus of this claim is apparently the Chinese government's paid propaganda inserts in newspapers, not malign activities on social media. This leaves open the possibility such activities are being conducted on social media, but no specific evidence has so far been presented.

To what extent has China employed social media to disseminate propaganda and manipulate public opinion abroad, and with what goals in mind? How successful have Chinese authorities been in their efforts? This chapter examines these two key questions. To answer these questions, we interviewed experts on Chinese censorship, propaganda, and social media; conducted a broad review of Chinese-language sources;

---

2 *National Security Strategy of the United States of America*, Washington, D.C.: The White House, December 2017, pp. 34–35.

3 Mark Landler, "Trump Accuses China of Interfering in Midterm Elections," *New York Times*, September 26, 2018.

4 David Nakamura and Ellen Nakashima, "Without Offering Evidence, Trump Accuses China of Interfering in U.S. Midterm Elections," *Washington Post*, September 26, 2018.

and leveraged the most recent Western literature on China's foreign policy goals, views of the internet, and approach to social media. As in the previous chapter on Russian approaches to hostile social manipulation, this chapter will first provide a historical context, followed by discussions of doctrine, strategies, actions, and effectiveness. The chapter as a whole is structured slightly differently to reflect the main themes that emerged from our survey of Chinese programs, but it covers the same four primary focus areas: recent history, goals and objectives, tools employed, and government structure.

History: China's Approach to Social Manipulation

As author and prominent Chinese social critic Murong Xuecun has noted, the CCP has used ideology and propaganda as governing tools "since the People's Republic was established in 1949," and this can even be dated to the CCP's founding in 1921.[5] Kristin Shi-Kupfer, writing for the Mercator Institute for China Studies, characterizes the Chinese system of rule as "governance through information control," and argues that "the Chinese government has recognized that it needs a comprehensive social media strategy if it is to win the 'battle for public opinion.'"[6] For China, foreign policy begins at home, and the majority of the PRC's efforts over recent decades to use information for political goals and to shape public opinion through propaganda has been focused first on defending the regime and secondarily on swaying foreign audiences.[7]

---

5 Murong Xuecun, "The New Face of Chinese Propaganda," *New York Times*, December 20, 2013.

6 Kristin Shi-Kupfer, "Governance Through Information Control," *China Monitor*, No. 26, Mercator Institute for China Studies, January 19, 2016. Moreover, as one analysis has pointed out, "The Party [has recognized] that social media, carefully managed, can help spread its messages effectively in the country with the world's largest number of internet users"; Anil Azad Pandey, "How the Chinese Communist Party Is Using Social Media to Win Friends and Influence People," *OZY*, October 25, 2017.

7 For an overview of recent work on Chinese influence operations targeting New Zealand, Australia, Germany, and the European Union, respectively, see Anne-Marie Brady, *Magic*

Nevertheless, the Chinese government sees itself in perpetual competition, or even constant war, with the United States and wider Western community in the ideological space. Although China's rhetoric has changed from the dramatic confrontational language of Mao Zedong's day, current President Xi Jinping has strongly reinforced a quiet but persistent belief among many Chinese thinkers that assumes China is in a zero-sum ideological competition with the West. From a Chinese perspective, the U.S. government is already engaged in a massive propaganda campaign against China and other countries, but Washington simply obfuscates the true intent by calling it "strategic communications."[8] Substantial research suggests that the Color Revolutions and Arab Spring fueled the CCP leadership's growing concern over the battle of hearts and minds and brought back memories of the fall of the Soviet Union.[9] In October 2011, then-President Hu Jintao said, "We must clearly see that international hostile forces are intensifying the strategic plot of Westernizing and dividing China, and ideo-

---

Weapons: China's Political Influence Activities Under Xi Jinping, Washington, D.C.: Wilson Center, 2017; Clive Hamilton, *Silent Invasion: China's Influence in Australia*, Richmond, Australia: Hardie Grant, 2018; "China's Operation Australia," *Sydney Morning Herald*, 2017; Didi Kirsten Tatlow, "China Reaches Into the Heart of Europe," *New York Times*, January 25, 2018; Thorsten Benner, Jan Gaspers, Mareike Ohlberg, Lucrezia Poggetti, and Kristin Shi-Kupfer, "Authoritarian Advance: Responding to China's Growing Political Influence in Europe," Global Public Policy Institute and Mercator Institute for China Studies, February 2018.

8 Shi Anbin and Peiyan Wang, "Stealth Propaganda: Concepts Evolution, Strategy" ["隐性宣传：概念•演进•策略"], *International Communications*, January 2016.

9 For an overview of China's lessons learned from the collapse of the Soviet Union, see David Shambaugh, *China's Communist Party: Atrophy and Adaptation*, Washington, D.C.: Woodrow Wilson Center Press, 2009; William Wan, "In China, Soviet Union's Failure Drives Decisions on Reform," *Washington Post*, March 23, 2013; James Palmer, "What China Didn't Learn from the Collapse of the Soviet Union," *Foreign Policy*, December 24, 2016. For an authoritative article analyzing the danger of Western social media (Twitter, Facebook, and Blackberry phones) to social stability and their role as a tool for the U.S. government to interfere in other countries based on the Arab Spring, see Wu Zaiping, "The Social Challenges and Responses to New Media" ["新媒体的社会挑战与应对"], *Journal of the Party School of the Central Committee of the C.P.C*, October 2012.

logical and cultural fields are the focal areas of their long-term infiltration"; Hu's prescription, in part, was to improve Chinese soft power.[10]

In April 2013, shortly after taking power, President Xi asserted more work was to be done, saying in a secret document that "Western forces hostile to China and dissidents within the country are still constantly infiltrating the ideological sphere" and specifically asserting that regime opponents "have stirred up trouble about disclosing officials' assets, using the Internet to fight corruption, media controls and other sensitive topics, to provoke discontent with the party and government."[11] Xi called for the CCP to "conscientiously strengthen management of the ideological battlefield," including "strengthen guidance of public opinion on the Internet [and] purify the environment of public opinion on the Internet."[12] As China deepens its engagement with the world, this struggle for controlling information about the CCP has extended to global public opinion, and the internet is only the latest battlespace.

Thus, while some observers hoped that the widespread adoption of personalized networked information technology, most commonly in the form of internet-enabled cellular phones with access to social media websites, might undercut the Party's high degree of control over information, Chinese authorities not only managed to rise to the challenge

---

10 Hu Jintao, "Resolutely Follow the Cultural Development Path of Socialism with Chinese Characteristics, Work to Build a Socialist Strong Culture Country" ["坚定不移走中国特色社会主义文化发展道路努力建设社会主义文化强国"], *Seeking Truth*, January 1, 2012; Edward Wong, "China's President Lashes out at Western Culture," *New York Times*, January 3, 2012; Evan Osnos, "China's Culture Wars," *New Yorker*, January 5, 2012; Damien Ma, "Beijing's 'Culture War' Isn't About the U.S.—It's About China's Future," *Atlantic*, January 5, 2012; "China's New Cultural Revolution," *Wall Street Journal*, January 4, 2012.

11 Chris Buckley, "China Takes Aim at Western Ideas," *New York Times*, August 19, 2013. For translation, see "Document 9: A ChinaFile Translation," ChinaFile, November 8, 2013.

12 Xi mirrored this tone in his speech to the 19th Party Congress in October 2017: "We will [. . .] strengthen the penetration, guidance, influence, and credibility of the media. We will provide more and better online content and put in place a system for integrated internet management to ensure a clean cyberspace. [. . .] We must oppose and resist various erroneous views with a clear stand" (Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," speech to the 19th National Congress of the Communist Party of China, via Xinhua, October 18, 2017).

but also found that they could use such new technologies to expand their influence. In retaining substantial control over information flows among the Chinese populace, China has built up one of the world's most sophisticated capacities for human- and machine-enabled keyword blocking and censorship and has also used such new technologies and platforms in innovative ways to shape domestic and foreign information flows related to China. Reflecting this, in November 2017 the U.S. nongovernmental organization Freedom House noted that, on the basis of Beijing's widespread content blocking, content removal, and content fabrication regimes, "for the third consecutive year, China was the world's worst abuser of Internet freedom."[13]

The next section describes China's foreign policy doctrine, including its goals for information operations. The following section lays out China's strategies for who manages social media and online messages to support the regime. The chapter then examines actual instances of Chinese information operations through social media. The chapter continues with an analysis of how effective China has been and concludes with an assessment of the implications.

Doctrine: China's Goals for Foreign Policy and Information Operations

Chinese foreign policy has, in recent years, adopted two key postulates, one being the importance of defending China's *core interests* (核心利益), and the other and more recent formulation centered on achieving *the great rejuvenation of the Chinese nation* (中华民族伟大复兴), often referred to more colloquially as realizing the *China dream* (中国

[13] *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*, Washington, D.C.: Freedom House, 2017. As one interviewee we spoke with noted, "The [Chinese] state's ability to collect, analyze, target and deploy data [is] now far greater than that of [Chinese] society" (RAND Interviewee #3). Another of the subject-matter experts we spoke with for this study pointed out that, "In its ideal world, China wants everything that is said about China internationally to follow what is said about China inside its borders," giving the regime total information control (RAND Interviewee #1).

梦).[14] These two organizing precepts parallel fairly closely the notions of defensive and offensive realism in international relations theory, though with a considerable degree of fuzziness in delineating between the more defensive approach to security policy (*core interests*) and the more aggressive, ambitious, or offensive security strategy (the *China dream*).[15]

The adoption by China of the *core interests* organizing framework in the late 2000s centered on three basic goals: preserving China's basic state system and national security (维护基本制度和国家安全); protecting China's sovereignty and territorial integrity (主权和领土完整); and continuing the stable development of China's economy and society (经济社会的持续稳定发展).[16] In practice, the first core interest is largely consonant with the preservation of the ruling status of the CCP, while the second and third interests serve as means to this end through the retention of control over Xinjiang and Tibet; the defense of China's claims in the South and East China seas; and the prevention of Taiwan independence, leading to the island's ultimate absorption.

By contrast, the *China dream*, while necessarily entailing the retention and/or integration of territories that Chinese leaders regard as theirs, looks further afield to a more ambitious set of goals. These include domestic economic goals such as achieving the *two 100s*,[17] which are linked to the centenaries of the founding of the CCP, in 2021, and of the PRC itself, in 2049; reducing social inequality; cleaning up the environment; developing national morals; and achieving the

---

[14] "Xi Calls for Persistently Pursuing Chinese Dream of National Rejuvenation," *China Daily*, September 26, 2017.

[15] Chinese military theorists further complicate such matters by talking in terms of *active defense* (积极防御) and preemptive counterattack (先发制人的反击), concepts that blur the lines between cause and effect so as to justify China's own efforts to take the initiative in shaping its environment or engaging its adversaries during peacetime or on the battlefield.

[16] Michael D. Swaine, "China's Assertive Behavior, Part One: On 'Core Interests,'" *China Leadership Monitor*, No. 34, September 2010.

[17] The *two 100s* refers to the economic goals of becoming *a moderately well-off society* (小康社会) by 2021 (the centenary of the founding of the CCP) and of completing the dream of national rejuvenation by 2049 (the 100th anniversary of the founding of the PRC).

strong nation dream (强国梦) of returning the country to a position of regional and global preeminence.[18] In his work report to the 19th Party Congress in October 2018, President Xi expanded upon these formulations. He offered a timeline that would see China accomplish the basics of *socialist modernization* (社会主义现代化) between 2020 and 2035, with the period from 2035 to 2049 dedicated to transforming the country into "a global leader in terms of comprehensive national power and international influence."[19]

Regional and Global Policy Objectives

Working within these two parameters, China has set its top policy regional goals to include preventing Taiwan independence (as well as deterring or, if necessary, defeating any U.S. intervention on Taiwan's behalf in the event of a conflict); disrupting any real or potential U.S. and/or third country efforts to contain or constrain China's growing influence; enhancing its own ability to elicit or compel compliance with its preferred policy options (including ultimately absorbing Taiwan); and degrading and ultimately eliminating U.S. regional influence, most notably through the erosion and then severing of U.S. alliances with Australia, Japan, South Korea, the Philippines, and Thailand.[20] Globally, China seeks to *democratize* international society,

---

[18] Robert Lawrence Kuhn, "Xi Jinping's China Dream," *New York Times*, June 4, 2013.

[19] Bonnie Glaser and Matthew P. Funaiole, "Xi Jinping's 19th Party Congress Speech Heralds Greater Assertiveness in Chinese Foreign Policy," Center for Strategic and International Studies, October 26, 2017.

[20] For analyses of the goals of Chinese foreign policy over the past decade, see Susan Shirk, *China: Fragile Superpower*, Oxford, UK: Oxford University Press, 2007; Andrew J. Nathan and Andrew Scobell, *China's Search for Security*, New York: Columbia University Press, 2012; David Shambaugh, *China Goes Global: The Partial Power*, Oxford, UK: Oxford University Press, 2013; Jae Ho Chung, "China's Evolving Views of the Korean-American Alliance, 1953–2012," *Journal of Contemporary China*, Vol. 23, No. 87, 2014, pp. 425–442; Yan Xuetong, "From 'Keeping a Low Profile' to 'Striving for Achievement,'" *Chinese Journal of International Politics*, Vol. 7, No. 2, 2014, pp. 153–184; Oriana Skylar Mastro, "Why Chinese Assertiveness Is Here to Stay," *Washington Quarterly*, Vol. 37, No. 4, Winter 2015, pp. 151–170; Camilla T. N. Sørensen, "The Significance of Xi Jinping's 'China Dream' for Chinese Foreign Policy: From 'Tao Guang Yang Hui' to 'Fen Fa You Wei,'" *Journal of Chinese International Relations*, Vol. 3, No. 1, 2015, pp. 53–73; Robert S. Ross and Jo Inge Bekkevold, eds., *China in the Era of Xi Jinping*, Washington, D.C.: Georgetown University

by which Beijing means reducing U.S. preeminence in international organizations while also defending the rights of states to "choose their own social, political and economic systems" free from external criticism over any domestic human rights abuses.

At both the regional and global levels, Chinese academics, think-tank analysts, and even top leaders have highlighted the roughly 60 to 65 million overseas ethnic Chinese as target audiences to be managed as well as vectors through which to spread economic, diplomatic, and political influence.[21] For this reason, Beijing has placed an extremely high priority on acquiring influence and, wherever possible, control over the global Chinese-language media, including radio, television, print media, and online content.[22]

"Magic Weapons": China's Offensive Approach to Defense

The Party focuses on a mix of defensive and offensive information goals and the means by which to accomplish them. It seeks to delegitimize opposition to CCP rule and paint those who would criticize the Party's leadership and its ruling status as an "extremely tiny handful" (小数的小数) of "anti-China" (反华) people with "ulterior motives" (别有用心) organized by "black hands" (黑手), often in the service of "hostile foreign forces" (敌对的外国实力). At the same time, in seeking to extend China's influence, the Party's propaganda embraces a dualistic image of the PRC's growing power as simultaneously

---

Press, 2016; Robert Blackwill and Kurt Campbell, *Xi Jinping on the Global Stage: Chinese Foreign Policy Under a Powerful but Exposed Leader*, Council Special Report No. 74, New York: Council on Foreign Relations, February 25, 2016; and Adam Liff, "China and the U.S. Alliance System," *China Quarterly*, April 2017.

[21] "Xi's Secret Economic Weapon: Overseas Chinese," *Nikkei Asian Review*, April 3, 2017; "Inside China's Secret 'Magic Weapon' for Worldwide Influence," *Financial Times*, October 26, 2017.

[22] Sarah Cook, "Resisting Beijing's Global Media Influence," *The Diplomat*, December 10, 2015; Sarah Cook, "Chinese Government Influence on the U.S. Media Landscape," testimony before the U.S–China Economic and Security Review Commission, May 4, 2017.

entirely benign—characterized by a path of "peaceful development" (和平发展) and the embrace of the Five Principles of Peaceful Coexistence (和平共处五项原则)—but also inevitable and irresistible (and consequential if crossed).

In addition to blending defensive and offensive information goals, the Party pairs its efforts to exert suasion through social and other forms of media with more traditional espionage and foreign influence operations aimed at recruiting willing collaborators; leveraging "useful idiots"; and preying on, intimidating, or otherwise silencing vulnerable populations. Indeed, President Xi reportedly sees the combination of propaganda and public opinion manipulation in tandem with United Front activities as so important to the perpetuation of the CCP's power and the achievement of the regime's foreign policy goals that he made himself the head of a new bureaucratic agency, the United Front Leading Small Group (统一战线领导小组), in 2015.[23] More recently, Xi purportedly described China's United Front activities and information operations as China's "magic weapons" for achieving the country's foreign policy goals.[24]

Learning Lessons from Other Countries' Information Operations

China has learned from the experiences of other countries in the information space, most prominently the United States. Beijing, especially the military, views the latest incarnation of ideological competition—public opinion warfare—as pioneered by the U.S. military with Operation Iraqi Freedom in 2003 and its successful use of mass media to shape public and elite opinion in both the United States and Iraq.[25] In

---

[23] Gerry Groot, "The Long Reach of China's United Front Work," *Lowy Interpreter*, November 6, 2017.

[24] Brady, 2017; "Inside China's Secret 'Magic Weapon' for Worldwide Influence," 2017.

[25] For an authoritative analysis of Chinese lessons learned from Iraq, see Dean Cheng, "Chinese Lessons from the Gulf Wars," in Andrew Scobell, David Lai, and Roy Kamphausen, eds., *Chinese Lessons from Other Peoples' Wars*, Carlisle, Pa.: Strategic Studies Institute, 2011, pp. 153–200.

For a specific Chinese analysis of U.S. public opinion warfare, see Cai Huifu, Wang Lin, Sheng Peilin, Yu Qi, Liu Xuemei, and Zheng Yu, "Research into News and Public Opinion Warfare During the Iraq War," *China Military Science*, August 2003, pp. 28–34.

more recent articles, Chinese military analysts have also drawn lessons from Russia's actions in Ukraine and Syria, highlighting the importance of starting information operations before political or military actions, as well as the benefits of going on the offensive to counter Western narratives, though these articles do not touch specifically on social media.[26] Other, broader articles have covered ISIS' use of social media for recruitment and the role of social media in the United States' war on ISIS, Japan's foreign propaganda work under Prime Minister Shinzo Abe, and Germany's use of social media.[27]

We found no authoritative articles drawing substantive lessons for future application from Russia's interference in the 2016 U.S. election, in contrast with extensive analysis and lessons learned from Russia's activities in Ukraine and Syria.[28] Most articles that did address allegations of Russian interference presented neutral or negative views, focusing on the security risks to computer systems, though such technical analysis of how "micro-propaganda" and misinformation spread through U.S. social networks would be applicable to potential Chinese influence operations in the future.[29] Early Chinese military analysis

---

[26] Zhu Ningning, "An Analysis of Russia's Unfolding of Media Warfare Tactics amid the Turbulent Political Situation in Ukraine," *Military Correspondent*, May 2014; Li Qiaoming, "Analysis of Modern Warfare Development Based on Russia's Two Conflicts," *PLA Daily*, August 16, 2016; Wang Jichang, "Main Experience of Russia's Military Operations in Syria," *China Military Science*, March 2016, pp. 119–126.

[27] Huang Dahui, "Analyzing the Abe Government's Foreign Propaganda Strategy" ["试析安倍政府的对外宣传战略"], Contemporary International Relations, June 2017; Zhou Yang, "Examination of Social Media Actions in U.S. Strikes on ISIS" ["美军打击ISIS的社交媒体行动探索"], *Military Correspondent*, July 2017; Chen Zheng, "Analysis of Information on Social Media for German Audience" ["德国受众社交媒体获取信息情况分析"], *International Communications*, August 2013; Bao Yu, "The Political Network Marketing Strategies of Islamic State Towards Western Countries," *Journal of Jiangnan Social University*, June 2016, pp. 17–21.

[28] Instead, most articles on the topic covered the events and even the negative consequences of stricter U.S. counterpropaganda rules on Chinese propaganda work. See Xu Shaomin, "Insights into the Impact of the Proliferation of Fake News in the United States and Europe on China's Public Diplomacy" ["欧美假新闻泛滥对我国开展公共外交的启"], *Public Diplomacy*, Vol. 2, 2017.

[29] For example, see Chen Hui-hui, "Commentary Analysis on 'Artificial Intelligence Technology Manipulating The US Election' Research Report," *Information Security and Commu-*

was more focused on the consequences of Russia getting caught, and the implications of the United States' enhanced counterpropaganda efforts for China's own propaganda.[30] However, the first positive assessment of Russian propaganda and disinformation efforts targeted at the United States appears to have been written in the military's propaganda journal in June 2018, potentially suggesting a shift in China's approach to the issue.[31]

One area where China has learned from Russia for social media is RT. One military analysis of RT's role as a "propaganda aircraft carrier" for Moscow examined its use of Twitter, Facebook, YouTube, Instagram, and other platforms for directly broadcasting "public opinion propaganda" (舆论宣传) to users' cell phones and tablets as a way to counter Western efforts to subvert Russia with another "color revolution" through social media.[32] A *People's Daily Online* article by Chinese academics argued that RT could teach China how to "leverage social networks to amplify the brand's effectiveness and influence 'people who are easy to influence,'" especially in places where Western media don't have as much impact, such as North Africa and the

nications Privacy, July 2017.

30 Chinese analysts referred to the bill as the "Murphy-Portman Counter-Propaganda Law." The bill itself did not mention Russia or China, but the Senators' press releases do target Russia and China ("S.3274–Countering Foreign Propaganda and Disinformation Act," U.S. Senate, 2016; "President Signs Portman-Murphy Counter-Propaganda Bill into Law," Office of Senator Rob Portman, December 23, 2016; Hu Xiaojian, "Decoding the U.S. 'Murphy-Portman Counter-Propaganda Bill,'" *International Study Reference*, July 2017, pp. 26–29.

31 Ma Chao and Sun Hao, "The Characteristics of Russian Public Opinion Propagation: Taking 'Russia Today' TV Station as an Example" ["俄罗斯对外舆论传播的特点:以'今日俄罗斯'电视台为列"], *Military Correspondent*, June 2018.

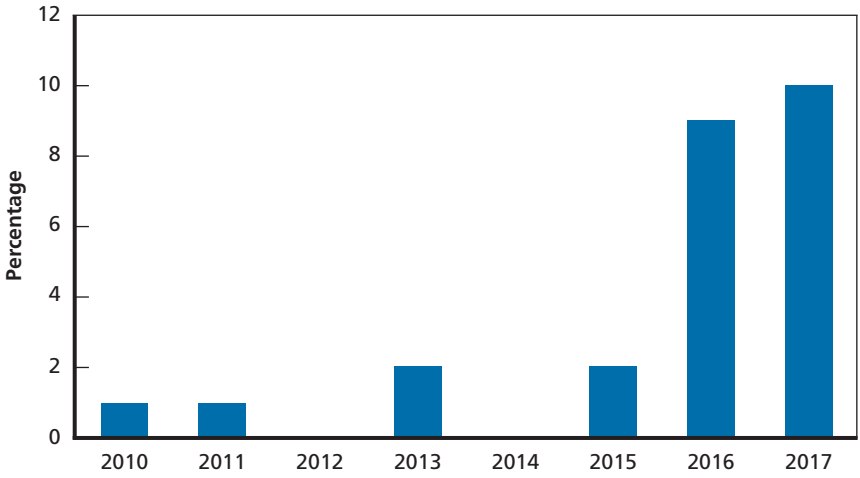
32 Ma Jianguang, Zhang Xiubo, and Zhang Naiqian, "Russia's New Front for Defending Internet Media" ["俄罗斯布防网络媒体新阵地"], *China Military Online*, April 13, 2016.

For another article on lessons learned from RT's use of YouTube, see Jiang Yunai and Luo Huanxin, "A Study on the Influence of Video Coverage on Internationally Well-Known Social Media Platforms: A Case Study of RT's English Language YouTube Account" ["国际知名媒体社交平台视频报道影响力研究——以RT的YouTube英文主账号为例"], *International Communications*, September 2017.

Middle East.[33] However, China is apparently also aware of the risks of being too much like RT, since state-run media covered Twitter's decision to ban RT from advertising on its platform.[34] Figure 4.1 offers evidence suggesting that Chinese-language publications that sometimes deal with information operations have been making more common reference to Russian sources and practices.

Some analysts suspect that China is likely learning from Russia's efforts using disinformation around the world, especially the 2016 U.S.

Figure 4.1
Articles Referencing *Russia Today* in Chinese-Language Publications Since 2016



SOURCE: China National Knowledge Infrastructure (CNKI) 2017 data through August 2017.

[33] Shi Anbing and Liu Ying, "Three Steps to Advance the Construction of International Communications Power" ["三步走"推进国际传播力建设"], *People's Daily Online*, May 19, 2014; Xu Lei, "What Can We Learn from Russia Today?" ["我们向"今日俄罗斯"学什么？"], *People's Daily Overseas Edition*, September 19, 2014; Gao Han, "Russia Today: Russia's External Propaganda Aircraft Carrier" ["今日俄罗斯"：俄罗斯的"外宣航母"], *Modern Audiovisual*, May 2016.

[34] Li Yiqing, "两家俄官媒推特账号广告功能遭关闭，曾被美指责"干预大选"", *The Paper*, October 27, 2017.

election. Former U.S. intelligence official Michael Morrell argued that "one of the consequences" of Russia's action in the 2016 election is that "other countries are now getting into the business of weaponizing social media. So the Chinese are now doing this with the Taiwanese."[35] Kent Harrington asserted that "Chinese cyber spies are also studying Russia's success," and Peter Mattis wrote that "Beijing's methods also appear to be evolving over the last year to incorporate Russian techniques," with Beijing's operations on Taiwan likely to be seen as "the leading edge."[36] All three experts quoted above are former CIA analysts, so we acknowledge that our absence of public evidence does not mean there is evidence of absence. We focus more on China's approach to Taiwan below.

Building Up "Soft Power" and Buying Friends

Reflecting China's growing assertiveness under Xi, major efforts have been made in recent years to build up China's soft power (软实力). In December 2016, Xi visited leading Chinese state-run media outlets and talked about the need for them to "tell China stories well" (讲好中国故事).[37] China's leaders also seek to build up the country's *international voice* (国际话语权; literally "international right to speak"), or influence and agenda-setting power. China's overall efforts at information management are far broader than just a focus on social media.

China's efforts to acquire such influence and shape global public opinion have involved the establishment of Confucius Institutions on foreign university campuses as well as censorship pressure on outlets such as Cambridge University's *China Quarterly* and other academic publishing firms such as Sage and Springer to censor and remove academic discussion of topics deemed sensitive by the Chinese govern-

---

35 Mike Morrell, quoted on "Face the Nation," CBS, February 4, 2018.

36 Kent Harrington, "Will China Weaponize Social Media?," *Project Syndicate*, February 5, 2018; Peter Mattis, "Contrasting China's And Russia's Influence Operations," *War on the Rocks*, January 16, 2018.

37 "President Xi Urges New Media Outlet to 'Tell China Stories Well,'" *Xinhua*, December 31, 2016.

ment.[38] CCP- and government-linked entities have also sought to buy up Hollywood film studios and movie distribution networks through ownership of theater chains, such as AMC and Carmike, and influence the content and promote self-censorship of Hollywood-produced films by leveraging controlled distribution in China.[39] And Chinese print media, most notably *China Daily*, have partnered with foreign media outlets (usually through a combination of paid inserts and reduced-cost content provision) to place their information in more widely read and trusted Western media outlets, such as the *Washington Post* and the *Wall Street Journal*.[40] For less wealthy media outlets (often from smaller or poorer countries), China simply offers *Xinhua* content as if it were a wire service, giving news firms that can't afford to post a reporter to China an opportunity to acquire free or steeply discounted content and ensuring that approved Chinese information runs in foreign media. China has also sought to influence Western social media companies through potential market access, most notably Facebook, which has reportedly occasionally agreed to or self-initiated censorship along Beijing's lines.[41]

One of the most significant areas of Chinese efforts to enhance China's informational profile throughout the region has been the steady investment in state broadcasting arms and their international subsidiaries and offshoots. China has set up new radio and television media outlets and rebranded others, most notably China Global Tele-

---

[38] Ben Bland, "China Censorship Drive Splits Leading Academic Publishers," *Financial Times*, November 4, 2017.

[39] Michael Cieply, "Deal Expands Chinese Influence on Hollywood," *New York Times*, May 20, 2012; Ryan Faughnder, "China-Owned AMC Seals Deal to Buy Carmike Cinemas, Making It the Largest Theater Chain in U.S.," *Los Angeles Times*, November 15, 2016; Clare Baldwin and Kristina Cooke, "How Sony Sanitized the New Adam Sandler Movie to Please Chinese Censors," Reuters, July 24, 2015; Richard Berman, "China's Rising Threat to Hollywood," *Politico*, October 4, 2016; Ben Fritz and John Horn, "Reel China: Hollywood Tries to Stay on China's Good Side," *Los Angeles Times*, March 16, 2011; Frank Langfitt, "How China's Censors Influence Hollywood," NPR, May 18, 2015.

[40] "China Is Spending Billions to Make the World Love It," *The Economist*, March 23, 2017.

[41] Mike Isaac, "Facebook Said to Create Censorship Tool to Get Back into China," *New York Times*, November 22, 2016; Alexandra Stevenson, "Facebook Blocks Chinese Billionaire Who Tells Tales of Corruption," *New York Times*, October 1, 2017.

vision (formerly China Central Television International, or China Central Television [CCTV] International) and, more quietly, China Radio International.[42] In some cases, the Chinese role in broadcasts is not always apparent, and Beijing appears to have a strategic concept for acquiring stations with reach into foreign capitals.[43] Recently China gathered CCTV, Radio China, and Radio China International into a single arm of state information dissemination: Voice of China. The new bureaucratic entity will fall under the CCP propaganda department.[44]

Targeting Specific Audiences

The *thought work* (思想工作) or information operations of the Party, the state, and the People's Liberation Army (PLA) are often collectively referred to as *public opinion management* (舆论管理) when undertaken inside China and *overseas propaganda work* (大外) if conducted outside of the PRC. The overall goals of such information operations are to defend the ruling status and interests of the CCP and to expand its ability to shape the international context China confronts.

Recent scholarly research suggests that Chinese domestic efforts to control public opinion seek primarily to cut off or distract from discussions that carry the potential for mobilization of antiregime sentiment inside China.[45] Externally, Chinese information operations are often targeted at specific communities, such as emigrant ethnic minorities including Tibetans, Uighurs, Mongols, and others; Falun Gong practitioners; dissident expatriates advocating for China's democratization; Hong Kong and especially Taiwan independence activists; and the broader global community of ethnic Chinese, who are seen as vectors for Chinese influence. China's use of various forms of social

---

[42] Koh Gui Qing and John Shiffman, "Beijing's Covert Radio Network Airs China-Friendly News Across Washington, and the World," Reuters, November 2, 2015.

[43] Koh and Shiffman, 2015.

[44] Steven Jiang, "Beijing Has a New Propaganda Weapon: Voice of China," CNN Business, March 21, 2018.

[45] Gary King, 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, 2017, pp. 484–501.

manipulation also targets key overseas audiences, such as decisionmakers, opinion-shapers, the business community, foreign educational and media outlets, and the general public.

Strategies: Who Manages the Media and the Messages?

Propaganda work is executed across all three major organs of governance in China: the CCP, the state apparatus (including the state-owned enterprises, or SOEs), and the military.[46] In addition, province-level administrative bodies[47] and local governments also engage in online propaganda. Coordination across the various administrative and Party bodies is not unheard of, but various units do not always operate or even typically appear to be operating from a central game plan. This is perhaps not entirely surprising since, as one recent study has argued, in excess of 200 distinct organizations within just one local subdistrict in the Chinese city of Ganzhou appeared to be involved in the blocking, removal, and fabrication of information; the number is presumably far larger when scaled up to include all bodies in China involved in propaganda and public opinion management (公共舆论管理).[48] The division of labor between party and government departments for their domestic and foreign social media engagement is also unclear but worth further study.

---

[46] Kenneth Lieberthal, *Governing China: From Revolution Through Reform*, New York: W.W. Norton & Co., 1995. Although the PLA is the armed wing of the CCP, and hence not technically a third organ of governance that can be separated from the Party, in practice the military operates in a space largely ungoverned by civilian authorities, including either state or Party officials. For another list of Chinese government organizations undertaking online propaganda, see Bradshaw and Howard, 2017, p. 17.

[47] In China, province-level administrative units include provincial governments; the governments of "autonomous regions," where ethnic minority populations are heavily clustered, including Guangxi, Inner Mongolia, Ningxia, Tibet, and Xinjiang; and the four province-level municipalities (Beijing, Chongqing, Shanghai, and Tianjin).

[48] King, Pan, and Roberts, 2017, pp. 484–501.

The Party's Publicity Department

At the pinnacle sits the CCP's Publicity Department (宣传部; known as the Propaganda Department prior to its renaming in 2013), which has responsibility for determining the most authoritative political and ideological messages distributed through the Chinese system.[49] The Publicity Department's focus tends to be on domestic online public opinion and filtering. The Publicity Department's official journal, *Party Construction,* suggests, based on a review of journal articles, that Chinese officials are increasingly interested in social media, especially mainly domestic platforms. Figure 4.2 highlights this growing interest in social media, with its disproportionate focus on domestic media.

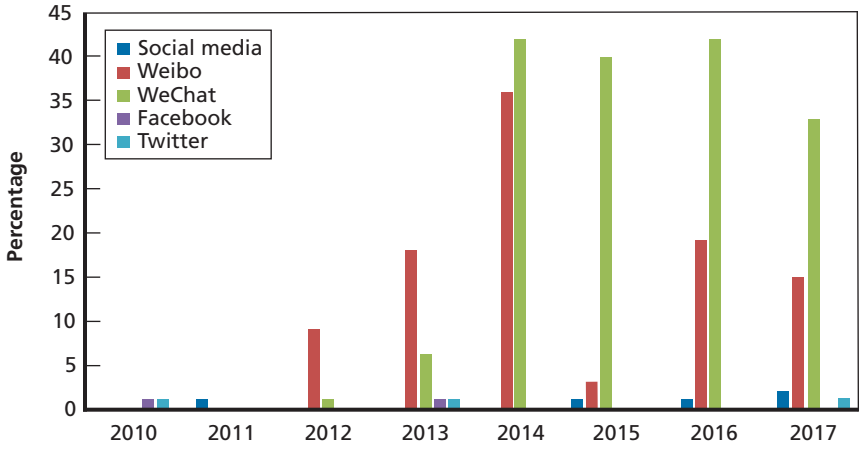
The Party's United Front Work Department

The United Front Work Department has come under the spotlight over the past year for its work to garner support for CCP policies from friendly forces at home and abroad.[50] While the UFWD's specific role in China's social media efforts abroad is unclear, it is very likely to be involved for foreign messaging, especially in foreign Chinese-language media. The *United Front Science* journal, published by the

[49] The former head of the Propaganda Department, Liu Yunshan, was quoted in one 2008 speech as saying, "Through the pertinent struggle of international public opinion, we have established a good international image and promoted the establishment of an international public opinion in favor of China. By comprehensively implementing the cultural strategy of going out, holding theme activities on Chinese culture, setting up overseas institutions of Chinese culture and vigorously establishing mainstream media in foreign countries, we have constantly expanded the international influence of Chinese culture" (Liu Yunsan, "Review and Outlook—This Article Is Abridged from the Speech Made by Comrade Liu Yunshan at the Meeting for Leading Comrades in Central Propaganda and Cultural Units on 25 December, 2008," *Seeking Truth*, January 2009.

[50] For recent research on the United Front, see Brady, 2017; Yimou Lee and Faith Hung, "How China's Shadowy Agency Is Working to Absorb Taiwan," Reuters, November 26, 2014; James Kynge, Lucy Hornby, and Jamil Anderlini, "Inside China's Secret 'Magic Weapon' for Worldwide Influence," *Financial Times*, October 26, 2017; Jamil Anderlini and Jamie Smyth, "West Grows Wary of China's Influence Game," *Financial Times*, December 19, 2017; Gerry Groot, "United Front Work after the 19th Party Congress," *China Brief*, December 22, 2017b; June Teufel Dreyer, "A Weapon Without War: China's United Front Strategy," Foreign Policy Research Institute, February 6, 2018; John Dotson, "The United Front Work Department in Action Abroad: A Profile of the Council for the Promotion of the Peaceful Reunification of China," *China Brief*, February 13, 2018.

Figure 4.2
Articles Referencing Social Media in *Party Construction*



SOURCE: CNKI database, 2017 data through October.

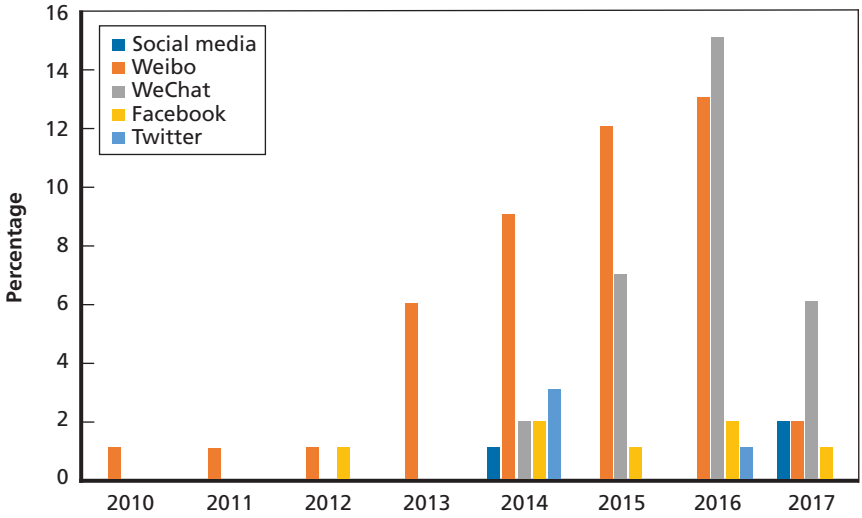
Chongqing office of the UFWD, suggests that Chinese officials are increasingly interested in social media, especially domestic platforms.[51] Figure 4.3 points to a similarly significant growth in the number of articles on social media in these two leading Chinese information and propaganda journals. To be sure, some growth in the treatment of an issue could reflect a rise in the issue's salience rather than any increase in policy attention. But the message of these data seems to be that Chinese scholars, analysts, and possibly officials are paying significantly greater attention to some of the topics involved in social manipulation.

---

[51] The United Front Department's official journal, *China United Front*, does not have any articles publicly available on the database CNKI after 2014, so we chose the Chongqing journal as a better source of data. *China United Front* had a similar focus on domestic social media platforms (Weibo from 2011 to 2014 and WeChat in 2014).

For articles on the need for the United Front Department to keep pace with evolving trends (i.e., social media) and the value of WeChat for domestic propaganda work, see Beijing Municipal Committee United Front Department, "The Historical Status and Practical Role of the United Front" ["统一战线的历史地位和现实作用"], *China United Front*, October 2012; Song Suxia, "Small WeChat and Big Family: Hebi City Builds WeChat Platform for United Front Work" [" '小' 微信 '大' 家庭——鹤壁市委统战部建立统一战线微信平台"], *China United Front*, May 2013.

Figure 4.3
Articles Referencing Social Media in *United Front Science*



SOURCE: CNKI 2017 data through May.

Myriad Government Offices

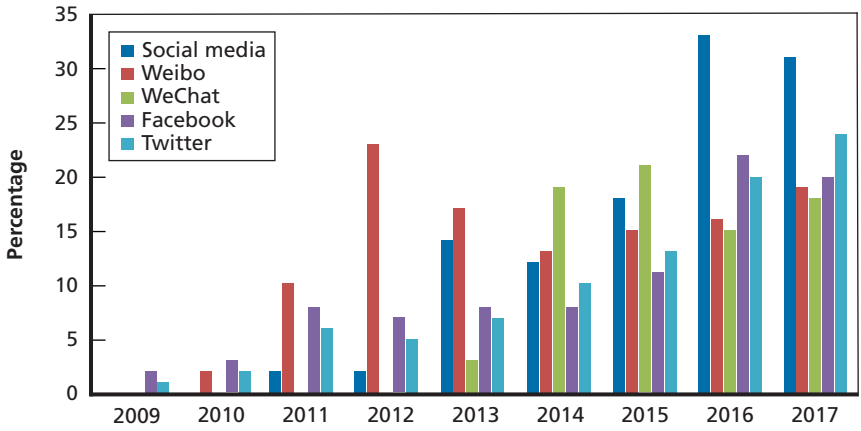
The government, in the form of the State Council Information Office (SCIO); various state-owned news agencies and media outlets such as *Xinhua* and CCTV; and the State Administration for Press, Publications, Radio, Film, and Television (SAPPRFT), produce, censor, and distribute products that convey general policy lines and leadership dictums to the Chinese public. Such bodies also serve to prevent or restrict messages not under the control of the Party from gaining widespread influence.

More recently, with the rise of the internet, the State Internet Information Office, Cyber Administration of China (CAC), and Ministry of Industry and Information Technology have joined the group of state entities exercising control over information, with special responsibilities for controlling access to information via the internet and operating the Great Firewall of China. The SCIO also has a key role to play in shaping external propaganda aimed at non–Chinese speaking audiences, and its interest in social media as a vector for influencing

foreigners is evident in the increased number of articles on the topic in its journal, *International Communications*.[52]

Articles referencing Facebook and Twitter in this key Chinese-language communications journal have grown from one and two articles in 2009 to 20 and 24, respectively, through most of 2017, showing a clear growing interest in Western social media platforms, including Facebook, Twitter, YouTube, and Instagram. As Figure 4.4 suggests, the growing number of articles on social media in this journal points to

Figure 4.4
Articles Referencing Social Media in *International Communications*



SOURCE: CNKI 2017 data through August.

[52] RAND Interview #3. A 2010 profile of the SCIO director provides some insight into the SCIO's overseas work and quotes the director as saying, "It is necessary for us to effectively carry out a campaign to win world opinion and to safeguard national security and social stability." See: Liu Jun, "Wang Chen, Guard of China's Image: A Review of His Statements and Actions in the Past Year Shows That the Question-and-Answer Papers Handed in by This Ministerial-Level Official, Who Used to Be a Journalist, Are Outstanding," *Guoji Xianqu Daobao*, March 12, 2010.

the government's rising interest in social media platforms. Other journals have even explored the role of Snapchat in foreign propaganda.[53]

Separately, as bodies focused primarily on controlling domestic threats to the ruling status of the Party and maintaining public order, the Ministry of State Security (MSS) and Ministry of Public Security (MPS) play roles in monitoring and controlling public discussion. The MSS also appears to be involved in external efforts to shape overseas access to information about China.

Another aspect of this is the use of the "fifty-cent party" (五毛党) to support CCP narratives on the internet.[54] These are typically young people who are reportedly paid 0.50 Renminbi for each post they make, earning the nickname "fifty-centers." They can be paid by any Chinese government organization and can be used for any reason, but recent research suggests their primary goal is to distract people, not actually engage with them.[55] There is no clear evidence that this army of paid commentators has been utilized on foreign social media, but this is possible.

State-Owned and "Private" Companies

Chinese state-owned internet service providers such as China Telecom, China UniCom, and China Mobile, as well as nominally private technology platform operators, such as Baidu (百度), Sina Weibo (新浪微波), and Tencent's WeChat (微信), also play important roles in enforcing censorship and compliance by users inside China. Such firms are themselves either controlled by Party appointments to management positions (in the case of SOEs) or deeply influenced by the existence of Party cells and elite cultivation in their management structures (in the case of the large "private" firms); they are also subject to being

---

53 Zhou Xiang and Han Weizheng, "Using Image Social Media to Improve China's International Communication Power" [利用图像社交媒体提升中国国际传播力研究"], *Academic Journal of Zhongzhou*, March 2017.

54 For one overview, see Ai Weiwei, "China's Paid Trolls: Meet the 50-Cent Party," *New Statesman,* October 17, 2012.

55 King, Pan, and Roberts, 2017.

fined or shut down if they host banned content.[56] Despite constant regulatory oversight, with censorship performed by the company and higher-level government departments, Weibo and other social media platforms were deemed to be jeopardizing national security in August 2017 and were put under investigation, further tightening the screw on censorship.[57] Inasmuch as information circulating in China can freely cross out of the country, such firms help to shape discourse and global discussions within the community of readers exposed to Chinese language materials, even though the primary focus of such firms is profit-making within the bounds of the PRC censorship regime.

The People's Liberation Army

The PLA, the armed wing of the CCP, also conceives of and executes overseas influence operations, including through the use of social media.[58] Chinese military theorists have written extensively on *information dominance* (信息优势), a concept that the authoritative military text *The Science of Strategy* (2013) describes as requiring a "favorable pre-combat posture" through the "synthetic application of political, economic, diplomatic, legal and public opinion means."[59] In attempting to achieve information dominance, the PLA employs social media, among other forms of outreach, to engage in what it terms the *three*

---

[56] Meng Jing and Celia Chen, "China Fines Tencent, Baidu, Weibo over Banned Contents in On-Going Crackdown," *South China Morning Post*, September 26, 2017.

[57] Beina Xu and Eleanor Albert, "Media Censorship in China," Council on Foreign Relations, February 17, 2017; Yaqiu Wang, "The Business of Censorship: Documents Show How Weibo Filters Sensitive News in China," blog post, Committee to Protect Journalists, March 3, 2016; Cate Cadell, "China Investigates Top Local Social Media Sites in Push to Control Content," Reuters, August 10, 2017.

[58] For an overview of the PLA's approach to political warfare, see Mark Stokes and Russell Hsiao, "The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics," Project 2049 Institute, October 14, 2013.

[59] Chinese Academy of Military Science Military Strategy Department, ed., *Science of Military Strategy* [战略学], 3rd edition, Beijing: Academy of Military Science Press, 2013, p. 129.

warfares (三种战争): public opinion warfare (舆论战争), legal warfare (法律战争), and psychological warfare (心里战争).[60]

The most notable example of the PLA's use of social media for strategic messaging appears to have come with its release, through the PLA Air Force's (PLAAF's) official Weibo microblog account (later promoted by the SCIO on Twitter), of a photo of a PLAAF H6-K strategic bomber flying over the disputed Scarborough Shoal in July 2016.[61] The PLAAF has also taunted Taiwan on Weibo after increasing flights around the island in 2017.[62]

This interest in social media is also evident in the growing number of articles published on the topic in the PLA's military communications journal *Military Correspondent*, as shown in Figure 4.5. This interest spans a familiar list of Western platforms, including Facebook, Twitter, YouTube, and Instagram, among others (though such articles are mostly focused on domestic Chinese platforms).

PLA writers primarily focus on wartime operations, but since they view the information domain as a perpetual conflict, much of their thinking applies to peacetime operations as well; they also tend to employ more militaristic and sensational rhetoric than Chinese civilian researchers. PLA analysts have noted that social media and other forms

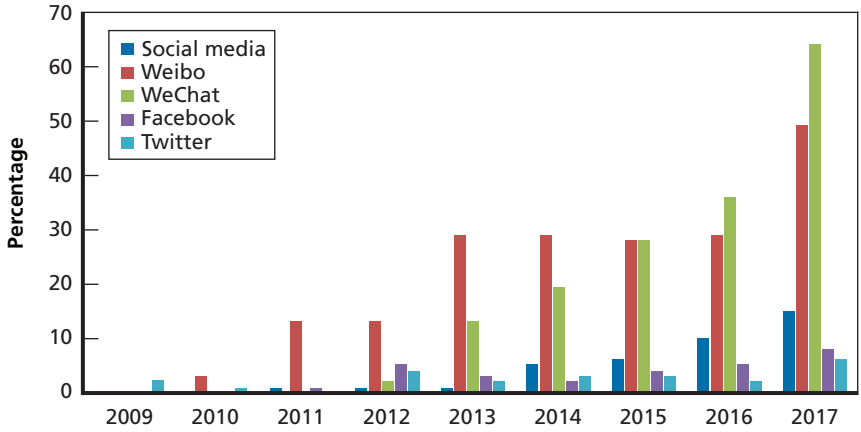
---

60 For an overview of the three warfares, see Stephan Halper, *China: The Three Warfares*, Washington, D.C.: Office of Net Assessment, 2013; Dean Cheng, "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response," Heritage Foundation, Backgrounder No. 2745, November 21, 2012; Dean Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge," Heritage Foundation, Backgrounder No. 2821, July 11, 2013; Elsa Kania, "The PLA's Latest Strategic Thinking on the 'Three Warfares,'" *Jamestown Foundation China Brief*, Vol. 16, No. 13, August 22, 2016.

61 Nathan Beauchamp-Mustafaga, Cristina Garafola, Astrid Cevallos, and Arthur Chan, "China Signals Resolve with Bomber Flights over the South China Sea," *War on the Rocks*, August 2, 2016.

62 Nathan Beauchamp-Mustafaga, Derek Grossman, and Logan Ma, "Chinese Bomber Flights Around Taiwan: For What Purpose?" *War on the Rocks*, September 13, 2017; PLAAF Weibo status, December 12, 2017. For articles about PLA propaganda targeting Taiwan, see Ma Yi, "Strengthening Agenda-Setting for Military News Coverage Targeting Taiwan," *Military Correspondent*, September 2010; Lu Wenxing, "Innovative Developments in Military Broadcasts to Taiwan in the New Communication Age," *Military Correspondent*, December 2010; Zhong Zhigang, "New Explorations on Military Propaganda Toward Taiwan Under the Goal of Building a Strong Military," *Military Correspondent*, November 2013.

Figure 4.5
Articles Referencing Social Media in *Military Correspondent*



SOURCE: CNKI 2017 data through August.

of personalized communications technology are particularly valuable for the conduct of "media warfare" (媒体战争), including the public signaling of China's claims and resolve, and have discussed the targeted coverage of scandals and other negative information involving enemy politicians to break their will to fight.[63]

PLA authors have argued that by leveraging propaganda spread through email, short messages, cell phone communications, and other interpersonal communications, including social media, China can do all of the following:

- seize the initiative
- bolster the debilitating psychological and morale-killing effects of kinetic attacks

[63] Sheng Peilin, and Li Xue, "On 'Media Decapitation,'" *Journal of the PLA Nanjing Institute of Politics*, May 2006, pp. 114–117; Wu Rui, "Be on Guard Against Other Kinds of Soft Warfare," *Military Correspondent*, November 2013, pp. 53–54; Zhu Yuping, "Factors and Inspiration for Public Opinion Warfare Under Informationized Conditions," *Military Art Journal*, October 2003, pp. 29–30.

- deceive enemy intelligence operations and degrade adversary understanding of the battlespace, making it "hard for people to distinguish the true from the false and thus more easily drive [the enemy] into a trap"
- target enemy leadership more precisely and at lower costs
- defend one's own morale and decisionmaking autonomy
- "[sow] discord in the enemy camp . . . [so as to] perplex, shake, divide and soften the troops and civilians on the opposing side."[64]

As a 2014 article asserted,

> "Cyber media warfare is a kind of combat operations with the Internet as the platform. [. . .] Targeted information infiltration is made through the Internet media for influencing the convictions, opinions, sentiments, and attitudes of the general public so as to effectively control the public opinion condition, shape strong public opinion pressure and deterrence over the adversary, and win an overwhelming public opinion posture for one's own side.[65]

Provincial Actors

Finally, provincial-level and local officials engage in efforts to censor, swamp, and distribute information online, including through social media. For example, circumstantial evidence suggests that the governments of both the Tibet Autonomous Region (TAR) and the Xinjiang Uyghur Autonomous Region (XUAR) have sought to shape global opinions about these two regions, where substantial human rights violations are ongoing, and have coordinated these operations with central authorities and Chinese tech companies.[66] In the case of Tibet,

---

64 Sheng and Li, 2006.

65 Chen Zhengzhong, "Preliminary Thoughts About Strengthening Cyber News Media in Wartime," *Military Correspondent*, July 2014.

66 For articles on the Tibetan provincial government's overseas propaganda work, including use of social media, see Lu Xin, "Three Highlights from 2011's New Media Propaganda" ["2011年新媒体外宣的三个亮点"], *People's Daily Online*, December 29, 2011; Xiong Yuhua, "To Seek Advantages and Avoid Disadvantages and Make Good Use of the 'Double-Edged Sword' of Internet—Cadres, Staff Members, and Workers of Our Region's Propaganda and

Chinese propagandists were found to be promoting the government narrative on Twitter, detailed further below, and the province's head of propaganda has called for online media to be the "new front" for external propaganda.[67] As leaks by Chinese sources have revealed, even district-level components of municipal governments operate internet propaganda offices.[68]

Actions: China's Information Operations Through Social Media

China's use of social media encompasses a range of activities, as categorized in Table 4.1.[69] We first discuss the defensive actions and then the

---

Cultural System Conscientiously Study the Spirit of the Sixth Plenary Session of the 17th CPC Central Committee," *Tibet Daily*, October 24, 2011; Chen Lin, "Effectively Strengthen Internet Propaganda and Management Work to Create Sound Internet Public Opinion and Cultural Environment for Society," *Tibet Daily*, May 26, 2012; "Further Present a Real Tibet to the World—Sixth Discussion on Earnestly Studying and Implementing Spirit of Comrade Li Changchun's Important Speech," *Tibet Daily*, August 5, 2012; Tang Dashan, "Tibet Should Build a Major External Propaganda Structure," *Tibet Daily*, September 14, 2013, p. 3; Shi Lei and Xiao Tao, "Chen Quanguo, Lobsang Gyaincain Meet Media Delegation 'Beijing Internet Media Red Land—Tibet'; Wu Yingjie Present at Meeting," *Tibet Daily*, August 20, 2014, pp. 1–2.

For articles explaining the Inner Mongolia and Shenzhen governments' foreign propaganda, see: Bi Lifu, "Innovating Foreign Propaganda in Ports and Improving Inner Mongolia's Image," *Theory Construction*, 2009, pp. 10–12; Wang Pan, "Casting a New 'Window to China'—Explorations and Thoughts on Shenzhen's Foreign Propaganda Work in the New Era" ["铸造新的"中国窗口"—新时期深圳特区外宣工作探索与思考"], *International Communications*, February 2012.

67 Jonathan Kaiman, "Free Tibet Exposes Fake Twitter Accounts by China Propagandists," *The Guardian*, July 22, 2014; Chen, 2012.

68 Anne Henchowitz, "Thousands of Local Internet Propaganda Emails Leaked," *China Digital Times*, December 3, 2014.

69 Other uses of such platforms to advance national security goals clearly exist but lie outside the scope of this research effort. For example, Chinese state and military intelligence organs have reportedly used social media platforms to engage in espionage and recruitment, scraping foreign users' social media postings to create a personal dossier on targets of influence attempts. While not directly related to the effort to push propaganda on social media, this approach has recently received substantial attention, and so we include it here as

Table 4.1
Taxonomy of Chinese Influence Operations via Social Media

	Type of Approach	
Target	**Defensive**	**Offensive**
Chinese	• Promoting government narratives • Reaffirming Party legitimacy through nationalism • Outreach to overseas Chinese • Enforcing the Party line abroad • Attacking regime opponents abroad	• Extending judicial reach • Intimidation through surveillance
Foreign	• Promoting government narratives • Enforcing the Party line abroad	• Military strategic messaging • Extending judicial reach • Spreading fake news

offensive actions in the order listed in the table. Many of these activities have fluid categorization and a degree of overlap, so readers can create their own breakdown of the examples provided. Thereafter, we discuss a few of China's self-restraints in using social media.

Promoting Government Narratives

Simple releases of official Chinese government or institutional positions, which are used to share basic information or present approved data, represent the most basic form of social media engagement—and the first of five defensive social media operations that we will describe. Most major institutions in China have webpages and blogs where information about the operations of the organization is presented. For example, the SCIO has a Twitter page where it presents the latest approved releases from the Chinese central government, while *People's Daily* maintains a Facebook account where it posts photos of visits to China

a footnote. See, for example, "German Intelligence Unmasks Alleged Covert Chinese Social Media Profiles," 2017; Javier C. Hernandez and Melissa Eddy, "China Denies Using LinkedIn to Recruit German Informants," *New York Times*, December 11, 2017.

by foreign leaders, images of pandas, and stories about China's latest high-speed rail connections. Such information is generally intended to present a favorable image of a China that is well-led, respected, perceived as nonthreatening by the outside world, and advancing Chinese national interests in a way that foreign audiences should accept and not try to change or oppose. Chinese propaganda journals have countless articles on how best to promote or explain various government policies—the Belt and Road Initiative, Party Congress meetings—and even how to present images of Xi Jinping himself.[70] This propaganda

[70] "Successfully Do Foreign Propaganda Work for the 90th Anniversary of the Party's Founding: Fully Show Our Party's Positive Image" ["做好建党90周年对外宣传工作 充分展示我党良好形象"], *International Communications*, January 2011; Xiao Lili, "Challenges and Public Opinion Responses for China's National Image in Africa" ["中国国家形象在非洲面临的挑战及舆论应对"], *International Communications*, August 2011; Liu Chen, "Audience Strategy for Foreign Communications on the Image of China's Economy" ["中国经济形象对外传播的受众策略"], *International Communications*, November 2011; Sun Ming, "International Public Opinion on This Year's 'Two Congresses'" ["今年"两会"的国际舆论关切"], *International Communications*, March 2013; Lian Xiaotong, "Analysis of Leaders' Public Diplomacy Strategy from a Cross-Cultural Perspective—Xi Jinping's 2012 Visit to the United States as Example" ["跨文化视野下领导人公共外交策略分析—以2012年习近平访美为例"], *International Communications*, September 2013; Jia Min, "Creator's Plight: The Good and Bad of Shaping Obama's Image" ["创新者的窘境:奥巴马形象塑造中的得与失"], *International Communications*, April 2014; Yao Yao, "The West's View of China, or the World's View of China? New Thinking on Building China's Global Image" ["西方的中国观,还是世界的中国观?—中国建构国际形象的新思路"], *International Communications*, July 2014; Xu Hua, "How Did Putin Create the Image of a Leader" ["普京如何塑造领袖形象"], *International Communications*, March 2015; Wang Chen and Zhou Ting, "Three Problems for Building and Communicating National Leader's Public Image" ["国家领导人公共形象的构建与传播三问"], *International Communications*, June 2015; Jiang Yunai, "Shaping National Leaders' Image Through Foreign Communication via New Media—2015 Twitter Reporting by Xinhua, People's Daily and CCTV as Examples" ["新媒体对外传播中的国家领导人形象塑造—以2015年新华社、《人民日报》、央视的推特报道为例"], *International Communications*, April 2016; Zhao Mingwu, "Messaging One Belt One Road Strategy: Problems and Responses" ["'一带一路'的政策传播:问题与应对"], *International Communications*, April 2016; Hu Yu and Lu Jun, "Experiences and Thoughts on Construction of Central-Level State-Owned Enterprises Image Abroad" ["央企海外形象建设的经验与思考"], *International Communications*, October 2016; "An Examination of International Public Opinion on One Belt One Road" ["一带一路"议题的国际舆情分析"], *International Communications*, May 2017.

can be targeted at both foreigners and Chinese abroad, and Chinese researchers attempt to track global discussion of China-related topics.[71]

One application of this on a mass scale for social media is astroturfing, or making state-run or state-orchestrated propaganda appear to be coming from the grassroots. In the case of Tibet, Chinese propagandists were discovered in 2014 to "have opened scores of fake accounts on Twitter to promote Beijing's line on the ethnically divided Himalayan region," though more recent analysis suggests this practice has ended.[72] For Taiwan, after President Tsai Ing-wen was elected in January 2016, there was a "coordinated grassroots messaging campaign" where "attackers posted pro-mainland comments [. . .] to show the reaction of Chinese citizens to Taiwan's election of Tsai Ing-wen [. . . and] expressed a desire to reunify China and Taiwan."[73] This illustrates the Chinese government's ability to conduct propaganda campaigns on foreign social media.

---

[71] For one example of overseas propaganda targeting Chinese abroad, see Ji Deqiang, "Global Communications for China's Anti-Corruption Campaign: Problems and Solutions—Based on Real Research of Chinese Students Studying Abroad" ["中国反腐的国际传播：困境与出路 一一基于对在华外国留学生的实证研究"], *International Communications*, December 2016.

For examples of Chinese research on global discussion and opinion about China, see Xiang Debao and Zhang Renwen, "Characteristics of Public Opinions About China on International Social Media in 2012" ["2012国际自媒体涉华舆情特征"], *Journal of Intelligence*, Vol. 32, No. 8, 2013, pp. 31–34; Xiang Debao, "Rules, Characteristics and Guidance Strategy for Public Debate over Tibet in International Social Media and the Public Opinion Struggle" ["国际自媒体涉藏舆情及舆论斗争的规律、特征及引导策略"], *Journal of Intelligence*, Vol. 35, No. 5, 2016, pp. 20–26.

[72] Kaiman, 2014. According to Kaiman, the human rights nongovernmental organization Free Tibet "found that the fake accounts had overlapping qualities. Most of their names were comprised of two Western-sounding first names strung together. About 90 of them were also closely intertwined—they followed one another and frequently retweeted each other's posts, often identical statements and links."

For more recent research, see Gillian Bolsover, "Computational Propaganda in China: An Alternative Model of a Widespread Practice," Computational Propaganda Research Project, University of Oxford, Oxford, UK, April 2017.

[73] Nicholas J. Monaco, "Computational Propaganda in Taiwan: Where Digital Democracy Meets Automated Autocracy," Computational Propaganda Research Project, University of Oxford, Oxford, UK, June 2017.

Under President Xi, Chinese propagandists have tried to produce less stilted, less formalistic products and are now regularly producing short videos intended for foreign audiences and distributed on Western social media, including Twitter and YouTube.[74] These videos explain recent Chinese events—the 13th Five Year Plan, the Belt and Road Forum, Xi's visit to the United Kingdom—and tout the leadership of Xi and the Party.[75] They are reportedly created by a British marketing company popular with the Chinese government, and they are released under the brand "Fuxing [Rejuvenation] Road Studio," a homage to Xi's stated goal for China.[76] These videos have improved in quality and appeal over time and clearly show the CCP is increasingly adept at reaching foreign audiences on social media, as well as able to leverage Western marketing expertise to tailor its messaging.[77]

Reaffirming Party Legitimacy Through Nationalism

China also makes or permits the circulation of social media content designed to stir up nationalistic sentiment among Chinese netizens by portraying popular anger against foreign governments perceived as insufficiently respectful of China's interests. In March 2017, two Chinese men filmed themselves smashing South Korean electronics while the Chinese national anthem blared in the background in a short video clip that went viral in China. The intention appears to have been to chasten the South Korean government over its decision to approve the

---

74 Zheping Huang, "China's Craziest English-Language Propaganda Videos Are Made by One Mysterious Studio," Quartz, October 27, 2015; Nick Stember, "The Road to Rejuvenation: The Animated Xi Jinping," in Gloria Davies, Jeremy Goldkorn, and Luigi Tomba, eds., *China Story Yearbook 2015: Pollution*, Canberra: ANU Press, 2016.

75 Olivia Geng, "'Very Big Muscles': Chinese Propaganda Video Lavishes Praise on Putin," blog post, *Wall Street Journal*, May 8, 2015; Felicity Capon, "Chinese Propaganda Cartoon Promotes Five Year Plan," *Newsweek*, October 27, 2015.

76 Chun Han Wong, "The Foreigner Advising Beijing on Propaganda," *Wall Street Journal*, May 13, 2016.

77 Matthew Robertson, "UK Firm Can't Figure Out Who Hired Them to Promote Chinese Propaganda Video," *Epoch Times*, October 19, 2015.

deployment of a U.S. Terminal High-Altitude Aerial Defense battery in Seongju, South Korea, a move that China objects to.[78]

Outreach to Overseas Chinese

China views overseas Chinese as an important population to target for influence operations.[79] These operations are focused mainly on Han Chinese, both PRC citizens living abroad and the ethnic Han Chinese diaspora who are not PRC citizens, but also include Chinese ethnic minority groups living abroad, both citizens and those who have a foreign nationality. Social media is now a key part of the Chinese government's connection to these groups.

One example of China's uses of social media for overseas outreach purposes has been the Chinese government's use of WeChat to contact and request personal information from Uyghurs (an ethnic minority in China that is Muslim and viewed as politically unreliable) who are now French citizens and living in France as part of a major effort to collect intelligence on, monitor, and shape the behavior of Uyghurs living abroad.[80]

Social media can also be used to target key groups for propaganda messaging. For example, a 2017 *International Communications* article about tailoring propaganda for Hong Kong middle-class professionals argues that the United Front Work Department should "learn from all kinds of new modes of propaganda and mobilization [on the internet], and 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

---

78 "Hotels Turn Away South Koreans, Chinese Smash Goods as Missile Row Widens," Radio Free Asia, March 13, 2017.

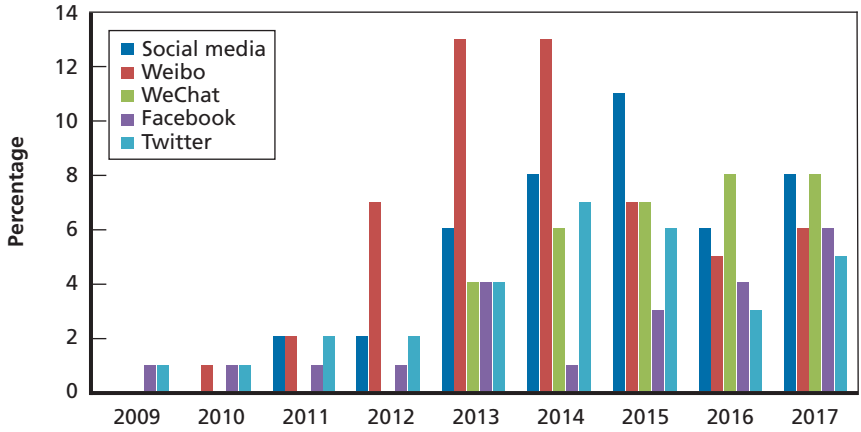
79 Timothy Heath, "Beijing's Influence Operations Target Chinese Diaspora," *War on the Rocks*, March 1, 2018.

80 Bethany Allen-Ebrahimian, "Chinese Police Are Demanding Personal Information from Uighurs in France," *Foreign Policy*, March 2, 2018a.

ideas."[81] Figure 4.6—while reflecting some interesting but still unclear patterns such as the spike and then decline in articles about Weibo—conveys one overall message: the growing attention that has been paid to reaching the Chinese diaspora through social media.

Another approach to spreading the Chinese government's narrative has been through co-opting Chinese living abroad, especially overseas students.[82] This has traditionally been low-tech. One article on the 2008 anti-China protests in France, when the Olympic torch traveled through the country, highlights the role played by a small number of

Figure 4.6
Articles on Chinese Diaspora and Social Media in *International Communications*



SOURCE: CNKI 2017 data through October.

[81] 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.

[82] On the value of Chinese students abroad, see Zhao Liangying and Xu Xiaolin, "Actively Build China's National Strategic Communication System" ["积极构建中国国家战略传播体系"], *Media Outpost*, September 2016; Han Song and Ping Chuan, "Grasp Important Points, Explain Difficult Points, Decipher Confusion Points: How to Explain 3rd Plenum Meeting of 18th Party Congress to Foreigners" ["抓重点 解难点 释疑点—如何做好十八届三中全会的对外解读"], *International Communications*, January 2014; Ma Han, "Research and Opinion on Current Problems in Building China's International Voice" ["当前中国国际话语权构建问题研究谫论"], *Journal of Yunnan Provincial Committee School of CCP*, December 2016; Bi, 2009; Hou Dongsheng, "Comparison and Analysis of Foreign Propa-

Chinese students there in conveying, or explaining, China's treatment of Tibetans.[83] The article contends that "the most reliable and most effective method for changing [locals'] erroneous beliefs about China or Tibet" is through overseas Chinese students' friendship with locals because adolescents are the easiest to convince, and "foreign propaganda work can be accomplished through organizing exhibitions, lectures, salons, and travel."

The dramatic increase in the numbers of Chinese students studying abroad in the West, combined with the advent of social media, provides Beijing more people to deliver the message and better ways to shape its messengers. One aspect of the outreach is to ensure ideological discipline. For instance, a 2014 article in the United Front Work Department's official journal touted the value of social media, along with lectures and conferences, in disseminating President Xi's speeches to overseas students.[84]

Recent coverage of Chinese student associations at U.S. universities has revealed that the Chinese embassy and consulates keep in touch with these organizations through WeChat and have tried to organize student sessions regarding major political events back home in China.[85]

---

ganda Related to Tibet Between Chinese Government and Dalai Lama Clique" ["中国政府与达赖集团在涉藏外宣上的比较和分析"], *Journal of Chongqing Institute of Socialism*, June 2012.

Foreign students in China are also targets for propaganda indoctrination (Bi, 2009; Yang Yunsheng, "Research on Foreign Propaganda for the China Dream" ["中国梦海外宣讲研究"], *New Orient*, June 2016).

For criticism of overseas Chinese students as poor conduits for influence, see Tan Feng, "Why China Became the 'Sacrificial Lamb' of U.S. Elections" ["中国为何成为美国大选的'替罪羊'"], *International Communications*, September 2016.

83 Cai Yintong, "Study Abroad Students: An Important Force for People-to-People External Propaganda" ["留学生: 民间外宣的重要力量"], *International Communications*, March 2009; Hou, 2012.

84 Song Shunan, "Gather the Abroad Students to Strengthen the Dream of National Revival—A Report of the Speech of General Secretary Xi Jinping Learning the 100th Anniversary" ["凝聚留学人员力量共筑民族复兴梦想—欧美同学会学习习近平总书记在百年庆典上的讲话纪实"], *China United Front*, February 2014.

85 Bethany Allen-Ebrahimian, "China's Long Arm Reaches into American Campuses," *Foreign Policy*, March 7, 2018b.

At the same time, the Chinese propaganda system clearly treats the overseas students as a vector for influencing foreign public opinion.[86] Notably, the article touts "Soft Power, Discourse Power, Cultural Identity, and Ethnic Awareness" as key terms for its content.

Enforcing the Party Line Abroad

Another aspect of China's use of social media for public opinion manipulation is its collection of information about foreigners from postings by Chinese citizens when they travel overseas. Such an approach effectively transforms any Chinese citizen using social media into an extension of the PRC state intelligence apparatus. This use of social media leverages reporting by Chinese citizens on overseas events that might "offend" Chinese sensibilities, potentially leading to costly consequences for foreigners, even in their own home countries. In numerous recent examples from Australia, Chinese students in that country have posted on their WeChat accounts the personal information of professors who referred to Taiwan as a separate country or described border territories to which China lays claim as Indian territory, leading to a

[86] A 2016 article extols the "irreplaceable special role" of overseas Chinese students in spreading the Chinese narrative on Tibet, especially their ability to use social media for propaganda against the Dalai Lama, and suggests the government needs to shape their opinions and guide their propaganda efforts; Qin Yongzhang, "Utilizing Overseas Chinese Students' Role for Foreign Propaganda Related to Tibet" ["发挥海外中国留学生群体在涉藏外宣工作中的作用"], *International Communications*, May 2016. The article further notes that "this non-governmental propaganda is more 'flexible' and 'lively' compared to the stereotypical image of our 'rigid' and 'formulaic' official propaganda. Their 'external propaganda' is more easily accepted by the majority of foreign citizens. It's easy to get twice the result with half the effort." One example of this is cited in another 2016 article about the role of overseas Chinese for Chinese soft power that recounts how Chinese alumni and the Chinese student association, among others, at Cornell University used social media to organize toward lobbying the administration to alter the wording of its congratulatory statement on Tsai Ing-wen's victory as Taiwan president to bring it in line with China's party line. RAND was unable to verify that the announcement's wording had actually changed. See Blaine Friedlander, "Taiwan Elects Its Second Cornell Alumnus as President," *Cornell Chronicle*, January 29, 2016; Yi Changjun, "Research on New Overseas Chinese Associations and the Construction of 'Soft Power'" ["海外新华侨华人社团与国家 '软实力' 建设研究"], *Journal of Huaqiao University*, May 2016.

flood of online complaints against the schools where the faculty were employed.[87]

When officials discern that information disadvantageous to the party or the government is circulating, the regime swings into action on social media by blocking or censoring the unauthorized information if it lives on a platform over which China has control. Then, once approved messages have been created and authorized, propaganda organs flood a variety of social media platforms with messages aimed at distracting, swamping, or drowning out anti-government arguments that could provoke social mobilization against the regime.[88] Such efforts are mainly targeted at countering domestic popular action, but insofar as no real barriers exist that would stop information in China's online space from flowing out to the outside world (in contrast with the Great Firewall that blocks information from the outside world from getting into China), such actions can have effects on the global discussions of China that are carried on in Chinese-language media anywhere worldwide where users access PRC social media platforms.

This effort has, in recent months, extended to foreign companies as part of a larger crackdown on perceived corporate sympathies for disputed territorial claims.[89] The campaign began in January 2018 when Marriott International, Delta Airlines, and Zara, among others, were forced to apologize for listing Tibet and Taiwan as separate countries. Then, a Marriott employee accidently "liked" a Twitter post by a Tibetan independence group that supported Marriott for listing Tibet as a separate country, leading to further Chinese criticism and the employee's eventual firing.[90] The next month, Mercedes-Benz posted a photo on its Instagram account with a quote from the Dalai Lama, and

---

87 Josh Horwitz, "Australian Professors and Universities Are Being Shamed into Apologizing for Offending Chinese Students," *Quartz*, August 29, 2017.

88 King, Pan, and Roberts, 2017; RAND Interview #5.

89 Richard Bernstein, "The Brands That Kowtow to China," *New York Review of Books*, March 2, 2018.

90 Teddy Ng, "Marriott Sacks Employee Who 'Liked' Twitter Post from Tibet Independence Group," *South China Morning Post*, January 13, 2018; Wayne Ma, "Marriott Employee Roy Jones Hit 'Like.' Then China Got Mad," *Wall Street Journal*, March 3, 2018.

"angry Chinese Instagram users had flooded Mercedes-Benz's account to express outrage," even though the app is banned in China.[91] The company was forced to apologize for offending the Chinese people, though it was reportedly still called "an enemy of the Chinese people" several days later by state-run media.[92] This suggests a coordinated campaign of pressure against Western companies in the service of upholding China's party line. Indeed, according to the *New York Times*,

> At a major Chinese internet conference last year, Mei Jianming, a Chinese antiterrorism expert, said Beijing should put more pressure on companies like Twitter. The goal would be to get them to change their terms of service so they could restrict posts by groups that Beijing considers subversive, like the World Uyghur Congress, which seeks self-determination for the people of the western Chinese region of Xinjiang.[93]

Attacking Regime Opponents Abroad

State security and information forces have also reportedly threatened or actually carried out attacks against real or perceived opponents of the regime through the use of cyberstalking, trolling, or hacking in a form of "informationalized intimidation." These attacks have been directed mostly against overseas communities of religious and ethnic minorities and political dissidents.[94]

---

[91] Amy B. Wang, "Bowing to Pressure from China, Mercedes-Benz Apologizes for Quoting the Dalai Lama in Ad," *Washington Post*, February 6, 2018.

[92] Pei Li and Adam Jourdan, "Mercedes-Benz Apologizes to Chinese for Quoting Dalai Lama," Reuters, February 6, 2018; Bernstein, 2018.

[93] Paul Mozur, "China Presses Its Internet Censorship Efforts Across the Globe," *New York Times*, March 2, 2018.

[94] Separately, the Chinese government also conducts cyberattacks against perceived regime opponents abroad, such as pro-Tibet groups (Nithin Coca, "The High-Tech War on Tibetan Communication," *Engadget*, June 27, 2015; John Markoff, "Vast Spy System Loots Computers in 103 Countries," *New York Times*, March 28, 2009; "Tracking Ghostnet: Investigating a Cyber Espionage Network," Citizen Lab, March 28, 2009; Katie Kleemola, Masashi Crete-Nishihata, and John Scott-Railton, "Targeted Attacks Against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114," Citizen Lab, June 15, 2015.

One of the most notable examples has been the attempt to intimidate Guo Wengui (also known as Miles Kwok), a wealthy PRC national who fled the country reportedly in possession of a substantial portfolio of compromising information about China's top leaders and who has threatened to release such information online in the United States.[95] Guo has allegedly been threatened via social media accounts purportedly controlled by the Chinese state security services. Pressure from China on American social media platforms is widely believed to have been the reason why Guo's Twitter and Facebook accounts were both briefly suspended in early 2017, and Chinese pressure is similarly believed to be the reason why an interview Guo was doing with Voice of America in April 2017 was suddenly curtailed, and why three of the reporters involved were ultimately fired.[96] Additionally, according to one interviewee, China appears to have purchased the services of Russian artificial intelligence bots in order to attack Guo in a timely manner and to quickly swamp Guo's Twitter feed with messages claiming to be from outraged pro-CCP Chinese nationals.[97]

This can also take the form of cyberbullying. In May 2017, a Chinese student gave a speech at her University of Maryland commencement ceremony and criticized her home country in her remarks.[98] She was heavily criticized on Weibo within China, but some of these attacks

---

[95] Michael Forsythe, "Billionaire Who Accused Top Chinese Officials of Corruption Asks U.S. for Asylum," *New York Times*, September 7, 2017b.

[96] RAND Interview #3; Paul Mozur, "Facebook Briefly Suspends Account of Outspoken Chinese Billionaire," *New York Times*, April 21, 2017; Michael Forsythe, "He Tweeted About Chinese Government Corruption. Twitter Suspended His Account," *New York Times*, April 26, 2017a; Choi Chi-yuk, "Voice of America Fires Three Staff over Explosive Guo Wengui Interview," *South China Morning Post*, November 15, 2017.

[97] Interview #3. The giveaway was apparently that the Russian Twitter bots, while posting slight varieties on a core anti-Guo-themed tweet in Chinese, nonetheless retained their pseudo-Russian names. Some of the bots reportedly did nothing but spam Guo's account with garbled messages that made no sense but that may have been intended merely to overwhelm the system or make it impossible for real users to get their own messages through.

[98] Mike Ives, "Chinese Student in Maryland Is Criticized at Home for Praising U.S.," *New York Times*, May 23, 2017.

were also posted on Twitter and Facebook, leading her to apologize.[99] There is no clear evidence that the Chinese government was involved in creating this sentiment, but the lack of censorship on Weibo suggests the attacks were tacitly allowed, and Chinese state-run media joined in the criticism.[100]

Extending Judicial Reach

More troubling still, relative to the defensive information operations discussed above, has been China's offensive social media operation aimed at deterring criticism of China by both Chinese citizens and foreigners. This effort aims to mute criticism of China by targeting and prosecuting even foreigners who use popular Chinese services such as WeChat (*Weixin*) or QQ.[101]

One of the most prominent examples of this type of operation is the arrest of Taiwan national Lee Ming-che and his prosecution inside China for purportedly discussing support for China's democratization on Chinese social media platforms. His posts were seen as endangering state security. During his trial, prosecutors also referenced discussions held by others on Facebook outside of China and treated these as evidence of crimes that could be prosecuted inside China, should the individual in question come into Chinese government officers' hands.[102] Another case is that of Zhang Guanghong, a Chinese activist living in China who shared an article critical of President Xi on WhatsApp. He is the first known person to be prosecuted "by Chinese authorities using conversations from a non-Chinese chat app as evidence," though

---

[99] Josh Horwitz, "A Chinese Student's Commencement Speech Praising "Fresh Air" and Democracy Is Riling China's Internet," *Quartz*, May 23, 2017a; "Student Heckled by Chinese Netizens After Praising US Fresh Air and Free Speech," *Study International*, May 24, 2017.

[100] Tom Phillips, "Chinese Student Abused for Praising 'Fresh Air of Free Speech' in US," *Guardian*, May 23, 2017.

[101] For a report on China's judicial punishment of social media–related dissent, see *Forbidden Feeds: Government Controls on Social Media in China*, New York: PEN America, March 13, 2018.

[102] This paragraph draws heavily from Jojje Olsson, "Beware of Chinese Social Media," *Taiwan Sentinel*, September 23, 2017.

experts suspect his phone was hacked and not that his WhatsApp's encryption was broken.[103] China's goal with this approach is very likely to deter others from making similar social media posts.

Intimidation Through Surveillance

Another use of social media for an offensive operation is its use as a surveillance asset. Chinese officials have mined domestic and foreign users' postings and personal webpages to collect data. Domestically, this information can then be used by police and state security officials to punish anyone guilty of crossing boundaries that Chinese officials want to reinforce.[104] With respect to foreign nationals, such information can lead to intimidation tactics intended to change behavior patterns (in some cases, simply alerting the individual that he or she is being watched may be enough to dissuade a foreign national from participating in activities China seeks to prohibit). Such information can also be used to ban foreign nationals from traveling to China (this is most useful if the individual is well-known and will suffer costs to his or her career, which could then be used to warn others not to engage in similar behavior).

In Australia, Chinese government officials have reportedly sought to discourage local citizens from attending Falun Gong performances by revealing that their online behavior is being monitored.[105] One Chinese-Australian argued that "China also monitors the social media accounts of dissidents in Australia, and many fear that their private messages and social networks might make them targets of the Chinese government."[106]

---

[103] Mozur, 2018.

[104] For a recent and disturbing domestic example that has garnered attention abroad (which is likely an added benefit for Chinese officials, who see such attention as magnifying the impact of their influence and ability to mark off areas where discussion is forbidden or severely constrained), see Eva Dou, "Jailed for a Text: China's Censors Are Spying on Mobile Chat Group," *Wall Street Journal*, December 8, 2017.

[105] Paul Maley, "From Beijing to Parramatta: How China Muscled Up to Council," *The Australian*, November 11, 2017.

[106] Alex Joske, "Beijing Is Silencing Chinese-Australians," *New York Times*, February 6, 2018.

Numerous Western celebrities have been banned from China for revealing support on social media platforms for causes or individuals opposed by the Chinese government. For example, the U.S. band Maroon 5 was forced to cancel a sold-out Shanghai concert after rhythm guitarist and keyboardist Jesse Carmichael tweeted out a happy birthday wish to the Dalai Lama in 2015.[107] Similarly, Canadian singer Justin Bieber was sharply criticized by Chinese Foreign Ministry spokesman Qin Gang after the pop star uploaded a photo of his visit to Japan's controversial Yasukuni Shrine to his Instagram account in 2014.[108] A separate case is that of the lingerie model Gigi Hadid, who was denied a visa to China in late 2017 to participate in the annual Victoria's Secret fashion show after PRC netizens found that she had made gestures that Chinese netizens claimed were derogatory toward Asians in photos posted to her sister Bella's Instagram account.[109] This example shows how the PRC government is careful to respond quickly against any perceived slights to Chinese public opinion so as to ensure that it maintains its reputation as a staunch and reliable steward of Chinese nationalism.

Another form of intimidation through surveillance is China's nascent social credit system. The program, which has been under development since at least 2014 and is slated for full implementation by 2020, seeks to build a composite score for each individual based on a wide range of criteria, including financial indicators (paying your bills on time), social activities (volunteering or not speeding while driving), and online behavior (not spreading "rumors").[110] In turn, this score will potentially affect many Chinese citizens' government benefits: educa-

---

[107] Bethany Allen-Ebrahimian, "Did China Just Ban Maroon 5?" *Foreign Policy*, July 16, 2015.

[108] Zachary Keck, "Justin Bieber Visits Japan's Yasukuni War Shrine," *The Diplomat*, April 24, 2014.

[109] Grace Tsoi, "Why Katy Perry and Gigi Hadid Were Missing from Shanghai's Victoria's Secret," BBC News, November 20, 2017.

[110] Mara Hvistendal, "Inside China's Vast New Experiment in Social Ranking," *Wired*, December 14, 2017; Josh Chin and Gillian Wong, "China's New Tool for Social Control: A Credit Rating for Everything," *Wall Street Journal*, November 28, 2016; Rachel Botsman, "Big Data Meets Big Brother As China Moves to Rate Its Citizens," *Wired*, October 21,

tion, employment, travel, a mortgage, or even the ability to stay at a state-owned hotel. Although it is unclear exactly how comprehensive and enforced this system will be in practice, it could make it possible for the state, as an Orwellian nightmare of Big Brother, to reengineer people's behavior with an invisible touch. Already, one application has been to online group chats such as WeChat; in September 2017, the Chinese government required "internet companies to establish credit rating systems for chat group users, and provide services to them in accordance with their credit scores," according to one report.[111]

This system is not known to be currently targeted at foreigners. In the future, however, as Chinese companies, especially financial institutions, play a larger role in American life, it is possible that this social credit system could be extended to foreigners beyond China's border as a condition for interaction with Chinese companies and could thus influence the behavior, private conversations, and social relations of U.S. citizens. Moreover, an even greater risk may be that autocratic governments around the world begin to look to China for the technology to establish their own systems of social monitoring and control, including the backbone of a social credit-like system supported with such technologies as facial recognition and AI. Beijing could seek to actively sponsor states affiliating with its form of political system through these means.

Military Strategic Messaging

Similarly, the PLA and selected Chinese central government organs have posted offensive messages on social media platforms when it served their interests. Some such postings have been used for signaling resolve, deterrence, or coercion to key domestic and overseas audiences by posting messages or imagery of PLA capabilities, exercises, or operations. One example is the PLAAF's posting on Weibo of an image of an H6-K strategic bomber flying over disputed islands in the South

---

2017; Jiayang Fan, "How China Wants to Rate Its Citizens," *New Yorker*, November 3, 2015; "China Invents the Digital Totalitarian State," *Economist*, December 17, 2016.

[111] Zheping Huang, "China Wants to Build a Credit Score That Dings Online Chat Group Users for Their Political Views," *Quartz*, September 8, 2017.

China Sea in summer 2016 after a Permanent Court of Arbitration ruling invalidated China's "9-dash line claim" over those territories.[112] Potentially suggesting similar interest in using Western social media, PLA propagandists have also called for the Chinese military to join Twitter.[113]

A separate and more ambiguous use of social media for military messaging involves the widespread phenomenon of military enthusiast bulletin boards and websites that have frequently been the first to report the initial operations or roll-outs of Chinese capabilities, some of which are likely not even close to being ready for operational deployment. The fact that photos or information about such capabilities are not sanitized after their initial postings strongly suggests that either the information is deliberately leaked or Chinese military authorities believe that, once out in the public domain, such information can be leveraged to their advantage.[114]

One way that the authorities may see such value is if the information circulating on bulletin boards or fan websites convinces foreign powers that China has a capability that it has not yet fully perfected months or years in advance of its operational deployment, thereby shaping foreign behavior in ways that China prefers. For example, when information about China's first advanced stealth fighter, the J-20, first began circulating, it did so via images on military fan websites such as *Tiexue.net*. Most updates on China's aircraft carrier program and images of various other Chinese military hardware have been delivered in the same way.[115]

---

[112] Beauchamp-Mustafaga et al., 2016.

[113] Zhang Leilei, "Actively Use Overseas Social Media for Military Foreign Propaganda" ["积极利用海外社交媒体参与军事外宣"], *Military Correspondent*, August 2016, pp. 59–60; Chen Jie, "Build a Military Foreign Propaganda Shock Brigade" ["打造军事外宣队的突击队"], *Military Correspondent*, June 2015, pp. 53–54.

[114] RAND Interview #2.

[115] Elizabeth Bumiller and Michael Wines, "Test of Stealth Fighter Clouds Gates Visit to China," *New York Times*, January 11, 2011; Wong, 2011; Sam LaGrone, "China's First Domestic Aircraft Carrier Almost Certainly Under Construction," USNI, September 30, 2015. For PLA articles on the value of letting sensitive military information be revealed through nonauthoritative or foreign sources, see Ding Chunguang and Ma Gensheng,

Spreading Fake News

In addition to using trolling to try to swamp the Twitter accounts of regime critics like Guo Wengui, Chinese officials have attempted to distribute false, incorrect, exaggerated, or fabricated information through official, unofficial, covert, or clandestine social media accounts created or operated by either human propagandists (五毛党) or artificial intelligence bots (机器五毛党).[116] To date, the number of instances in which China has deliberately engaged in a targeted push of such "fake news" appears to be relatively rare, and all known cases have been exclusively found in Taiwan.[117] China is reported to have manufactured disinformation against the Tsai administration about religion, retirement, and infrastructure.[118] As J. Michael Cole argues,

> Beijing also knows it can rely on traditional media in Taiwan to amplify the [disinformation] message through their own coverage, which—due to the competitive nature of Taiwan's media environment—often entails poor fact-checking and attribution. Thus, a piece of (dis)information (or "fake news") originating in China will often go through a process of circular corroboration by replicators—traditional and online media—in Taiwan. As a

---

"Effectively Controlling Lively Spokesmen—on the Control of the Dissemination of Major Military News," *Military Correspondent*, April 2011; Liu Yi, "Public vs. Secret: Military News Releases," *Military Correspondent*, August 2009.

[116] As noted throughout this chapter, the overwhelming body of research reviewed for this study suggests that China's main means of engaging online is through human operators, not computer programs or artificial intelligence.

[117] A possible counterpoint to this is a recent report claiming that Chinese internet search giant Baidu purportedly investigates more than three billion fake news claims per year. It is unclear whether any of the claimed "fake news" stories include content deliberately fabricated by Chinese authorities or not; it is also possible that some of these include real stories that the PRC government, seeing them as unfavorable, decides to label as "fake news" ("China's Biggest Search Engine Baidu Looks Into 3 Billion Fake News Claims a Year," Bloomberg, October 10, 2017).

[118] For an overview of recent Chinese disinformation campaigns against Taiwan, see J. Michael Cole, "Will China's Disinformation War Destabilize Taiwan?" *National Interest*, July 30, 2017b; J. Michael Cole, "China Intensifies Disinformation Campaign Against Taiwan," *Taiwan Sentinel*, January 19, 2017a; Ying Yu Lin, "China's Hybrid Warfare and Taiwan," *The Diplomat*, January 13, 2018.

> result, this (dis)information is normalized and becomes part of the narrative. Subsequently, the (dis)information becomes the subject of heated debates on evening TV talk shows, compelling the embattled (and distracted) government to respond with denials or corrections. [119]

One China-originated rumor from mid-2017 claimed that the Tsai administration had banned the burning of incense and "ghost money" in Taoist temples. This rumor, spread through social media, appeared to have links back to China and ultimately led to a mass protest in Taipei, where an estimated 10,000 people turned out to demand that the government lift the ban (in fact, there was never a ban, so there was no ban to lift).[120] Taiwan's National Security Bureau asserted that China also used Weibo, WeChat, LINE, and other online media platforms to spread rumors that President Tsai would reform Taiwan's pension system and was threatening to cut off payments for those who left the country.[121]

China also reportedly funded a pro-unification website in Taiwan, *Fire News*, that was nominally run by a Taiwan political party, with the hope of penetrating the Taiwan military, though it is unclear whether this website trafficked in fake news.[122] This offensive social media oper-

---

[119] Cole, 2017b.

[120] "Authorities Deny Rumor of Ban on Incense, Ghost Money Burning," Central News Agency (Taiwan), July 21, 2017; "Taiwan's Taoists Protest Against Curbs on Incense and Firecrackers," BBC News, July 23, 2017; David Spencer, "Is the Incense Ban Furor More Than Just Simple Fake News?" *Taiwan News*, July 27, 2017. As Spencer's piece notes, "Media investigations of the document, which purports to be an official government document proposing an outright ban, have shown that the original version was in fact in simplified Chinese [RAND author's note: Taiwan uses classical Chinese characters, whereas simplified characters are used in China] and originated on COCO01.net, an online content farm with a track record of publishing false information about Taiwan."

[121] "National Security Unit: Anti–Pension Reform Protests Had Intervention from Chinese Forces" ["國安單位：反年改陳抗 有中國勢力介入"], *Liberty Times*, July 18, 2017; "Taiwan Cuts 18 Pct Interest in Civil Service Pension Reform Bill," Reuters, June 27, 2017; "Taking on Taiwan's Ruinous and Partisan Pension System," *Economist*, May 18, 2017.

[122] Huang Chien and Hsieh Chun-lin, "Prosecutors: China Paid Wang for Propaganda," *Taipei Times*, January 3, 2018; Jason Pan, "Military Men Probed over Wang Ties," *Taipei Times*, January 4, 2018.

ation was, in fact, an intelligence gathering operation. It was meant to be accomplished in part through *Fire News'* social media presence, as the Chinese government offered cash to Taiwanese military personnel for their social media engagement, specifically their "likes" and other interactions on the *Fire News* Facebook page. According to reporting in Taiwan, "For closer two-person exchanges in which the contact opened up about their feelings regarding politics and deeply personal information, a reward of NT$50,000 was to be given."[123] We could find no similar credible claims of such Chinese disinformation campaigns in other countries.

China's Self-Restraint in Using Social Media

Juxtaposed against this range of offensive actions using social media, the Chinese government appears so far to have restricted its embrace of social media in some ways that would help with its manipulation of foreign public opinion. Most notably, there is little to no evidence that China uses bot-operated platforms.

Giving Up on Bots, for Now

This engagement by the Chinese state on Western social media platforms appears to be largely human-operated and not run by bots. According to one recent report by Oxford researchers, "The Chinese state has given up the fight over discourse on Twitter [using bots], both in English and in Chinese."[124] The one recent exception may be against the dissident Guo Wengui, but the fact that the Chinese had to resort to Russian bots in a hurry to spam Guo's account reinforces our finding that the Chinese themselves do not have the necessary bot infrastructure on Twitter. Others have argued that China used bots on Twitter to criticize Marriott International for its website's categoriza-

[123] Huang and Hsieh, 2018.

[124] Bolsover, 2017. A similar conclusion was reached for Chinese social media propaganda against Taiwan (Monaco, 2017).

tion of Tibet as a separate country, but the authors were unable to corroborate this claim.[125]

This, however, does not mean bots are not actively posting about China on Twitter; the Oxford report found that anti-China dissident groups, including prodemocracy and pro-Tibet activists, have likely created their own armies of bots to spam Chinese language speakers.[126] Moreover, as another Oxford report concludes, "these facts do not preclude usage of malicious political bots in future Chinese propaganda efforts, but they lead to the conclusion that bots do not currently play a central role in China's official propaganda apparatus."[127]

Effectiveness of China's Efforts

Despite China's extensive information operations around the world, it is difficult, if not impossible, to find clear evidence of their effect on foreign public opinion toward China (see Figure 4.7). According to a wide range of public opinion surveys, China's favorability has been decreasing in most places around the world. In the United States, opinion has trended downward since 2011 but has always been fairly negative.[128] To be fair, Chinese information operations may have been effective in forestalling an even greater drop in favorability, and thus the gains from these operations may be largely hidden. It is difficult to assess what impact China's social media activities have in supporting foreign public opinion, but it is clear the Chinese government views that as an important vector for such influence.

However, a growing body of Chinese research into China's favorability around the world suggests that the CCP has reason to be concerned with its global reputation. China recognizes that its gover-

---

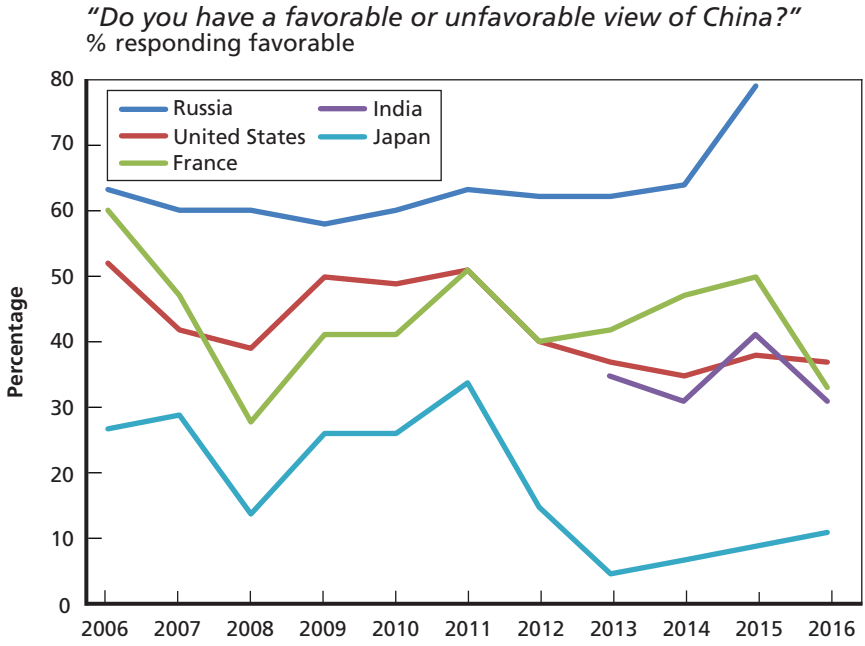
[125] Josh Rogin, "How China Forces American Companies to Do Its Political Bidding," *Washington Post*, January 21, 2018. For the Marriott Twitter post in question, see Marriott Corporation, tweet, Twitter, January 10, 2018.

[126] Bolsover, 2017.

[127] Monaco, 2017.

[128] "China Is Spending Billions to Make the World Love It," 2017.

Figure 4.7
Global Opinion of China

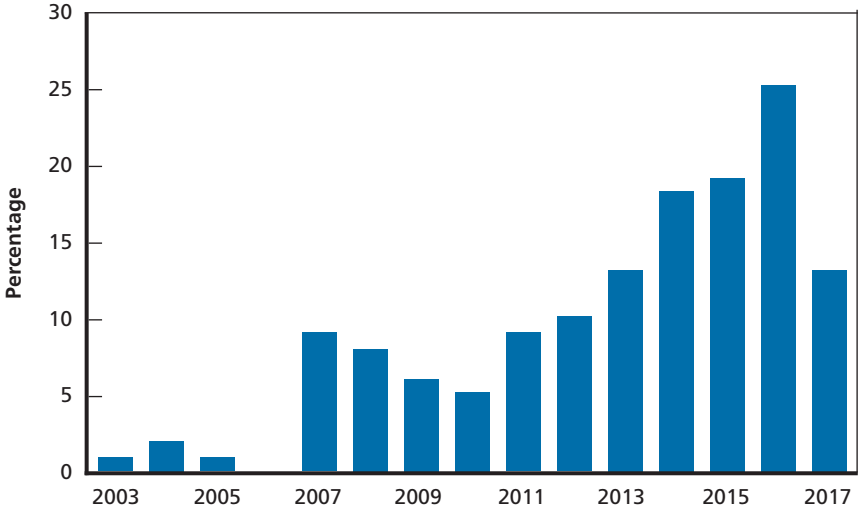


SOURCE: Pew Research Center, undated.

nance model is relatively unattractive and that its growing economic and military power naturally provoke concerns among neighbors and other global actors. As indicated by Figures 4.8 and 4.9, Chinese journals have devoted an increasing amount of attention over the past two decades to the issues of foreign public opinion and how to shape it.

China often favors economic solutions to its foreign policy challenges and has spent significant sums on high-profile public projects to curry favor with local populations abroad. China has engaged successfully with selected world leaders by bestowing foreign investment, favorable economic terms, and direct monetary incentives, which promote favorable international discourse about China. Yet in the end, the impact of these efforts is still unclear.

Figure 4.8
Chinese Journal Articles on Foreign Public Opinion of China



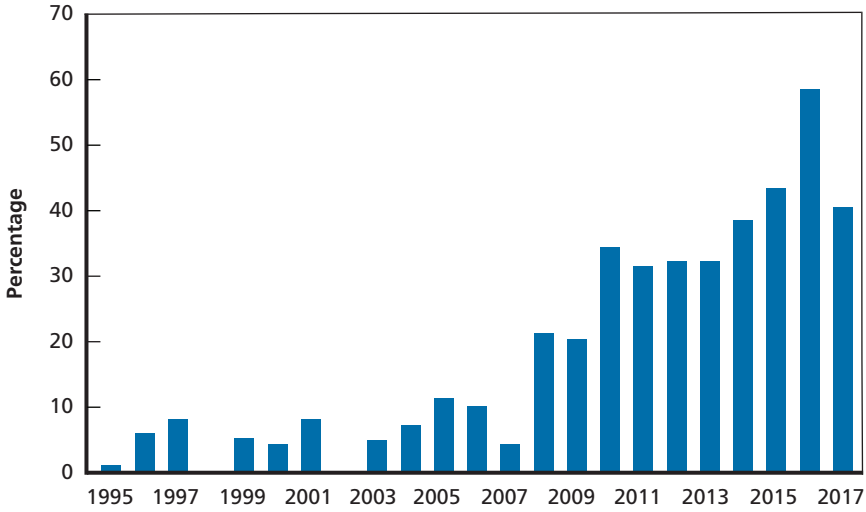
SOURCE: CNKI, 2017 data through August. Search term for all Chinese journals was "涉华舆情."

One successful aspect of China's information operations has been its penetration of Western social media platforms.[129] Since joining Twitter and Facebook in 2011 and 2013, respectively, *People's Daily* now has accumulated 4.4 million and 41 million followers, respectively. English-language versions of any Chinese government–affiliated social media accounts that we identified have predated their Chinese-language versions, suggesting that the driving interest has been engaging foreigners, not Chinese citizens abroad. Most recently, the Chinese embassy in Washington, D.C., joined Facebook, declaring that "by engaging with the American people on social media, the embassy hopes to open new flows of communication."[130] One attempt to catalog all known Chinese government–affiliated accounts on Western social media found at least 75 accounts on Twitter, at least 60 on Facebook,

[129] Paul Mozur, "China Spreads Propaganda to U.S. on Facebook, a Platform It Bans at Home," *New York Times*, November 8, 2017b.

[130] "Chinese Embassy in US now on Facebook," *China Daily*, February 13, 2018.

Figure 4.9
***International Communications* Articles on Shaping Foreign Public Opinion of China**



SOURCE: CNKI, 2017 data through August. Search term was "(国际舆论 or 海外舆论) and 引导."

and at least ten on Instagram, though this is unlikely to be exhaustive.[131] Another aspect of China's propaganda outreach is mobile applications for its media organizations, including China Global Television Network (CGTN), which has delivered over 1 million downloads on the Android platform.[132] A selection of Chinese state-run social media accounts can be found in Table 4.2, indicating the Chinese government's desire to shape foreign discourse about China. It should be

[131] "Table of Chinese Foreign Propaganda Accounts for News on Twitter" ["Twitter中国外宣帐号列表之新闻类"] *Medium*, November 12, 2017; "Table for Chinese Foreign Propaganda Pages for News on Facebook" ["Facebook中国外宣专页列表之新闻类"], *Medium*, September 17, 2017; "Table of Chinese Foreign Propaganda Accounts on Instagram" ["Instagram中国外宣帐号列表"], *Medium*, December 19, 2017.

[132] For a brief discussion of CGTN's social media strategy, see Yu Xiaoqing, "The Growth of China's Outreach Flagship Media: 20 Years of Transformation of an English Anchorwoman" ["中国外宣旗舰媒体成长记：一位英文女主播的20年蜕变"], *The Paper*, April 1, 2017.

Table 4.2
Select Chinese Government and Media Accounts on Western Social Media Platforms

	Twitter Account Created (Year)	Twitter Followers	Facebook Account Created (Year)	Facebook Followers
Global Times (English)	2009	459,000	2012	18 million
China Daily	2009	1.6 million	2010	32 million
CCTV (English)	2009	482,000	2009	46 million
People's Daily (English)	2011	4.4 million	2013	41 million
Xinhua	2012	11.7 million	2012	39 million
People's Daily (Chinese)	2013	196,000	n/a	n/a
CCTV (Chinese)	2013	1,000	2014	3 million
CGTN	2013	6.2 million	2013	55 million
State Council Information Office (SCIO)	2015	10,000	2015	180
Sinopec	2015	21,000	2016	1 million
China-Pakistan Economist Corridor	2016	101,000	n/a	n/a
Global Times (Chinese)	2017	1,000	2016	5,000

NOTE: Chinese government–affiliated accounts are also present on a wide range of platforms, including YouTube, Instagram, and Snapchat.

noted that while these accounts currently support China's broader propaganda efforts, they could easily be used for more malign purposes in the future, especially a conflict scenario, with a vast audience already harnessed through peacetime activities.

It is difficult to gauge how much the Chinese government is spending on propaganda in foreign countries, but one U.S. scholar has

estimated $10 billion per year.[133] Individuals connected to the Chinese government have also spent millions buying foreign media, including $260 million for the *South China Morning Post*, the most widely read English-language newspaper in Hong Kong. The government has paid to place news-like propaganda supplements in prominent foreign newspapers;[134] has been playing propaganda videos on billboards in New York City's Times Square since at least 2011, likely at a cost of millions of dollars; and has debuted special videos for then-President Hu's state visit to Washington in 2011 and again following the 2016 international ruling that largely voided Chinese territorial claims in the South China Sea.[135]

China's "advertising" spending on Western social media is equally opaque, but recent *New York Times* reports confirm that the Chinese government does pay to deliver its propaganda to foreign audiences. According to one report, China "spends hundreds of thousands of dollars" on Facebook advertising alone to promote its content on the network.[136] According to another, "an editor at China's state-run news agency, Xinhua, paid [a company] for hundreds of thousands of followers and retweets on Twitter," with the intent of helping Xinhua expand its reach on the social media platform.[137] This lines up with earlier reporting that Xinhua's Twitter followers were growing at an unnatural rate and suggests that other Chinese propaganda organizations may also be buying followers and influence on Western social

---

[133] David Shambaugh, "China's Soft-Power Push," *Foreign Affairs*, July 2015.

For various attempts to catalog Chinese propaganda spending, see "China Is Spending Billions to Make the World Love It," 2017; Jamie Smyth, "China's $10bn Propaganda Push Spreads Down Under," *Financial Times*, June 9, 2016; Anne-Marie Brady, "China's Foreign Propaganda Machine," *Journal of Democracy*, Vol. 26, No. 4, October 2015.

[134] Chris Buckley and Jane Perlez, "By Buying Hong Kong Paper, Alibaba Seeks to Polish China's Image," *New York Times*, December 13, 2015.

[135] Kristina Cooke, "China News Agency Leases Plum Times Square Ad Space," Reuters, July 26, 2011; Angela Doland, "Watch the Chinese Propaganda Ad Playing 120 Times a Day in Times Square," *AdAge*, July 27, 2016.

[136] Mozur, 2017b.

[137] Nicholas Confessore, Gabriel J. X. Dance, Richard Harris, and Mark Hansen, "The Follower Factory," *New York Times*, January 27, 2018.

media.[138] Clearly, the Chinese government is willing to exploit U.S. social media companies for its propaganda purposes.

2016 U.S. Election: Interference Deferred

No evidence has surfaced to suggest that the Chinese government interfered with the U.S. 2016 election. The U.S. intelligence community report on Russian interference in the election and testimony on the topic by many current and former senior U.S. officials did not suggest China played a role in manipulating the 2016 election.[139] While China does not appear to have engaged in widespread or targeted disinformation efforts intended to interfere with another country's electoral outcomes in the way Russia is widely suspected of having influenced U.S., British, and other European electoral or referendum results, China's growing international influence, especially the rise of Chinese-language social media applications owned by Chinese companies, suggests that the PRC may be in the position to attempt to influence U.S. politics in the future, if it so chooses.[140]

Articles reviewed for this study also did not suggest a strong correlation between Chinese propaganda and major U.S. campaign issues, except for populism and immigration, which both spiked in prominence in 2017.[141] However, at least some Chinese analysts believed that

---

[138] Tom Grundy, "Did China's State-Run News Agency Purchase Twitter Followers?" *Hong Kong Free Press*, April 14, 2015; Alexa Olesen, "Where Did Chinese State Media Get All Those Facebook Followers?," *Foreign Policy*, July 7, 2015.

[139] Former White House Chief of Staff Reince Priebus in July 2017 suggested that China and North Korea also interfered with the 2016 election, but this was later clarified to refer to broader hacking activities not specifically targeted at the election ("Reince Priebus Breaks Down Trump's Trip to the G-20 Summit," Fox News, July 9, 2017; Jason Silverstein, "North Korea and China Also Interfered in U.S. Election, Reince Priebus Says," *New York Daily News*, July 9, 2017).

[140] This was the conclusion too of a *New York Times* report in early November 2017. See Mozur, 2017b.

[141] Relevant articles include Zhai Huixia, Xie Lianghong, and Yu Yunquan, "New Perspective on Western Research on 'China Model' Since Global Financial Crisis" ["国际金融危机以来西方对 '中国模式' 研究的新视角"], *International Communications*, January 2012; Zhou Xinyu and Feng Bo, "Foreign Communication of Chinese Values Under the Waves of Populism in the West" ["西方民粹主义浪潮下的中国价值观对外传播"], *International*

the wave of populism in the West presented an opportunity for Chinese propaganda. One article claimed that as the West is "enveloped" in a "crisis of spirit," this presents a "new opportunity for the foreign communication of Chinese values." To seize this moment, Chinese propaganda should "tell different stories to different audiences," and this tailored messaging would pertain to "the elites vs the common people, Christians vs Muslims, locals vs immigrants, whites vs Asians and Blacks, as well as people opposed to vs supportive of globalization."[142] our research did not find much further analysis on targeted messaging, but this "new opportunity" suggests there may be future interest in refining the granularity or nuance of propaganda efforts aimed at groups that may have outsized impacts on election outcomes.[143]

One noteworthy aspect of a Chinese role, if not state interference, in the 2016 U.S. election was an effort to mobilize Chinese-American

---

Communications, February 2017; Xu Xiujun, "Foreign Communication of Chinese Global Governance Ideas Under Counter-Globalization Trend" ["逆全球化思潮下中国全球治理观的对外传播"], *International Communications*, March 2017; Yan Liang, "Global Changes and Foreign Communication Responses After Trump's Taking Office" ["特朗普上任后的世界变局与对外传播应对"], *International Communications*, February 2017; Xiao Fei and Caichan Minbao, "Analysis of Online Public Opinion Dangers and Online Public Opinion Guidance Countermeasures for Overseas Border Conflicts" ["涉外边境冲突的网络舆情风险与舆论引导对策探析"], *International Communications*, August 2016; Zhao Qinghai, "New Western Reflections on Globalization" ["西方对全球化的新反思"], *International Communications*, January 2008; Liu Yang, "Thoughts on Change of U.S. Administration and Adjustments to China's International Communications Strategy" ["对美国政府更迭与中国对外传播策略调整的思考"], *International Communications*, February 2017; Kou Liyan, "Strategic Communications in the 'Micro-Struggle'—The Impact and Response of Trump Entering the White House on China's Strategic Communications" ["在"微斗争"中开展战略传播—特朗普入主白宫对中国战略传播的影响及应对"], *International Communications*, February 2017; Wu Xu, "Trump's 'Twitter Diplomacy': China's International Communications Facing New Challenges" ["特朗普的"推特外交":中国对外传播面临的新挑战"], *International Communications*, February 2017.

[142] Zhou and Feng, 2017.

[143] One article did provide an in-depth analysis of the demographics of U.S. presidential candidates' Instagram followers, which could be one future vector for nuanced propaganda (Wang Bin and Chen Yu, "Political Figures' Campaign Concept as Shown Through Social Media—Taking Hilary and Trump's Instagram Accounts as Example" ["政治人物在社交媒体上的竞选理念呈现—以希拉里和特朗普的Instagram账号为例"], *International Communications*, September 2016, pp. 62–65).

voters through WeChat.[144] WeChat is a semiprivate messaging application owned by Tencent, a Chinese internet company with close ties to the Chinese government. WeChat has an estimated 100 million users outside China, with an estimated "few thousand WeChat groups in the U.S. with political and social issues themes."[145] Numerous reports indicate that Chinese-Americans initiated political groups on WeChat with the intent to mobilize voters for their preferred candidate, mostly Trump.[146] According to one report, "Chinese-American blogger Xie Bin and seven others launched a WeChat page aimed at influencing Chinese-Americans to vote for Trump."[147] The article focuses on the vulnerability of WeChat, like Western social media platforms, to fake news: "WeChat's design does not make it easy to fight biases or fake news. Information on the platform spreads quickly within and between WeChat groups, but the sources of information—and therefore their verifiability—are de-emphasized [. . . .] One of the main challenges that WeChat and other closed networks will face is the difficulty of verifying information in a system that does not value verification." Some Chinese-American voters claimed that WeChat "played a significant role in mobilizing Trump's Chinese supporters. It was

---

[144] For an overview of Chinese-Americans in the 2016 election, see "Chinese-Americans Are Becoming Politically Active," *Economist*, January 19, 2017.

For an overview of WeChat's entrance into the United States, see Emily Parker, "Can WeChat Thrive in the United States?" *MIT Technology Review*, August 11, 2017.

[145] Louise Lucas, "Questions over Pace of Growth As Wechat Nears 1bn Users," *Financial Times*, August 30, 2017; Mengzi Gao, "Chinese Trump Supporters Thank WeChat," *Voices of New York*, November 11, 2016.

[146] Esther Wang, "Conservative Chinese Americans Are Mobilizing, Politically and Digitally," *Pacific Standard Magazine*, October 11, 2017; Liu Zhen, "How One Chinese American Became Politically Aware . . . and Joined the Ranks of Trump Supporters," *South China Morning Post*, November 2, 2016; Kate Linthicum, "Meet the Chinese American Immigrants Who Are Supporting Donald Trump," *Los Angeles Times*, May 27, 2016; Andi Wang, "Meet Some of the Chinese Americans Voting for Trump," PBS, August 20, 2016; Jessica Stone, "Chinese-Americans Voters Mobilize Ahead of US Election," CGTV, November 1, 2016; "独家：用中国社交网 在美华裔组建特朗普支持团," *Sina*, May 11, 2016; Stephanie Zu, "揭秘特朗普最大华裔助选团 组织集资全靠微信," *Sohu*, November 6, 2016.

[147] Eileen Guo, "How Wechat Spreads Rumors, Reaffirms Bias, and Helped Elect Trump," *Wired*, April 20, 2017.

more powerful than any other promotion tools," and the discourse on WeChat apparently had an impact on the Chinese-language media in California.[148] There are no indications there was any Chinese government support or involvement in these activities, but the reliance of U.S. political activities on Chinese-hosted platforms raises questions about potential future censorship or manipulation.

Moreover, there is evidence the Chinese government is interested in activating Chinese-Americans to play a more "positive" role in setting the course of U.S.-China policy, as one article criticized Chinese-Americans for being a "silent group" in the electoral process and allowing China to become a "scapegoat" for U.S. politics, implicitly arguing that making them more proud to be Chinese would "improve how Americans see China."[149] Chinese researchers have also published articles on factors affecting Chinese-American political participation in both voting and running for office.[150]

It is not beyond the imagination to project a future election, at any level of government and for any country, where the Chinese government orders Chinese-owned social media platforms to censor views critical of China and/or views critical of China's preferred candidate. This censorship would qualify under the report's definition of hostile social manipulation because it would seek to have a malign and harmful impact on social discourse about U.S. domestic politics and shape the election in China's favor. This would probably be predominantly, if not exclusively, targeted at Chinese-Americans, due to some of the population's consumption of primarily Chinese-language information. From a Chinese perspective, such operations might be considered

---

148 Gao, 2016; Grace Wyler, "What Do Chinese-Americans Think of Trump's Tough China Talk? We Asked Them," *Los Angeles Daily News*, January 4, 2017.

149 Tan, 2016, pp. 13–14.

150 Ye Xiaoli and Gu Haoyu, "The Factors on Election Campaign of Modern Chinese-American: Based on the Analyses of Sustainability" ["当代美国华人竞选影响因素: 基于可持续性的分析"], *Overseas Chinese Journal of Bagui*, September 2017, pp. 31–38; Ye Xiaoli and Gu Haoyu, "The Analysis for Influence Factors of Chinese-American Political Participation: Take the Protesting Action to the Insulting Chinese for an Example" ["当代美国华人政治参与影响因素分析: 以抗议ABC辱华行动为例"], *Overseas Chinese Journal of Bagui*, June 2015, pp. 13–20.

defensive in orientation, since they would seek to blunt or eliminate criticism of China, and the Chinese government likely could tailor the censorship to an allegedly offensive user's registered location or even geolocation. Moreover, this operation would be largely invisible to users unless they double-checked the content of their conversations through another method.[151] While it would be difficult to argue that such actions would directly affect the outcome of an election, they would certainly shape public Chinese-American discussion and potentially reinforce existing beliefs in the absence of robust debates over campaign issues. This approach would stand in contrast with the Russian model, since Russia does not control social media platforms used by many U.S. citizens who speak Russian, and the Russian-language population in the United States is far less than that of Chinese speakers.[152] One example of this is that, in February 2018, WeChat reportedly began blocking the *New York Times* from opening inside its application for users located outside of China.[153]

Conversely, a 2012 article in the PLA's *Military Correspondent* heralded the work of a Chinese-language newspaper in Texas that hewed to the CCP's narrative, noting that "one out of four ethnic minorities in the United States relies upon media in their mother tongue to get information and express their feelings, and the influence of these media surpasses that of the media of the country in which they reside."[154] The article claimed that "over the past few years, the [newspaper] has

---

[151] The Canadian internet freedom nongovernmental organization Citizen Lab has found that WeChat can censor commentary without alerting the sender that his or her message was not received by the intended recipient. This is currently only for China-based accounts, and censorship is focused mostly on group chats, but this censorship could very likely be extended to international accounts (Lotus Ruan, Jeffrey Knockel, Jason Q. Ng, and Masashi Crete-Nishihata, "One App, Two Systems: How WeChat Uses One Censorship Policy in China and Another Internationally," Citizen Lab, November 30, 2016).

[152] According to the 2010 Census, nearly 3 million people in the United States speak Chinese at home while roughly 850,000 speak Russian. See: "Number of Russian Speakers in U.S. Quadruples in 30 Years, Census Report Says," *Moscow Times*, August 8, 2013.

[153] Amy Qin, Twitter, February 1, 2018.

[154] Yu Baozhu, "The 'Chinese Times' [Huaxia Shibao] Builds a Bridge of China–US Cultural Exchange," *Military Correspondent*, January 2012, p. 54.

energetically publicized and supported ethnic Chinese individuals participating in politics and running for public office such as mayor, state representative, city councilor, and district court justice, and it has some influence in the overseas Chinese community." The article further described the owner as attending a SCIO training seminar in China for overseas Chinese-language media and singing a media-inspired version of "We Are the Heirs of Communism," which hails the media role in serving China.

Chinese propaganda officials have long been conscious of the power of social media in U.S. political movements. For example, a 2010 article in the Publicity Department's official journal noted that the U.S. Communist Party had set up a dedicated multi-media team and was using its Twitter and Facebook accounts to expand its influence, while a 2011 article highlighted the important role social media played in the Occupy Wall Street protests.[155] Whether the Chinese government attempts such interference in future elections is likely to be determined by many factors only partly influenced by the U.S. government.

Conclusions and Implications for U.S. Policy

In summation, China's uses of social media appear largely focused on controlling information about China itself and shaping global narratives about China that circulate overseas, especially among targeted communities of interest, such as ethnic and religious minority groups; Chinese dissident groups; and key influence agents, such as foreign media, cultural outlets, academics, and government decisionmakers. The most interesting evidence of China using social media to spread propaganda to shift external political sentiment appears to be with respect to Taiwan. Given the sensitivity and importance of Taiwan to China's official self-identity and narrative, this is perhaps unsurprising.

---

[155] Chen Shuoying, "U.S. Communist Party Seeks Development in Changing World" ["美国共产党在变化的世界中寻求发展"], *Party Construction*, June 2010; Shen Shishun, "'Occupy Wall Street' Wasn't By Chance" ["'占领华尔街'并非偶然"], *Party Construction*, December 2011.

China's Operations Will Likely Grow Bigger and Stronger

China's information operations today are immature compared with those of Russia. As one study reviewed for this research suggested, "China's leadership struggles with credibility in social media," and China is still learning how to convey propaganda online in a way that is less stilted and more effective.[156] The CCP's much-feared Central Discipline Inspection Commission confirmed this finding in June 2016 when it reproved the Party's Propaganda Department for distributing news propaganda that was poorly targeted and insufficiently effective.[157]

Disturbingly, the Party appears to have resolved to redouble its efforts and devote even more resources to information control and messaging. This suggests that China's officials may become increasingly sophisticated in their messaging in the years ahead, since they have substantial room for improvement; some reports already suggest efforts to make official propaganda more attractive by experimenting with cartoons, folk rock ballads, rap, and other forms of entertainment.[158] While some of these initial attempts to make propaganda more attractive and credible may fail, Chinese officials are likely to learn what works and what doesn't over time and get better.

Under Xi Jinping, China appears to have identified the improvement of propaganda content, delivery, and reception as increasingly important goals. One leading observer of Chinese media policy has warned that China's efforts to insulate its regime from criticism and to build influence abroad may include efforts to export China's censorship and content fabrication technologies and experiences to other authoritarian regimes worldwide, representing a separate challenge that

---

[156] Shi-Kupfer, 2016.

[157] "China's Propaganda Department Not Good Enough at Propaganda—Gov't," *Hong Kong Free Press*, June 9, 2016.

[158] "China's Five-Year Plan Now Has Its Own Psychedelic Music Video," *Wall Street Journal*, October 27, 2015; Amy X. Wang, "China's Government Has a Bizarre Official Rap Song, Featuring President Xi Jinping," *Quartz*, December 31, 2015; Josh Horvitz, "China's Military Has Released a Rap Video in Order to Lure More Recruits," *Quartz*, May 3, 2016; Hannah Beech, "Communist Chinese Rap 'This Is China' Attacks Western Media," *Time*, June 20, 2016.

could come from the proliferation of information control and fabrication technologies.[159]

Watch Taiwan for What Comes Next

Taiwan has often borne the brunt of China's foreign propaganda, and it appears that the Chinese government may be targeting Taiwan with its most aggressive and most advanced social manipulation efforts. As described above, Taiwan has been subjected to the PLA's clearest intimidation, the most likely case of Chinese disinformation, the most obvious case of Chinese netizens supporting CCP propaganda on foreign social media, and China's first extrajudicial punishment for social media posts outside of China (levied against a citizen of Taiwan). China is likely to expand the use of some or all of these tactics beyond Taiwan in the coming years. The U.S. government could benefit from increasing its dialogue and cooperation with its Taiwanese counterparts on countering Chinese social manipulation operations, both to support Taiwan's democracy and to better understand and prepare for future Chinese efforts around the world.

China's Operations Blur the Line Between Defensive and Offensive

As documented in the previous chapter, Russia's social manipulation efforts have partly taken the approach of aggressively targeting discrete audiences and pushing fabricated content at them to play to their political prejudices so as to create division and social strife. In contrast, China's uses of social media for propaganda appear to be part of a much more general but less obvious attempt to delete, manage, and ultimately control information about China both within and beyond its borders with the goal of making the world safe for the CCP, normalizing it, and extending its influence. While potentially less blatant, less risky, and less aggressive, China's approach nonetheless carries significant risks for U.S. interests (and upsides for Beijing)—risks including the accelerating use of informational tools to reach outside China to

[159] Sarah Cook, "China's Party Congress Hints at Media Strategy for a 'New Era,'" *The Diplomat*, November 4, 2017b.

punish opponents, deter criticism, and achieve specific economic and political effects.

A 2017 article on countering anti-China media abroad reveals how the line between defensive and offensive goals can be blurred to justify subversive attacks on non-Chinese citizens abroad.[160] The authors argue that anti-China media, especially Chinese-language media such as *Epoch Times* or Voice of America, pose a threat to the Party and domestic stability because of their ability to promote a negative image of China, brainwash Chinese living overseas, leak state secrets, and infiltrate back into China. The article's policy recommendations include increasing the monitoring of foreign public opinion, expanding the reach of China's foreign propaganda efforts, and controlling Chinese social media used by Chinese living abroad. Lastly, the authors suggest the Chinese government should actively "sanction and attack" these hostile media organizations through "diplomatic, educational, technical [. . .] and legal" methods, and work to sow division between the employees of the organizations to make them abandon their anti-China stance.

Chinese-Americans Need U.S. Government Outreach

Like their Russian counterparts, PRC officials appear to regard ethnic Chinese communities living outside of China as particularly attractive vectors for influence operations. This calculation underscores the importance of working with the Chinese-American community to ensure that (a) they feel welcomed by the U.S. government and (b) they know resources are available to help combat Chinese attempts to target them and turn their loyalty away from the United States. This calculation also points to (c) the need to help sensitize the Chinese-American community to the threat posed by Chinese propaganda, and (d) the desirability of authentic, Chinese-language content to counter Chinese information and influence operations.

---

[160] Wu Feng and Li Yaofei, "The Latest Status and Operation Model of Overseas Anti-China Media and Countermeasures" ["境外反华媒体的最新态势，及应对策略"], *Journal of Intelligence*, March 2017, pp. 36–42.

In conclusion, China's uses of social media for hostile social manipulation are substantial and appear poised to grow both more extensive and more sophisticated in the years ahead. Meeting this challenge will require an understanding of the organizational actors, goals, messages, and actions by which China seeks to exercise influence via social media.

CHAPTER FIVE

Does Hostile Social Manipulation Work? Measures of Success in Russian Activities in Europe and the United States

The rise of hostile social manipulation as a strategy, and the extensive campaigns conducted by Russia and China as surveyed in the last two chapters, has led to urgent warnings about the effect on Western democracies. Democracy is now "vulnerable to attack by foreign adversaries in new and powerful ways," one analysis claimed. "Fear and uncertainty are Americans' greatest weaknesses," it continued, and hostile influence operations could help produce a "distracted, inward-looking America afraid of its own shadow."[1]

Such concerns are apt, given the intentions of the major information manipulators and the emerging technologies that could empower their social manipulation campaigns. Yet warnings about the potential effect of social manipulation often take for granted one of the most important aspects of the issue: The actual effect such campaigns have on beliefs, attitudes, and behavior.[2] It turns out to be extremely difficult to measure such effects, in part because of the blizzard of variables that go into shaping what people think and do. Such campaigns are often designed to intensify the views of people who already believe certain things, and it can be almost impossible to evaluate the change in attitudes or conviction. Many of the existing measures of the effects of social manipulation campaigns look to data such as the number of

[1] Laura Rosenberger, "Shredding the Putin Playbook," *Democracy Journal*, No. 47, Winter 2018.

[2] On this issue, see Carina Storrs, "How Effective Are Misinformation Campaigns to Manipulate Public Opinion?" *Scientific American*, September 29, 2017.

times viewers clicked through onto content or "liked" a post, which do not necessarily reveal very much. There are significant groups, both ideologically motivated and profit-driven, who have been responsible for much more of the spreading of malicious information than Russia; Russian activities often pair those and reinforce those trends, but they do not create them.

To be clear, we have repeatedly argued in this report, the fact that a foreign power undertook such a campaign should spark great concern among the governments and citizens of every country affected by Russian social manipulation. This is true almost regardless of the outcomes of those campaigns: No matter their effectiveness, the United States and other targets of these techniques must work to ensure that such manipulation cannot happen in the same way again. At the same time, it remains important to understand whether the campaigns have been effective in achieving their states' outcomes. The U.S. and international response can be informed with a sense of whether Russia is rapidly achieving momentum in the geopolitical outcomes it desires.

In fact, at this writing, there remains scant evidence of how effective the most well-known social manipulation campaigns have been in achieving their objectives, or even what those objectives specifically were, in some cases. Yet without such evidence, there is little basis for judgments about the risks—or lack of them—resident in Russian and Chinese campaigns of social manipulation.[3] To get some sense of whether and how such campaigns can have meaningful effects, we evaluated evidence on outcomes of Russian social manipulation campaigns targeted at the United States and Europe that have so far taken place. We looked at two classes of evidence: the current condition of some indicators, to have a sense of whether their status reflects what Russia would want; and the trends in indicators, where evidence is available, of the shifts over the past three to four years.

The sum of this evidence does not allow a strong judgment about the effects of existing social manipulation campaigns. They have clearly

---

[3] Braden R. Allenby, "The Age of Weaponized Narrative," *Issues in Science and Technology*, Summer 2017, p. 66, admits that "experts disagree on whether these techniques were decisive in the Brexit vote or the US election" but then suggests that "that is beside the point."

pushed a great deal of content into the public debate and generated measurable outputs in social media activity, such as views and shares. In a very few cases, specific outcomes can be identified—such as an anti-Trump political protest sparked by a Russian Facebook post. But apart from such anecdotal cases, for the time being we have no authentic way of knowing their larger effect on attitudes or behavior. Most of what is known so far is in terms of abstract statistics of production and viewership (what might be termed *output* measures)—how many posts were made by Russian-controlled sites, how many people may have clicked on or "liked" them. This information tells us very little, however, about beliefs or attitudes: What did people think *before* they saw the posts? Did they change their thinking or likely behavior? Even the basic statistic of retweeting a post does not indicate whether the person was retweeting it to support or condemn the message.

To gain a better sense of the possible effectiveness of such campaigns, we reviewed available evidence about the effects of known campaigns. Existing campaigns with measurable data at this point are almost entirely of Russian origin and focused on the United States and Europe. Because it is so difficult to disaggregate the effects of social media or disinformation campaigns from other variables—and even within those, to identify the specific effects of Russian activities—we looked at *outcome effects* that the Russian campaigns might be seeking. If these campaigns are succeeding, we ought to see movement in the directions Russia desires in several indicators, including[4]

1. Public opinion toward Russia in the target countries or in specified subpopulations. This includes general favorability ratings,

[4] Another outcome that Russia appears to seek is the strengthening of right-ring or populist parties throughout Europe with some sympathy for Moscow. We investigated this issue in some depth but concluded that the variables at work in the waxing and waning of those parties are so complex that the factor does not serve as even a good indirect indicator of the outcome effects of Russian efforts. Broadly speaking, there is some evidence that the pro-Russian right-wing parties reached something of a plateau of influence by 2017, but there are worrisome hints of further growth, especially in places like Germany. That growth, however, appears to have little direct connection to Russian support or sympathy for Russia in key EU countries. We therefore have not used the status of right-wing parties as an outcome measure for Russian social manipulation efforts.

perceptions of whether Russia is a threat, and attitudes toward Vladimir Putin.
2. Broader public opinion in the target countries on a range of social and economic attitudes that Russia might be seeking to undermine: faith in institutions, confidence about the future, and others.
3. The geopolitical orientation of these countries as measured by their general official statements, national security strategies and related documents, and specific policies that indicate a relative tilt toward Russia or the West.
4. Specific outcomes in elections or referendums.

If these outcome measures are all moving in directions Moscow would favor, then it would appear it is having some of the effect it desires. That finding would still not associate specific social manipulation efforts to those outcomes, but it would at least begin to give some clue as to the effects Russia might be having. If, on the other hand, important indicators are moving *against* Moscow's interests, that would potentially tell us important things about the limits of its manipulation campaigns.

Of course, each of these outcomes is influenced by many factors; flows of information—and the further subset of foreign information—are only one variable. For example, the political prospects of right-wing parties are the product of a wide range of economic and social factors in given countries. Russian social manipulation efforts could be having some effect that is camouflaged by larger trends—counteracted, for example, by opposing factors, or rendered largely irrelevant by rapid momentum in the direction Moscow desires. This chapter does not, therefore, offer direct evidence of the specific effects of manipulation programs, but rather a larger and more indirect sense of whether they appear to be having the effects Russia intends.

We also attempted to establish some degree of focus through correlations in key time periods. In terms of timing, our research suggests that, despite long-term efforts at what were once called "active measures," the more elaborate and focused social manipulation campaigns have taken place since 2013. We have therefore reviewed data

and events in the period 2014–2017, to determine whether any correlation emerges in the period when social manipulation activities were being significantly ramped up. The sections below include our findings for the United States, United Kingdom, France, Germany, the Baltic States, and Poland.

In seeking influence in each of these countries, Russia is using a combination of efforts that include those that fall under our concept of hostile social manipulation, but also broader, more traditional forms of clandestine and intelligence operations and direct political engagement. Measuring outcomes will tend to conflate these distinctions, by examining the most general measures of outcomes Russia is seeking. Nonetheless, the resulting picture will give a sense of whether its hostile social manipulation efforts, working alongside other tactics, are achieving the results Moscow desires. And where possible, we offer evidence below on the effects of specific techniques of social manipulation, such as the use of social media campaigns.

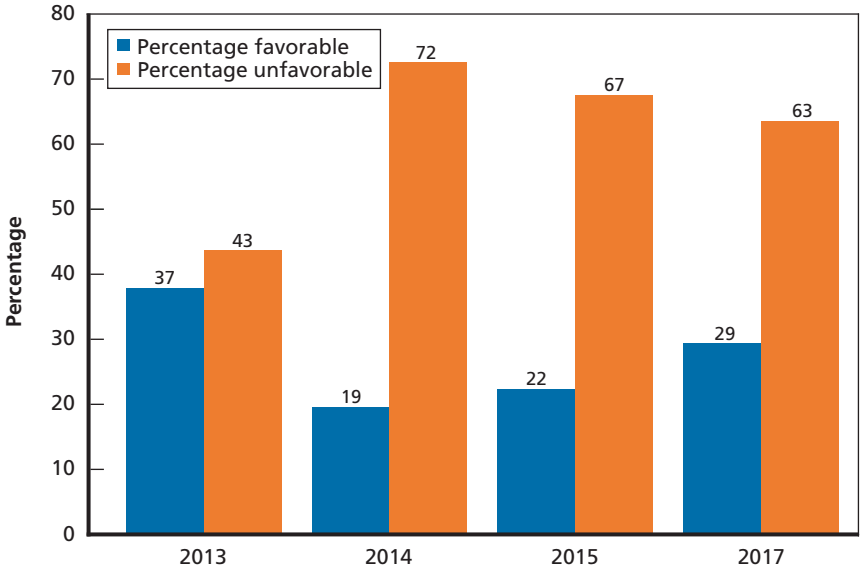
United States

Multiple public reports suggest that the United States has, especially since about 2015, been one of Russia's leading targets for hostile social manipulation. We evaluated evidence for possible effects of these programs. The United States and other Western societies have been beset by several long-term political, social, and economic ills—including economic insecurity and inequality, gridlocked governance, and rising partisanship. Polling evidence shows strong signs of these trends across many issues. The major question is whether we see significant additional movement since 2014.

Public Attitudes Toward Russia

As indicated in Figure 5.1, the percentage of the American public that views Russia favorably increased by 10 percentage points between 2014 and 2017, from 19 percent to 29 percent. Russia is more favored among younger Americans aged 18 to 29. Forty-seven percent of the American public believed in 2017 that Russia's power and influence is a major

Figure 5.1
Favorable Ratings for Russia Among American Public, 2013–2017



threat (compared with a slightly lower European average of 41 percent). Somewhat amazingly, the numbers of Americans who believe that Russia "respects the personal freedoms of its people" and who have confidence in Vladimir Putin to do the right thing *increased* by a few percentage points between 2014 and 2017.[5]

These numbers are somewhat less surprising on closer examination. For one thing, a healthy majority of Americans—70 to 80 percent—continues to view Russia unfavorably, expresses little or no confidence in Putin's decisions, and agrees that Russia does not respect its peoples' freedoms. If the rise in favorability ratings tops out under 30 percent and goes no higher, it will not reflect anything close to a majority.

---

[5] Unfortunately, Pew began asking this question in only 2017. Jacob Poushter and Dorothy Manevich, "Globally, People Point to ISIS and Climate Change as Leading Security Threats," Pew Research Center, August 1, 2017. These graphs include results from similarly phrased questions in consistent polls, which, in some cases, are not comprehensive across all years but which give a clear sense of trends over time.

Nor do these figures reflect anything like the favorability ratings of the pre-2014 period. As recently as 2011, Gallup polling found 51 percent of Americans indicating a favorable attitude toward Russia, and only 42 percent unfavorable. In 2002 the numbers were 66 percent favorable, 27 percent not. The 2017 figures are 28 percent favorable and 70 percent negative. In 15 years, therefore, American attitudes toward Russia have undergone an 80-point negative swing—from a 40-point overall favorability balance to a 40-point negative balance. According to Gallup, the number of Americans who believe that Russian military power poses a "critical" or "important" threat was 86 percent in 2016, as opposed to 81 percent in 2014 and 68 percent in 2004.[6]

It turns out that the small favorable shift was largely limited to one side of the political spectrum, largely as a result of a key intervening variable—the stance of the U.S. President. President Trump praised Vladimir Putin during this period and called for improved relations, suggested that Russia was being helpful on prominent issues, and expressed dismay that the relationship had become so negative. Partly because of this signaling, sharp partisan divisions emerged in Americans' perceptions of Russia: Democrats are now much more likely to view Russia unfavorably and as a major threat. In 2015, a similar percentage of Democrats and Republicans held negative views of Russia (71 percent and 73 percent, respectively). From 2015 to 2017, Republican views on Russia became significantly more positive. In 2017, 41 percent of Republicans viewed Russia favorably, compared with only 16 percent of Democrats. A July 2017 NPR/PBS poll found that 73 percent of Democrats thought Russian political interference was a major threat, while only 17 percent of Republicans did. About four out of ten Democrats named Russia as the country that represents the *greatest* danger to the United States in a 2017 poll—the highest percentage expressing this view in nearly three decades.[7]

---

6 Gallup, "Russia," survey results, undated.

7 Rob Suls, "Share of Democrats Calling Russia 'Greatest Danger' to U.S. Is at Its Highest Since End of Cold War," Pew Research Center, April 20, 2017. On differences in estimates of Russia's effect on the election, see Jennifer De Pinto, Fred Backus, Kabir Khanna, and Anthony Salvanto, "Republicans Blame Bill, Not Trump, for Health Care," CBS News, March 29, 2017.

Finally, under the influence of the extensive reporting of Russian election interference and other confrontational steps, U.S. public opinion on Russia fell back in 2018 compared to its slight recovery in 2017. In a 2018 Gallup poll, 72 percent of Americans expressed an unfavorable attitude toward Russia—compared with just over 50 percent in 2014 and compared with just 25 percent expressing a positive opinion.[8] The one-year shift was not dramatic, but between 2017 and 2018, there was a generally 2–percentage point negative swing in attitudes. A Pew poll from March 2018 showed that 68 percent of Americans held an unfavorable opinion of Putin, with only 16 percent holding a favorable opinion.[9]

If measured against 2002 or even 2010–2011, therefore, U.S. favorability toward Russia has experienced a catastrophic decline. The modest recovery since 2014 is almost entirely a partisan phenomenon, and that is largely driven by the attitudes and statements of the President. Absent this intervening variable, it is difficult to assess where U.S. attitudes would be, but, given the dramatic differences in party attitudes, it is almost certain that President Trump's position on the issue has had a far larger effect than Russian disinformation campaigns. As of 2018, positive attitudes toward Russia began to decline again. To the extent that Moscow sought to build a base of favorable policies in American public opinion, then, Russian manipulation efforts have not been effective as measured by this indicator.

Public Attitudes: Social and Economic Issues

Yet Russia may not intend to achieve that goal at all—it may be content with sowing chaos and undermining social cohesion, regardless of the effect on American attitudes toward Russia. Multiple reports suggest that Russia is conducting a broader assault on national unity, with the objective of weakening institutions, decreasing confidence in insti-

---

8 Gallup, undated.

9 Kristen Bialik, "Putin Remains Overwhelmingly Unfavorable in the United States," Pew Research Center, March 26, 2018.

tutions, and increasing societal divisions.[10] The new *National Security Strategy* states that Russia is attempting to "undermine the legitimacy of democracies."[11] While it is difficult to assess the degree to which a democracy has been undermined, there are some available metrics to assess shifts in confidence in institutions and divisions in society that can provide some sense of whether Russian efforts appear to be driving the needle in directions it would desire.

While very low, public confidence in Congress has remained stable in recent years; only 7 to 12 percent of Americans have had "a great deal" or "quite a lot" of confidence in Congress since 2013. However, the percentage of Americans who have "a great deal," "quite a lot," or "some" confidence in Congress *increased* from 44 percent in 2016 to 51 percent in 2017 (before sliding backward by a percentage point or two in various measures in 2018).[12] The proportion of Americans saying they had "quite a lot" or a "great deal" of confidence in the Supreme Court grew from 36 percent to 40 percent between 2010 and 2017; over the same period, the same two highest categories of confidence grew 2 percent apiece for big business, public schools, television news, and newspapers. It grew 9 percent for banks. In sum, general levels of confidence in major institutions have generally not been falling over the past three to five years: Gallup concluded in June 2017 that the average confidence across 14 major institutions was up 3 percent from the prior year.[13] Trust in media followed a similar pattern—sinking to an unprecedented low by 2016 based on long-term factors and recover-

---

10 Robert D. Blackwill and Philip H. Gordon, "Containing Russia, Again," *Foreign Affairs*, January 18, 2018.

11 *National Security Strategy of the United States of America*, Washington, D.C.: The White House, December 2017, p. 14.

12 Gallup, "Confidence in Institutions," survey results, 2017.

13 Frank Newport, "Americans' Confidence in Institutions Edges Up," press release, Gallup, June 26, 2017.

ing slightly in 2017.[14] This, too, is a partisan phenomenon: Democrats' confidence in the media actually grew significantly in this period.[15]

Those figures appear to have very slightly worsened in 2018, but, given the degree of partisan rancor and stagnating policymaking on many issues, it is in some ways surprising that the numbers did not fall further. Indeed, most of the variation can be correlated with other changes—recovery from the 2008 financial crisis in the case of banks, for example, and reaction to the election of Donald Trump among many Americans in terms of the presidency.

At the same time, partisan mistrust in the United States has reached unprecedented levels. According to Pew data, by 2016 58 percent of Republicans held "very unfavorable" views about Democrats, and 55 percent of Democrats held similar views about the GOP. But these numbers have been on a steady rise since the 1990s, fueled by growing partisan attacks, partisan news networks, and other phenomena. The proportion of Republicans holding such very negative views about Democrats, for example, was 21 percent in 1994 and has been rising steadily since that time.[16]

In sum, the decline of U.S. attitudes on these measures was well underway by 2014, and polls do not show a unique decline in key attitudes since then—and even in some cases display uneven recovery. In areas where negative attitudes remain very high, they are obviously linked to the current political situation in the country, which creates multiple intervening variables that make it impossible to distinguish a unique effect from Russian activities. If Russia is attempting to sow discord in the United States, therefore, we have no direct evidence that its efforts are producing the outcomes it desires. Its social media posts, disinformation, and other activities may be exacerbating existing trends on the margins.

---

[14] Art Swift, "Americans' Trust in Mass Media Sinks to New Low," press release, Gallup, September 14, 2016.

[15] Art Swift, "Democrats' Confidence in Mass Media Rises Sharply from 2016," press release, Gallup, September 21, 2017.

[16] Pew Research Center, "Partisanship and Political Animosity in 2016," June 22, 2016.

National Orientation

Between 2014 and 2017, U.S. national policies, especially in the security realm, demonstrated a significant tilt toward greater confrontation with Russia.

The United States continues to be a leader in NATO, deploying troops and holding joint drills and exercises intended to send a message of strength and cohesion to Russia. In 2015, the United States authorized the European Reassurance Initiative (later termed the European Deterrence Initiative) to provide funding to enhance deterrence and defense and improve the readiness of forces in Europe. The amount of American money dedicated to the security of Eastern Europe has tripled under President Trump, and the number of deployed troops has also increased.[17] The United States deployed 300 troops to Estonia and increased the amount of military equipment provided to the Estonian government in 2017.[18] The United States is leading a multinational battlegroup in Poland under NATO's Enhanced Forward Posture[19] and has troops throughout Central and Eastern Europe as part of Operation Atlantic Resolve.[20] Partly in support of such activities, U.S. defense spending broke a recent trend and began to increase in the fiscal year 2018 budget proposal.

U.S. policies toward Russia have become consistently more hostile since 2014. That year, the United States imposed sanctions on Russia due to Russia's annexation of Crimea and incursion in Ukraine. Two successive U.S. National Security Strategies have condemned Russian aggression and pointed to Russia as a major national security threat; the 2017 version argued that Russia "challenge[s] American power,

---

17 Tomáš Valášek, "Trump's Relationship with NATO, One Year into His Presidency," Carnegie Europe, December 28, 2017.

18 Natasha Turak, "Estonia Has No Doubts on Trump's Commitment to NATO, Says Prime Minister Juri Ratas," CNBC, January 26, 2018.

19 "NATO's Enhanced Forward Presence Factsheet," NATO Public Diplomacy Division, May 2017.

20 Atlantic Resolve is funded and enabled by the European Reassurance Initiative (*America's Continued Commitment to European Security: Operation Atlantic Resolve*, U.S. Department of Defense Special Reports, undated).

influence, and interests, attempting to erode American security and prosperity."[21] In 2016, Washington expelled Russian diplomatic personnel and imposed additional sanctions on Russia in response to Russia's meddling in the U.S. presidential election; the following year, it approved a plan to begin providing military defensive weaponry to Ukraine, such as antitank missiles, an issue that had previously been under debate. In 2017 the U.S. Congress passed the Countering America's Adversaries Through Sanctions Act (CAATSA), which increases sanctions against Russia and imposes penalties on entities conducting "significant" business with Russian defense and intelligence sectors.[22]

In terms of public attitudes, about six out of ten Americans hold a favorable view of NATO, an improvement of 9 percentage points from 2016. This is the highest level of public support for the security alliance in recent years.[23]

Election Outcomes: 2016

By far the most important possible effect of Russian social manipulation campaigns would have been to alter the outcome of the 2016 presidential election. U.S. intelligence agencies have publicly indicated that they have "high confidence" that Russia intended just such a result. The unclassified Director of National Intelligence (DNI) summary indicated that Russian President Vladimir Putin "ordered" an influence campaign that blended "covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third party intermediaries, and paid social media users or 'trolls.'"[24] A major component of the campaign was allegedly the hacking of Democratic Party emails and their release through such sites as WikiLeaks and Guccifer 2.0. In terms of the timing, the DNI

---

21 *National Security Strategy of the United States of America*, 2017.

22 John Wagner and Karoun Demirjian, "Trump Blames Congress for 'All-Time' Low Relationship with Russia; Lawmakers Push Back," *Washington Post*, August 3, 2017.

23 Bruce Stokes, *NATO's Image Improves on Both Sides of Atlantic*, Pew Research Center, May 23, 2017.

24 U.S. DNI, "Assessing Russian Activities and Intentions in Recent U.S. Elections," unclassified assessment, January 6, 2017, p. ii.

report refers to evidence that the Russian campaign was underway by March 2016.

As noted, we did not, from the beginning, attempt to reach a determination on the question of whether Russian activities determined, or strongly influenced, the actual outcome of the election. The mere fact that a foreign power undertook such a campaign should be of intense concern to all Americans, whether it was the decisive factor, or even a strongly contributing variable, to the outcome. No matter the effectiveness of Russia's efforts, the United States must work to ensure that such manipulation cannot happen in the same way again, regardless of the outcome.

We did, however, survey available public evidence on the elements of the Russian manipulation efforts directed at the United States during the period before the election. The purpose was to understand the tools employed and build some initial sense of the apparent outcomes. This evidence is significant, but it does not allow us to make a clear determination of just how decisive these activities were.

Multiple public reports indicate that Russia undertook a range of not-always-well-coordinated lines of effort to shape the outcome of the election. These included extensive social media efforts—spreading information, trolling and commenting, and directly purchasing advertisements; releasing direct propaganda through RT and other outlets; generating fabricated information to discredit some candidates and promote others; and hacking personal and institutional databases to release potentially compromising information, specifically Clinton campaign and Democratic National Committee emails partly revealed through Wikileaks. One estimate suggests that 11.4 million people saw Russian ads before and after the election.[25]

A critical distinction in this one case is between the theft and release of controversial documents and the broader campaign of social media influence and disinformation. The theft of Democratic Party

[25] Grassegger and Krogerus, 2017. This analysis was completed before the release of the Mueller Report, which offered even more detailed evidence to confirm Russia's efforts to influence the 2016 elections. That report clarifies the extent of Russian efforts, but it does not provide new evidence on their actual effects.

documents and their release through Wikileaks clearly had the effect of distracting the leadership of the Clinton campaign in the final days of the election.[26] Campaign officials were scrambling to respond to the controversies generated by leaked emails when they could have been taking actions to affect the election results. A more quantifiable effect of the release can be found in shifting poll numbers after the document release, which has caused some observers to conclude that this action alone may have had a significant effect on the election's outcome.[27]

Our analysis neither validates nor refutes that hypothesis. Such numbers and implications are more than reason enough, however, for the United States to engage in determined efforts to ensure that Russia or other outside actors cannot manipulate U.S. electoral outcomes. As we will argue in the section of this report on future scenarios, moreover, hostile social manipulators are only scratching the surface today of what might be possible in a decade, and the reasons for concern are many. At the same time, it is important to understand that the more directly influence-seeking components of social manipulation campaigns are not magic wands—they have significant limitations, at least as of today, that constrain the actual effect on attitudes and behavior.

One limitation is the role of other variables in influencing election outcomes. Economic insecurity in the United States, for example, turned out to have been more profound than many understood before the election, creating a much more viable basis for an insurgent candidate than some polling showed going into 2016.[28] Social manipulation efforts can take advantage of such conditions, but they cannot create them. As one analysis of Russia's activities concludes, they have "succeeded in stirring confusion only because there were so many weaknesses for them to exploit in the first place."[29]

---

[26] Ben Nimmo, "Election Watch: Beyond Russian Impact," Atlantic Council Digital Forensic Research Lab, February 27, 2018.

[27] This case is made by Kathleen Hall Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President*, New York: Oxford University Press, 2018.

[28] Nate Silver, "It Wasn't Clinton's Election to Lose," 538.com, January 23, 2017.

[29] Henry Farrell, "American Democracy Is an Easy Target," *Foreign Policy*, January 17, 2018.

A second qualifying factor regarding the effect of Russian social media–based influence operations on the election is the limited role of actual disinformation. A study by Matthew Gentzkow found that only about 15 percent of the American public reported seeing a set of representative fake news stories offered by pollsters, and about 8 percent admitted that they believed them. That compares with 70 percent who saw the true stories listed in the poll, and 60 percent who believed those stories.[30] Other polls suggest that most Americans are concerned about the effects of fake news, suggesting that at least a certain proportion of people are likely to be on the lookout for it.[31]

Even if a bot or fake account generates thousands of messages, moreover, it may be only one of a hundred or more sites consulted by a given voter, saying much the same thing as the rest. Put simply, many American voters faced an avalanche of partisan and sometimes inaccurate information on social media and the internet, only a fraction of which originated in Russia. It is impossible to determine the unique effect of that component. It is not even clear how much of the material can be traced to Russia: One researcher who attempted to identify accounts or posts that could be attributed to Russia points out that there were significant numbers of Russian posts, but that there was also "a lot of organic support for Trump," which led to reposting and retweeting of messages. "Trying to disaggregate the two was difficult, to put it mildly."[32] In some cases, accounts assumed to be Russian trolls turned out to be authentic Americans simply posting similar material.

A major study of the traditional media's role in the election provides important perspective on the possible role of outside actors—and the difficulty of separating out their unique influence. A Harvard study of the information environment headed into the election found that media in general, but especially on the right, were polarized, and

---

30 Based on voting rates and other baseline assumptions, researchers compiled a rough estimate suggesting that these stories might have affected voting shares by tiny amounts—something like 0.001–0.005 percent (Allcott and Gentzkow, 2017).

31 See Pew Research Center, "Many Americans Believe Fake News Is Sowing Confusion," December 15, 2016b.

32 Shane, 2017a.

that certain alt-right websites, such as Brietbart, exercised a disproportionate influence over conservative online discussion of issues.[33] In other words, the online media landscape was preset to achieve just the results that are presumed from Russian disinformation: Create a highly partisan approach to issues, focus on criticism of Hillary Clinton, and spread prominent examples of disinformation. Those outcomes were overdetermined by the political and media landscape of the electoral context. The degree to which Russian intervention had measurable effects on the outcomes cannot be known relative to other variables.

Subsequent analyses by social media firms found that the amount of Russian-generated or Russian-recirculated information, while impressive when viewed in isolation, was modest relative to the overall infosphere before the election. Even the pure information distribution numbers themselves, when placed into context, do not necessarily suggest a dramatic role for disinformation about the 2016 election. Statistics from the internal analyses of Facebook, Twitter, and Google must be used with care: It is unclear what methodology was used to generate these numbers, and they are only as good as the companies' efforts to identify specifically Russian sources, which are at best imperfect at the moment. Nonetheless, the available statistics do place these activities into context:[34]

- Of the political advertising conducted through Facebook, over half was viewed after the election. A quarter of the messages were never viewed at all.
- The 80,000 posts from the 120 Russian Facebook accounts represented four one-thousandths of a percent (0.004 percent) of total News Feed content distributed by Facebook during that period.

---

[33] Robert Faris, Hal Roberts, Bruce Etling, Nikki Bourassa, Ethan Zuckerman, and Yochai Benkler, "Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election," research paper, Berkman Klein Center for Internet and Society, Harvard University, August 2017, p. 5.

[34] These data are derived from the testimony of Facebook, Twitter, and Google executives before the Senate Committee on the Judiciary, October 31, 2017 (U.S. Senate Committee on the Judiciary, "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions," subcommittee hearing video, Washington, D.C., October 31, 2017).

- The 36,000 automated Twitter accounts later identified as controlled by Russia represented one one-hundredth of a percent (0.012 percent) of total accounts at the time. The 1.4 million tweets they sent in the six-week preelection period starting September 1, 2016, represented less than three-quarters of one percent (0.74 percent) of even the specifically *election-related* tweets sent at the time, and they reflected only a third of a percent (0.33 percent) of impressions of election-related content—which means these tweets were viewed less often than average election-related content. In other words: Of all original tweets in that six-week period, only 1 percent were about the election; and *of those*, only three-quarters of 1 percent were traced to Russian-influenced automated accounts.
- While 68 percent of Americans report using Facebook, only 24 percent use Twitter, suggesting that the reach and effect on the overall population will be somewhat limited.[35]
- Those same Twitter accounts were also retweeting messages sent by authentic Twitter accounts, but the numbers were similarly low. Russian-controlled accounts appear to have been responsible for only 0.4 percent to 0.6 percent of retweets of messages from accounts such as @HillaryClinton or @realDonaldTrump.

Part of the issue, obviously, is that the overall social media ecosystem is simply vast: 328 million Twitter users, 2 billion Facebook members, 3.5 billion Google searches per day. Between 2015 and 2017, Facebook sent over 33 *trillion* stories to peoples' News Feeds; each person gets an average of 220 stories per *day*. In just the six-week period from September 1, 2016, to November 15, 2016, there were 16 billion tweets, 189 million of which were identified as being election-related. The fact that Russian bots and human operators generated tens of thousands of Facebook posts and tweets sounds impres-

[35] Aaron Smith and Monica Anderson, "Social Media Use in 2018," Pew Research Center, March 1, 2018.

sive—until one realizes that between 2015 and 2017, Americans were exposed to 33 *trillion* Facebook posts alone.[36]

A more relevant statistic may be the proportion of Russian-generated messages received by smaller target audiences. Russian bot–produced tweets or Facebook posts may have been a fraction of the overall political messages in that period—but were they a much larger proportion of the tweets and posts viewed by specific potential voters of a particular political persuasion in specific states? As of this writing, we simply do not know. There is reason—from both the general proportions of Russia-related content and the studies of partisan content cited above—to doubt that Russian sources would have been dramatically more influential even with such target audiences. Some studies, as noted above, also show that some of the most significant voting swings in 2016 took place among populations with the least social media exposure. Nonetheless, more research is clearly required on the specific reach and effect of targeted messaging.

In sum, the available evidence surveyed for this analysis does not support a definitive judgment of the degree of effect achieved by Russian social manipulation efforts before the 2016 U.S. election. It does, however, demonstrate a serious potential threat to the integrity of current and future elections if such activities continue and become more sophisticated. The available evidence also suggests that Russia appears to have achieved more-direct effects through the theft and release of documents—a form of political warfare sometimes known as "doxfare"—than with social media messages that aimed to shift attitudes or behavior.

United Kingdom

Outside the United States—and indeed for a longer period and with a wider range of social manipulation programs—Russia has been targeting social stability and democratic processes throughout Eastern and

---

[36] Patrick Ruffini, "Why Russia's Facebook Ad Campaign Wasn't a Success," *Washington Post*, November 5, 2017, p. B1.

Western Europe.[37] An important target has been the United Kingdom, both in general terms and specifically focused on two recent referendums—the one on Brexit and one on Scottish independence.

Generally speaking, the basic pattern in many European countries is the same, a pattern reflected in evidence from the British case. In all cases, as in the United States, there was some limited recovery between 2014 and 2017 in public favorability attitudes toward Russia. This shift, however, is largely a partisan phenomenon even in Europe, with right-wing parties encouraging a more pro-Russian view among their followers. Favorability ratings remain far lower than they were as recently as 2010–2013. And they declined somewhat in 2018 under the influence of continuing Russian political meddling and clandestine operations in the West.

Meanwhile, the general geopolitical orientation of almost all European nations tilted away from Russia in this period, with NATO and EU states committing to a robust range of measures designed to counter Russian power and influence. Russian efforts at direct intervention in elections or referenda appear to have had some marginal effect but cannot be said to have directly caused any outcomes. The primary risk, the evidence suggests, is not Russian manipulation as much as the social, economic, and political instability that Russia seeks to leverage.

Public Opinion on Russia

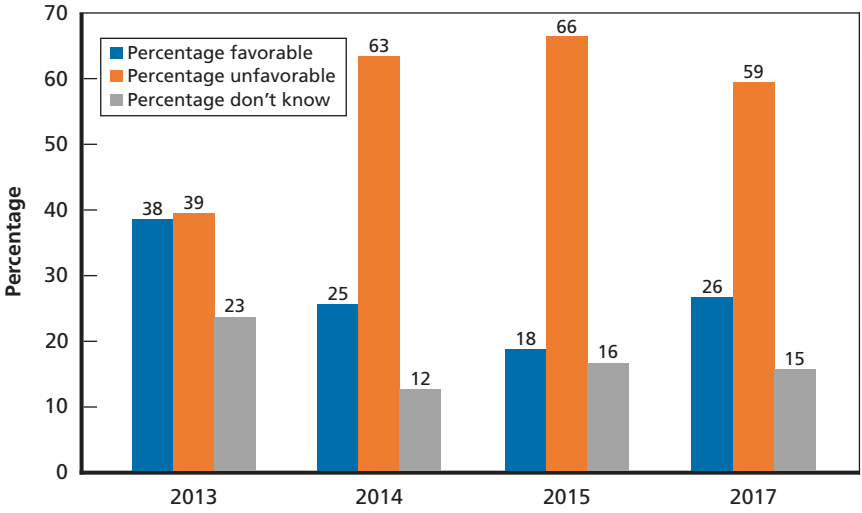
While there has been an increase in the percentage of the British public that views Russia favorably since 2015 (as noted in Figure 5.2), this percentage is still well below 2013 levels. The percentage of the British public that views Russia favorably has increased by 8 percentage points since 2015, although it is still considerably lower than it was in 2013. Forty-three percent of the British public believes Russia's power and influence is a major threat.[38] Almost half of the British public views

---

[37] Arguably the most extensive U.S. government statement of the issue is U.S. Senate, Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, Minority Staff Report, January 10, 2018.

[38] Unfortunately, Pew began asking this question in only 2017. Margaret Vice, "Publics Worldwide Unfavorable Toward Putin, Russia," Pew Research Center, August 16, 2017.

Figure 5.2
Favorability Ratings of Russia Among British Public, 2013–2017



Russia as a serious threat. Unlike France and Germany, the British are slightly more confident that Trump would do the right thing in world affairs (22 percent) than they are that Putin would (19 percent). As in the United States, then, there has been some variation since 2014 but not a dramatic recovery from the precipitous drop in favorable attitudes toward Russia beginning in 2014. And as in the United States, in the wake of renewed Russian provocations—and particularly, in the British case, of the alleged poisoning of former Russian citizens in the United Kingdom—these attitudes worsened in 2018, with over 60 percent of Britons saying Russia was a threat to world peace. And again, these are all far lower than attitudes as recently as 2011, when 50 percent of Britons held a favorable view of Russia.[39]

In the meantime, public support for NATO has remained strikingly stable over the past several years, with about 60 percent of the British public indicating a favorable attitude and only 20 percent saying they had an unfavorable view (with the remainder saying they

[39] Pew Research Center, "Global Indicators Database," database, undated.

"don't know"). About two-thirds of the British public is confident that the United States would come to the aid of a NATO member country if it were to become engaged in a military conflict with Russia.[40] However, less than half of the British public believes that the United Kingdom should use force to defend a NATO member country if it became engaged in a serious military conflict with Russia—and the trend is in a negative direction: In 2015, about half of Britons said yes and 35 percent no; by 2017, the percentages were almost equal at just over 40 percent in each category.

Elections and Referendums

In June 2016, the British public voted to leave the European Union by a small margin (the vote had a turnout of 72 percent; 51.9 percent of referendum participants voted to leave the European Union).[41] Despite many public reports suggesting direct Russian interference in the referendum, there is so far little direct proof of any effect from the relatively modest actions Russia is confirmed to have taken.

Most fundamentally, the origins of the Brexit vote lay in decades of rising skepticism within the United Kingdom toward the European Union. Brexit was one example of a rising populist tide throughout the West, one with roots in the socioeconomic challenges mentioned earlier. The National Centre for Social Research report on the vote concludes that the referendum outcome reflected the growing concerns of "more 'authoritarian', socially conservative voters about the social consequences of EU membership," singling out immigration as an especially contentious issue.[42] This trend of thinking has apparently continued after the vote: According to polling data collected by the *British Social Attitudes* survey, post-Brexit Britain is "far more sceptical about the EU than it had ever been previously."[43] The "Leave" campaigns

---

[40] Stokes, 2017.

[41] "EU Referendum Results," BBC News, 2016.

[42] "The Vote to Leave the EU," *British Social Attitudes*, Vol. 34, National Centre for Social Research, undated, p. 2.

[43] "The Vote to Leave the EU," undated, p. 16.

pushed public opinion in a more Euroskeptic direction and aggravated preexisting social anxieties about EU membership.[44]

Research by the Computational Propaganda Project at the OII found that political bots (highly automated social media accounts) played a "small but strategic" role in spreading misinformation during the discourse on "StrongerIn-Brexit."[45] In the weeks leading up to the referendum, the two single most active accounts from each side of the debate were bots. Both bots, @ivoteLeave and @ivotestay, followed similar processes: They only retweeted messages that supported their side and did not create new content.[46] In general, the social media bots were used more for repeating messages than for engaging in discussions. Less than 1 percent of the accounts in the sample generated almost *one-third* of all the traffic in the sample, signaling a high level of automation in the online discourse on the referendum.[47] Throughout the period covered by the study (June 5–12, 2016), the pro-Leave bots were much more active, tweeting more than three times as often as the pro-Remain bots.[48]

Other sources have found evidence of Russian-inspired or -controlled social media accounts broadcasting sensationalistic messages in the weeks before Brexit. Not all of these appear to have been anti-Brexit, but they were apparently designed, in part, to exacerbate tensions and intensify the hostility of the debate.[49]

Several factors point to a possible influence of social manipulation in the Brexit vote. For one thing, the result was very close, and a close vote offers an opportunity to shift enough voters to influence the outcome of the election. Polling conducted in the weeks leading up to the referendum was indicating that neither side had a substantial

---

44 "The Vote to Leave the EU," undated, p. 17.

45 Howard and Kollanyi, 2016.

46 Howard and Kollanyi, 2016, p. 2.

47 Howard and Kollanyi, 2016, p. 4.

48 See Table 2, p. 4, of Howard and Kollanyi, 2016. Bots tweeted about 28,000 pro-Remain tweets, compared with about 97,000 tweets from pro-Leave bots.

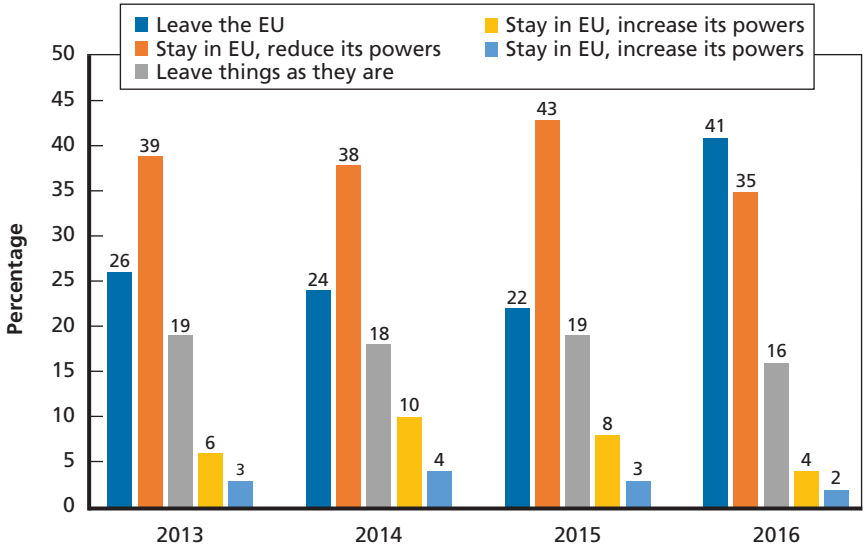
49 Matt Burgess, "Here's the First Evidence Russia Used Twitter to Influence Brexit," *Wired*, November 10, 2017.

advantage over the other, and that there was a significant segment of the electorate that was undecided and could potentially be influenced. A poll conducted in early June showed Remain at 44 percent, Leave at 42 percent, and those who did not know how they would vote at 13 percent.[50]

Second, while some research suggests that "relatively few" British felt strongly committed to a European identity to begin with,[51] Figure 5.3 shows a significant increase in the percentage of the public wishing to leave the European Union between 2015 and 2016. This appears to indicate some late changes in attitude, when a social manipulation campaign might have been underway.

Third, a considerable proportion of voters were "fence-sitters," not strongly committed to a side until days before, or even the day of, the

Figure 5.3
British Attitude Toward Relationship with European Union



[50] Toby Helm, "Third of EU Referendum Voters Won't Make Up Their Minds Until Week Before Poll," *The Guardian*, June 11, 2016.

[51] "The Vote to Leave the EU," undated, p. 20.

vote. A report from the London School of Economics estimates that up to 30 percent of people would either (1) not decide how to vote in the referendum until the last week, or (2) change their minds in the last week. A full 15 percent would not make up their minds at all until the day of the vote.[52] This uncertainty provided an opportunity for well-timed advertisements, propaganda, and misinformation to sway a voter's position. Because disinformation campaigns tend to peak between one and two days before elections,[53] they can have an especially strong impact when a significant portion of the electorate will not make up their mind until the day of the election.

Fourth, the vote was a referendum, not a general election. Interestingly, the proportions of late deciders and side-switchers tend to be higher in referendums than in general elections.[54] Referendums typically tend to be more unpredictable than general elections, partly because the process is not as simple as voting for the candidate(s) of one's party, even if the referendum issue is situated along partisan lines. This raises an interesting question of whether the nature of a referendum itself makes it more susceptible to social manipulation.

Fifth, social media use increased significantly in the United Kingdom over the past few years. In 2011, about 45 percent of the British population used social media.[55] In 2017, this percentage increased to 64–66 percent.[56] Given that social manipulation as we currently conceptualize it seems to be especially pernicious on social media, this 20-percent growth is significant. Social media provides an accessible way to assess the trends in one's social group, and people calculate that

---

[52] Michael Bruter and Sarah Harrison, *The Impact of Brexit on Consumer Behavior*, Lansons, London School of Economics, and Opinium, June 9, 2016. The report also says that arguments put forward by the Leave camp are met by voters with more skepticism than those advanced by those in Remain, even among those who say they back Brexit.

[53] Panagiotis T. Metaxas and Eni Mustafaraj, "Social Media and the Elections," *Science*, Vol. 338, No. 6106, October 2012.

[54] Bruter et al., 2016.

[55] Office for National Statistics, "Internet Access—Households and Individuals: 2017," August 3, 2017a, chapter 7.

[56] Office for National Statistics, "Social Media Usage in the United Kingdom," Statista Dossier, August 2017b, p. 7.

it is appropriate to believe something or behave in a certain way when they perceive that people comparable to them are believing or acting in that way.[57]

Against these suggestive factors, however, must be posed significant counterevidence about the potential role of Russian intervention in Brexit. First, there is no persuasive public evidence of what precisely Russia did to influence the vote. Several subsequent analyses have suggested a modest effort. Facebook's survey of activity on its platform found only 97 cents' worth of Brexit-related political advertising traceable to Russian sources.[58] Twitter also uncovered relatively few openly purchased Brexit-related advertisements.[59] Several different surveys of Russian-linked accounts found numbers in the dozens, sending out messages numbering in the hundreds to low thousands—a tiny proportion of the tens of millions of tweets sent about Brexit.[60] An extensive survey of Russian-originated Twitter and YouTube activity prior to the vote found that the sources "contributed relatively little to the overall Brexit conversation."[61] One of the authors of that study summarized their findings this way: "Overall, I think the Russian activity during Brexit seems to have been minimal. The real source of misinformation about the Brexit debate was homegrown."[62]

Second, there is also no reliable evidence of the actual effect on the outcome of the surge in bot-related posts in the days before the referendum. Given the massive public information campaign by both

---

57 Robert B. Cialdini, *Pre-Suasion: A Revolutionary Way to Influence and Persuade*, New York: Simon and Schuster, 2016, pp. 192–208.

58 David D. Kirkpatrick, "Facebook Sees Little Evidence of Russian Meddling in 'Brexit' Vote," *New York Times*, December 13, 2017.

59 Data cited in Alliance for Securing Democracy, *Securing Democracy Dispatch*, December 18, 2017.

60 Georgina Lee, "Here's What We Know about the Alleged Russian Involvement in Brexit," 4News, November 16, 2017.

61 Vidya Narayanan, Philip N. Howard, Bence Kollanyi, and Mona Elswah, "Russian Involvement and Junk News During Brexit," Oxford, UK: Oxford Program on Computational Propaganda, Oxford University, December 19, 2017.

62 Philip Howard, quoted in Kirkpatrick, 2017.

sides, it is not at all clear how even hundreds of thousands of additional social media posts could have had a measurable effect on attitudes or voting. The referendum passed by over a million votes, and there is no evidence of a Russian operation on a scale capable of generating such a shift in public attitudes.[63]

Third, the role of tweet-generating bots is unclear. Although pro-Leave bots produced many more tweets than pro-Remain bots, the percentage of each side's traffic generated by bots was similar. It also must be noted that Twitter is much less popular in the United Kingdom than Facebook, and only about 25 percent of the population uses it.[64] As of July 2017, Facebook held 74 percent of the "market share" in the United Kingdom, with Twitter holding only 12 percent of the British social media market.[65]

National Orientation

Under the governing Conservative Party (in power since 2010), Great Britain's basic national orientation has remained staunchly pro-NATO and pro-West, with repeated reaffirmations of the alliance with the United States and a growing hostility toward Russian aggression. Like the United States, Great Britain has become increasingly confrontational toward Russia since 2014.

In terms of defense spending, the British defense budget has remained steady since 2014, at between 2.19 and 2.14 percent of gross domestic product (GDP). In 2015, the British government committed to continuing to meet NATO's member defense spending target of

---

63 "Russian Twitter Trolls Meddled in the Brexit Vote. Did They Swing It?" *The Economist*, November 23, 2017. The Senate Foreign Relations Committee report, *Putin's Asymmetric Assault on Democracy* (U.S. Senate, Committee on Foreign Relations, 2018), discusses the UK case (pp. 116–119) but offers no meaningful evidence of a significant Russian campaign or any effect on voting.

64 Based on information from "Number of Twitter Users in the United Kingdom (UK) from 2012 to 2018 (in Million Users)," Statista, 2017; and Stuart Dredge, "More Than One-Fifth of Britons Will Use Twitter This Year, Claims Report," *The Guardian*, February 20, 2014.

65 "Market Share Held by the Leading Social Networks in the United Kingdom (UK) as of July 2017," Statista, 2017, p. 12.

2 percent of GDP by increasing its defense budget by 0.5 percent above inflation every year until 2021. The United Kingdom has the largest defense budget in the European Union, and the second largest defense budget in NATO.[66]

The United Kingdom remains one of the few NATO member countries that is meeting the 2 percent of GDP defense-spending threshold (though just barely). In March 2017, the United Kingdom began to move troops to Estonia as part of a major NATO mission in the Baltics and one of the biggest deployments to Eastern Europe in decades.[67] At a June 2017 meeting of NATO defense ministers, British Defense Secretary Sir Michael Fallon announced several new British contributions to NATO. The British Royal Navy will lead half of NATO's maritime forces for a year, increase offensive cybersupport for NATO operations, and increase advisory support to the Afghan government and security forces.[68]

Britain has traditionally been reticent when it comes to additional coordination and cooperation among EU member states' militaries, contending that it is a duplication of NATO.[69] Britain is not participating in the new EU Permanent Structured Cooperation (PESCO) defense pact, which is unsurprising given its impending departure from the European Union. However, at the 2018 United Kingdom–France Summit, the United Kingdom committed to several measures to strengthen security cooperation with France and Europe more broadly.[70] These measures include British provision of logistical support to the French mission in Mali; the establish-

---

66 "Defence Budget Increases for the First Time in Six Years," press release, United Kingdom Ministry of Defence, April 1, 2016.

67 "British Troops Land in Estonia for Nato Mission to Deter Russia," *The Guardian*, March 18, 2017.

68 "Defence Secretary Steps up UK Commitments to NATO," press release, United Kingdom Ministry of Defence, June 29, 2017.

69 Arthur Beesley, "EU Sets Timetable for Tighter Military Coordination," *Financial Times*, June 22, 2017.

70 "UK and France Commit to New Defence Cooperation," press release, United Kingdom Ministry of Defence, January 18, 2018.

ment of a UK–France Defence Ministerial Council; and a British commitment to work with European countries to develop the European Intervention Initiative proposed by French President Emmanuel Macron.[71] The two countries also stated the need for the British defense industry to continue to engage in European military research and development programs.

In sum, then, if Russian social manipulation efforts had any goal of reducing British support for Western alliances or institutions, they appear to be failing.

France

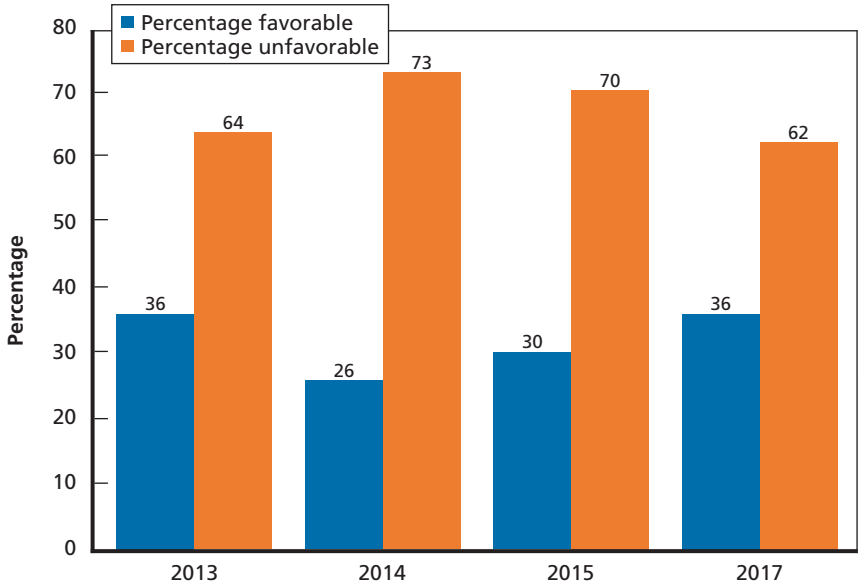
France reflects the same general set of trends visible throughout Europe. Opinion of Russia recovered somewhat between 2014 and 2017 but remained far below earlier heights. France remains strongly supportive of Western institutions and responses to Russian meddling. In the French case, the government took powerful efforts to mitigate and deter Russian interference in a recent presidential election, with apparently productive results. As a result of these general factors, while the percentage of the French public that views Russia favorably has significantly increased (by 10 percentage points) since 2014 (see Figure 5.4), almost half of the French public perceives Russia to be a major threat to France, and other indicators of attitudes toward Russia have remained stable. France is committed to increasing defense spending over the next five years and, along with Germany, led efforts to finalize a new EU defense agreement.

Public Opinion Toward Russia

The percentage of the French public that views Russia favorably has increased by 10 percentage points since 2014. French men are far more likely to view Russia favorably than French women; there is a 17–per-

[71] "Sorbonne Speech of Emmanuel Macron—Full Text/English Version," blog post, *Ouest France*, September 26, 2017.

Figure 5.4
Favorability Ratings of Russia Among French Republic, 2013–2017



centage point gender gap.[72] Forty-five percent of the French public believes Russia's power and influence is a major threat.[73]

The percentages of French confident that Putin would do the right thing in world affairs (18 percent) and that Trump would do the right thing (14 percent) are similar, if both very low.

National Elections

Evidence from the French election suggests that the #MacronLeaks disinformation campaign was ineffective because it did not reach the only high-value community (if the goal was influencing the election): French citizens of voting age. In the days before the runoff, online alt-right communities collaborated to manufacture and allegedly steal

[72] Vice, 2017.

[73] Unfortunately, Pew began asking this question in only 2017.

incriminating documents belonging to the Macron campaign.[74] In line with findings that disinformation campaigns tend to peak between one and two days before elections,[75] #MacronLeaks traffic surged on May 5–6. The traffic associated with #MacronLeaks during this peak was "nearly comparable in scale" to the volume of *all* election-related discussion on May 5–6, meaning that for a period of time (about 48 hours), the #MacronLeaks disinformation campaign acquired "significant collective attention, which in turn could have potentially had disastrous effects in terms of public opinion manipulation."[76] Additionally, because the peak occurred so close to the actual time of voting, there was not sufficient time for corrections and countermessaging.

However, though #MacronLeaks received a lot of attention, it turned out to be a relatively ineffective method of influencing French public opinion or voting behavior: The users who engaged with the campaign were mostly foreigners belonging to the alt-right Twitter community, not French users who could actually have an impact on the French election.[77] The #MacronLeaks case is instructive for the wider debate on social media manipulation: One should not assume that widespread online attention for a certain claim or piece of misinformation will translate into manipulation of the actual target community.

The first round of the 2017 French presidential election was held on April 23, 2017. As no candidate won a majority in the first round, a runoff was held between the top two candidates, Emmanuel Macron of En Marche! and Marine Le Pen of the National Front (FN), on May 7. Macron won the second round by a decisive margin. This was the first time in the history of the Fifth Republic of France that the runoff did not include a nominee of the traditional left or right parties.[78] This was also likely the first time in French history that fears

---

74 "Macron Leaks: The Anatomy of a Hack," BBC News, May 9, 2017.

75 Metaxas and Mustafaraj, 2012.

76 Metaxas and Mustafaraj, 2012.

77 Emilio Ferrara, "Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election," *First Monday*, Vol. 22, No. 8, August 2017.

78 "Macron et Le Pen au Second Tour D'une Présidentielle hors Norme," *Sud-Ouest*, April 23, 2017.

of voter manipulation by external actors conducting disinformation campaigns via social media channels were so pronounced. The extent of misinformation proliferation in parts of the United States in the run-up to the 2016 presidential election[79] and fears that political bots had influenced referendum voters in the United Kingdom concerned many in France and beyond. However, the consensus is that the French resisted attempts at social manipulation and deception better than their European and American counterparts. This section will examine available research into social manipulation efforts in the French election, which include the use of political bots and alt-right online "armies" to spread disinformation and influence public opinion.

One study conducted by the OII focuses on the use of bots and the prevalence of distinct types of political content shared on Twitter before both rounds of the presidential election. The study used a dataset containing about 842,000 tweets collected between March 13 and 19, 2017 (over a month before round one), and a dataset of about 960,000 tweets collected between April 27 and 29, 2017, four days after the first round and about two weeks before the second.[80] Both datasets selected tweets that used a variety of hashtags associated with the presidential candidates and the election.

Overall, the researchers found that evidence of social manipulation efforts significantly increased between their first and second rounds of data collection. In the first sample, highly automated accounts generated a relatively small amount (7.2 percent) of the content being shared about French politics (see Table 5.1). This percentage of bot-driven Twitter traffic more than doubled in the sample taken a few weeks before the runoff election, as shown in Table 5.1. However, bot-driven traffic still constituted much less of the discourse

---

79 Philip N. Howard, Gillian Bolsover, Bence Kollanyi, Samantha Bradshaw, Lisa-Maria Neudert, "Junk News and Bots During the U.S. Election: What Were Michigan Voters Sharing over Twitter?" Data Memo 2017.1, Oxford, UK: Project on Computational Propaganda, Oxford Internet Institute, University of Oxford, March 26, 2017.

80 Clementine Desigaud, Philip N. Howard, Samantha Bradshaw, Bence Kollanyi, and Gillian Bolsolver, "Junk News and Bots During the French Presidential Election: What Are French Voters Sharing over Twitter in Round Two?" Data Memo 2017.4, Oxford, UK: Project on Computational Propaganda, Oxford Internet Institute, University of Oxford, May 4, 2017.

Table 5.1
Comparing Metrics of Social Manipulation Efforts and Effects in Rounds One and Two of French Election

	Round One	Round Two
Percentage of election-related Twitter traffic driven by bots	7.2%	16%
Number of bots driving traffic about each candidate	100	500
Ratio of links to professional news to links to nonprofessional news	2:1	1:1
Percentage of election-related traffic classified as "junk news"	4%	6%

on French politics leading up to either round of the election than it did in the lead-up to the UK referendum (where bots generated a full third of referendum-related traffic). Before round one, there were about 100 bots driving traffic about Le Pen and 100 about Macron; by the second round, there were over 500 bot accounts tweeting about each candidate.[81] However, these accounts generated different proportions of the candidate's traffic: 19.5 percent of the Twitter traffic about Macron was driven by highly automated accounts, compared with 14 percent of the Twitter traffic about Le Pen.[82] In round one, Twitter users in France shared links to high-quality news and political information at a ratio of two links to professional news for every one link to other kinds of news sources.[83] This ratio shrank to about 1:1 in the second round of voting.

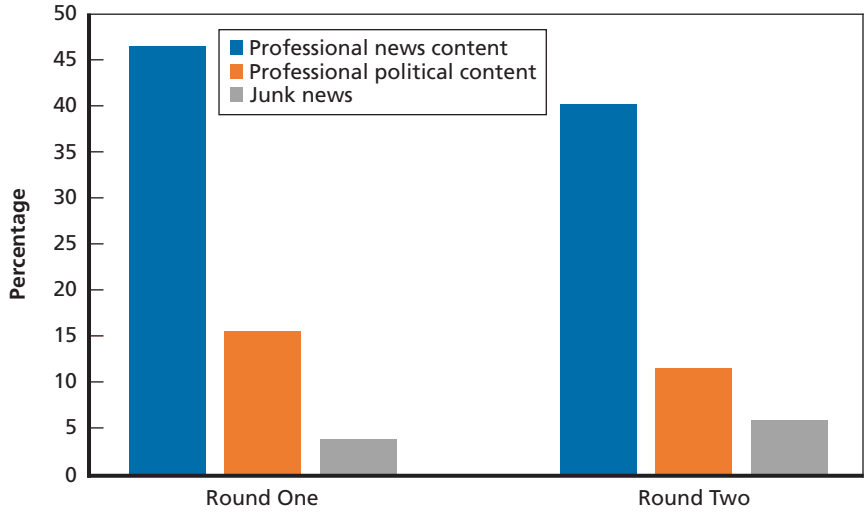
Before both rounds of the election, users most often shared legitimate news and political information (as noted in Figure 5.5). In round one, the largest proportion of content (46.7 percent) shared by Twitter users interested in French politics came from professional news organizations. Only 7 percent of the almost 9,000 links to content shared

[81] OII did not analyze the content or valance of specific tweets, so it is not possible to determine whether these automated accounts were pushing positive or negative information about the candidates or whether they were likely being run by the campaign itself or a saboteur.

[82] Desigaud et al., 2017, p. 3.

[83] Note that while "junk" or "fake" news is included in this category, this category also includes civil society content and personal blogs. Much of this category is composed of thoughtful work produced by civil society and individuals discussing political issues. About 21 percent of this category was judged to be junk news (Desigaud et al., 2017).

Figure 5.5
Political Content Shared by Twitter Users in Rounds One and Two of the 2017 French Election



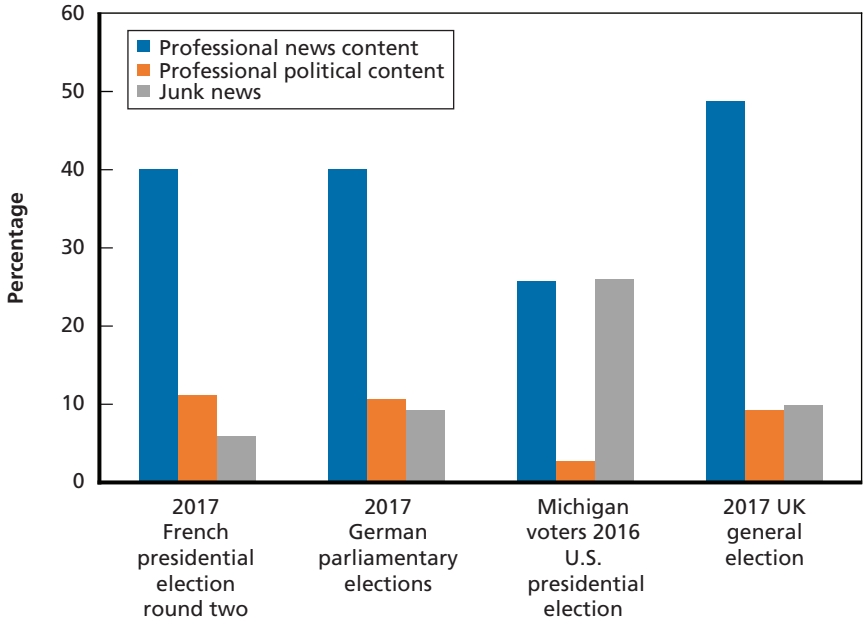
by users in this sample led to either what OII classifies as "junk news" based on misinformation[84] or to content produced by known Russian sources of political information. However, there was a noticeable shift in the second sample; users shared a lower proportion of credible sources and a slightly higher proportion of fake news.

Overall, Twitter users discussing French politics proved less susceptible to spreading misinformation and fake news than users discussing American, German, or British politics.[85] Figure 5.6 compares the prevalence of several types of political content shared on Twitter shortly before elections in France (round two), Germany (September

[84] "This content includes various forms of propaganda and ideologically extreme, hyperpartisan, or conspiratorial political news and information. Much of this content is deliberately produced false reporting" (Desigaud et al., 2017, p. 3).

[85] Monica Kaminska, John D. Gallacher, Bence Kollanyi, Taha Yasseri, and Philip N. Howard, "Social Media and News Sources During the 2017 UK General Election," Data Memo 2017.6, Oxford, UK: Project on Computational Propaganda, Oxford Internet Institute, University of Oxford, June 5, 2017, p. 6.

Figure 5.6
Political Content Shared by Twitter Users in Several Elections (in percentages)



2017 parliamentary elections),[86] the United States (sample of Michigan voters in 2016 presidential election),[87] and the United Kingdom (June 2017 general election).[88]

Automated bots potentially controlled by state actors were not the only interlopers in political discourse on the French presidential elections. According to Buzzfeed News, which gained access to a chatroom called "The Great Liberation of France" via an anonymous user, purported Trump supporters were posing online as French voters in

[86] Lisa-Maria Neudert, Bence Kollanyi, and Philip N. Howard, "Junk News and Bots During the German Parliamentary Election: What Are German Voters Sharing over Twitter?" Data Memo 2017.7, Oxford, UK: Project on Computational Propaganda, Oxford Internet Institute, University of Oxford, September 19, 2017.

[87] Howard et al., 2017.

[88] Kaminska et al., 2017.

attempts to promote Marine Le Pen and troll her opponents.[89] The group was devoted to creating "as much chaos on social media as possible" to make right-wing candidate Marine Le Pen and her supporters in the FN seem like the most legitimate voice in French politics. Their strategic planning document laid out several upcoming European elections they hoped to influence and even demonstrated familiarity with the effective marketing strategy of segmentation and targeting.[90] It is unclear how large this group is, though Buzzfeed explains that it is part of a larger network of private chatrooms (some operating in English and some in French) with similar *raisons d'etre*. This network shares strategies and targets among its members. According to the anonymous user who granted Buzzfeed access, "the shared agenda is to get far right, pro-Russian politicians elected worldwide. It's not so much a conspiracy as it is a collaboration. . . . The alt-right sees the US as compromised and Russia as the good guys" who will oppose Muslim influence.

Evaluating Impact

If we assume, as many observers do, that France resisted social manipulation efforts effectively, we can draw out some interesting thoughts for future research. With limited metrics and information, some potential reasons for French resistance stood out: the relatively lower penetration of social media in France compared with other countries recently plagued by social manipulation efforts and the improved awareness of social manipulation and the capacity to combat it among social media companies and traditional media (which France enjoyed because other countries, such as the United Kingdom and the United States, were hit by alleged social manipulation first). Finally, the runoff vote was not close, with Macron garnering about double the votes of Le Pen. Even if disinformation campaigns did succeed in persuading some voters to

---

89 Ryan Broderick, "Trump Supporters Online Are Pretending to Be French to Manipulate France's Election," Buzzfeed News, January 24, 2017.

90 The document instructs citizens from certain countries to conduct reconnaissance and provide links to socially relevant YouTube channels, Twitter accounts of journalists, and other relevant online communities, explaining that the leadership is not familiar with internet segments in every targeted country.

support Le Pen, it was clearly not enough to change the outcome of the election.

One reason may be that social media use in France is significantly lower than in the United States or United Kingdom.[91] Only 40 to 45 percent of the French population used social media in 2016.[92] In comparison, 81 percent of Americans[93] and 64 to 66 percent of the British population has a social media account.[94] Given that so much of social manipulation is believed to occur on social media networks, this divergence is notable and worthy of further examination. Susan Banducci, a social scientist at the University of Exeter, does make the important point that misinformation spread on social media may have "second-order influence" beyond the immediate audience. Journalists could perceive "bot-boosted" messages as a shift in the public mood, or bots could push unsubstantiated rumors into the credible media, thus influencing the wider public.[95] However, this risk is likely decreased the lower the proportion of the population that actively uses social media, at least in part because the media understand this fact and know Twitter cannot give the pulse of the entire French public.

A second reason for the limited effects in French elections may be that social media companies such as Facebook were more aware of the dangers of fake news and social manipulation by spring 2017 and took steps to combat them. Better policing and proactive responses to fake accounts or news stories by Facebook may have helped France

---

91 All of the data on social media use are sourced from Statista. Statista provides access to statistics and studies gathered by market researchers, trade organizations, scientific publications, and government sources.

92 French use of social media was more difficult to pinpoint than that of other countries, though most estimates fell within the 40 to 45 percent range. This range is provided by the following sources: "Share of Individuals in France Participating in Social Networks from 2011 to 2016," Statista, 2017; "Number of Social Network Users in France from 2014 to 2018 (in Millions)," Statista, 2017; "Social Network Usage in France," Statista Dossier, 2017.

93 "Percentage of U.S. Population with a Social Media Profile from 2008 to 2017," Statista, 2019.

94 "Social Media Usage in the United Kingdom," Statista Dossier, August 2017, p. 7.

95 Chris Baraniuk, "Beware the Brexit Bots: The Twitter Spam out to Swing Your Vote," *New Scientist*, June 22, 2016.

better withstand attempts at meddling.[96] In response to increased pressure following allegations that state actors used Facebook to influence the 2016 U.S. presidential election and UK referendum, the company stepped up its efforts to combat automated accounts and fake news. A few weeks before the first round of the French election, a Facebook security team manager announced that Facebook had improved its ability to recognize and neutralize "inauthentic accounts."[97] Facebook also established a program in France to use outside fact-checkers to combat fake news in users' feeds. In April 2017, Facebook deleted more than 30,000 fake accounts in France that were found to be repeatedly posting stories (a sign of automation) or violating its guidelines.[98] By July, that number had reportedly jumped to 70,000 accounts, many of which were spewing propaganda or spam related to the election.[99]

Third, French traditional media took a proactive approach to countering misinformation. One of France's most well-known news organizations, *Le Monde*, compiled a comprehensive, easy-to use database of unreliable news or political information websites months before the election.[100] People can visit *Le Monde*'s page and type in a URL or site name to check whether it is a credible news source. In addition, the organization offers downloadable web browser extensions that use a color-coded system to alert readers when something they are reading is false (red) or unverified (yellow).

Fourth, the runoff vote between Le Pen and Macron was not close. French polling, which is more experienced and skilled than American or British polling at accounting for the impact of "shy" far-

---

96 Tom Regan, "Facebook Helped Blunt Russian Meddling in French Elections," *Engadget*, July 27, 2017.

97 Shabnam Shaik, "Improvements in Protecting the Integrity of Activity on Facebook," Facebook, April 12, 2017.

98 Eric Auchard and Joseph Menn, "Facebook Cracks Down on 30,000 Fake Accounts in France," Reuters, April 13, 2017.

99 Joseph Menn, "Exclusive: Russia Used Facebook to Try to Spy on Macron Campaign—Sources," Reuters, July 27, 2017.

100 Jessica Davies, "*Le Monde* Identifies 600 Unreliable Websites in Fake-News Crackdown," *Digiday*, January 25, 2017.

right voters (partly because the FN party has been around for decades), indicated that this would not be a close race.[101] Polling suggested that Macron would win by a decent margin; he received about two-thirds of the vote to Le Pen's one-third. Even if a considerable number of people were influenced enough by misinformation campaigns to shift their vote (which is entirely possible), it would likely not have been enough to change the outcome.

National Orientation and Security Policies

Defense spending in France has trended slightly downward over the past decade, from highs of 2.5 percent in 2003–2004 and 2009 to under 2 percent by 2016–2017. More recently, however, France added about $2 billion to its 2018 defense budget as part of a plan to increase defense spending over the next five years.[102]

More broadly, since 2014 France has taken a host of steps designed to demonstrate toughness in the face of Russian intimidation. It canceled the sale of two naval helicopter carriers to Russia in response to Russia's annexation of Crimea and actions in Ukraine, called on the International Criminal Court to investigate Russia for possible war crimes in Syria, and formally identified Russian media organizations RT and Sputnik as organs of influence during the 2017 French presidential election. France's 2017 defense and national security strategic review describes Russian activity in the North Atlantic region as a major concern for France and its allies, including Russia's efforts to divide the European Union.

While France remains a committed member of NATO, the French government appears to be focusing on its relationships within the European Union. One recent analysis argues that France's 2017 Strategic Review indicates a "slow reversal" of the two previous French governments' heavy investment in a strong partnership with the United States. The author argues that France supports the concept of "mini-

---

[101] Emily Schultheis, "What Went Right with the French Campaign Polls?" *The Atlantic*, May 13, 2017.

[102] Pierre Tran, "France Adds $2B to Defense Budget, Moving Closer to NATO Spending Target," *Defense News*, September 27, 2017.

lateralism," cooperating in small groups below the level of large organizations such as NATO, as a way for France to prioritize European partnerships.[103]

Public support for NATO in France decreased by 15 percentage points from 2015 to 2016, dropping to its lowest point since 2009 (when Pew began collecting data), though it recovered somewhat in 2017.[104] Only a small majority of the French (53 percent) would support their country using force to defend a NATO ally if it were to become engaged in a "serious military conflict" with Russia—but unlike Great Britain, this figure has actually increased from 2015, when the same small majority opposed France using military force to defend a NATO ally. The percentage of the French public that believes the United States would use force to defend a NATO ally in a conflict with Russia dropped from 65 percent in 2015 to 60 percent in 2017.

President Macron called for an overhaul of the European Union in a September 2017 speech, proposing a variety of goals and initiatives the European Union could set for itself to increase integration of European nations. For example, he proposed that the French and German markets could be completely integrated by 2024.[105] He also proposed a European Intervention Initiative "aimed at developing a shared strategic culture" and advocated for enhancing intelligence sharing and coordination among Europe's intelligence services to deal with an increasingly complex and diverse terrorist threat.[106] Though the United Kingdom is set to leave the European Union and has traditionally been reluctant to embrace further coordination of European militaries, at a January 2018 UK-France summit, President Macron encouraged the United Kingdom to join the European Intervention Initiative, and the United Kingdom agreed to several measures to increase cooperation with France.[107]

---

[103] Alice Pannier, "Between Autonomy and Cooperation: The Role of Allies in France's New Defense Strategy," *War on the Rocks*, November 2, 2017.

[104] Stokes, 2017.

[105] "Sorbonne Speech of Emmanuel Macron—Full Text/English Version," 2017.

[106] "President Macron's Initiative for Europe: A Sovereign, United, Democratic Europe," French Ministry for Europe and Foreign Affairs, September 26, 2017.

[107] "UK and France Commit to New Defence Cooperation," 2018.

France and Germany recently led efforts to convince EU countries to integrate logistics and crisis response troops and cooperate on weapons research and development (such as a new generation of tanks) in a new defense agreement.[108] In December 2017, 25 EU member states signed the PESCO defense pact.[109] The participating countries (which notably do not include the United Kingdom) are set to begin several joint defense projects in 2018. PESCO allows member states to jointly develop military capabilities and invest in projects as part of a wider goal to enhance interoperability of European forces. These projects include creating a European military training center and establishing common standards for military radio communications. An adviser to the EU High Representative for Foreign Affairs and Security Policy called PESCO a "game-changer" after years of stalled EU efforts on greater security cooperation.[110] PESCO will increase both interoperability of European forces and the efficiency of European defense spending.[111]

Germany

The impact of social manipulation efforts on the German political and social environment is difficult to assess—while only a minority of Germans view Russia favorably or believe it treats its people fairly, there have been noticeable increases in these minorities over the past few years. At the same time, German defense spending increased in 2017, German citizens' support for NATO has increased since 2015, and Germany has recently led efforts to strengthen the capacity of militarily weaker NATO members and establish a new EU defense and security cooperation agreement (PESCO).

---

[108] Michael Peel, "EU States Poised to Agree Joint Defence Pact," *Financial Times*, November 7, 2017.

[109] "Twenty-Five EU States Sign PESCO Defense Pact," *Deutsche Welle*, December 11, 2017.

[110] Peel, 2017.

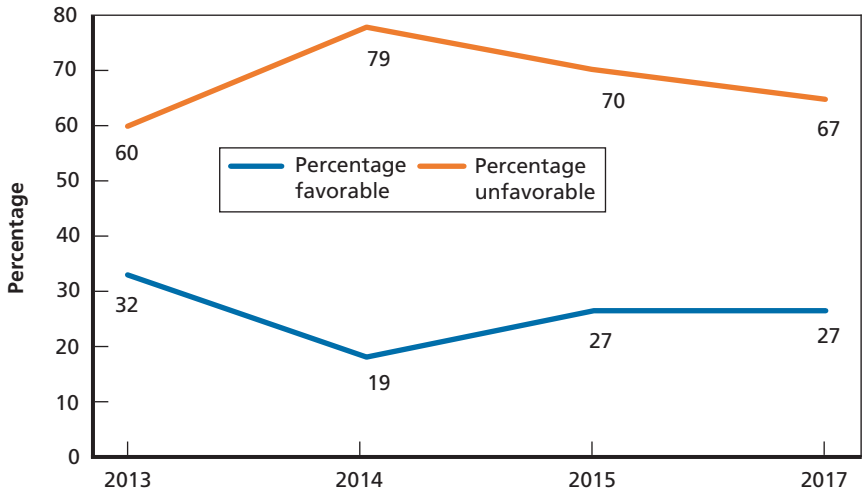
[111] Peel, 2017.

Public Attitudes Toward Russia

As in many other countries, in Germany trends in public attitudes toward Russia since 2014 are surprisingly favorable (see Figure 5.7). The percentage of Germans who view Russia favorably has increased since 2014. Only 33 percent of Germans believe that Russia's power and influence is a major threat.[112] Germans are more confident that Putin would do the right thing in world affairs (25 percent) than they are that Trump would do the right thing (11 percent). From 2014 to 2017, the percentage of Germans agreeing that the Russian government respects the personal freedoms of its people increased from 8 percent to 14 percent.

In Germany, young men are the most likely demographic to hold favorable views of Russia. There is a 14–percentage point gap between men who hold favorable views of Russia and women who hold favor-

Figure 5.7
Favorability Ratings for Russia Among German Public, 2013–2017



[112] Unfortunately, Pew began asking this question in only 2017. German firm Bertelsmann Stiftung found similar results in a 2016 poll: About 38 percent of Germans perceived Russia to be a threat. Gabriele Scholer, "Russia—A Threat to European Security? A View from Germany," Bertelsmann Stiftung, October 1, 2016.

able views.[113] A plurality (39 percent) of the group that indicated favorable views of Russia was between 18 and 29 years old (this is also typically the age group with the highest use of social media, which is an interesting correlation). This age group is also the most likely to believe that Russia respects the personal freedoms of its people.

National Orientation and Security Policies

German defense spending as a percentage of GDP has remained stable for over a decade, remaining within 1.2 to 1.4 percent of GDP since 2000.[114] There was an uptick in defense spending in 2017 from the past several years. Angela Merkel's Christian Democrats (CDU) and the center-left Social Democratic Party (SPD) both support increasing defense spending, but the two parties diverge on scale: The SPD does not agree with Defense Minister Ursula von der Leyen's proposal to increase the defense budget to up to 2 percent of GDP by 2024.[115]

Germany remains a committed and important member of NATO, although the proportion of its GDP allocated to defense remains below NATO's 2-percent threshold. In addition to increasing defense spending, Germany is taking a leading role in developing the capabilities of NATO members under NATO's Framework Nation Concept (FNC).[116] In the past year Germany has increased defense ties with the Czech Republic and Romania under the FNC; each nation contributed a brigade to a German-led multinational division.[117]

---

[113] Vice, 2017.

[114] "Military Expenditure by Country As Percentage of Gross Domestic Product," Stockholm International Peace Research Institute, 2017.

[115] Nina Werkhäuser, "German Military Spending Gets Political," *Deutsche Welle*, August 8, 2017.

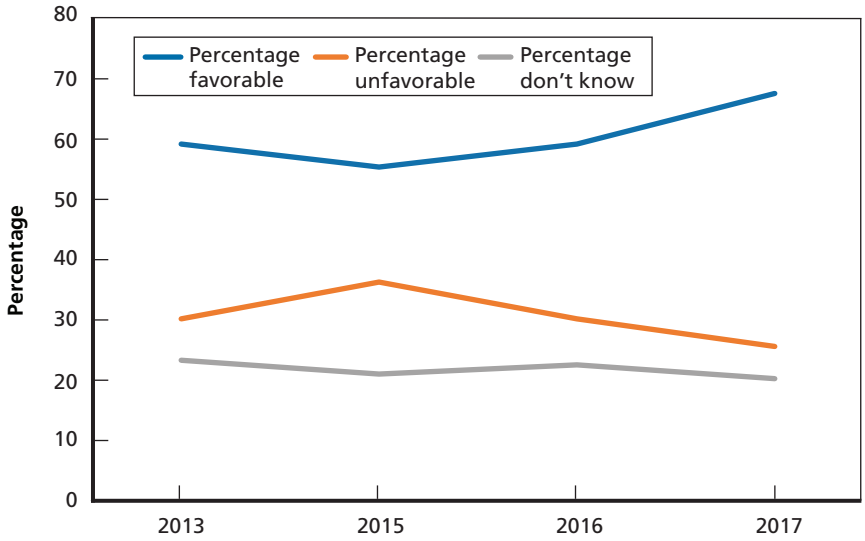
[116] Rainer L. Glatz and Martin Zapfe, "Ambitious Framework Nation: Germany in NATO," German Institute for International and Security Affairs, September 2017, p. 1.

[117] "Germany, Romania and the Czech Republic Deepen Defence Ties," North Atlantic Treaty Organization, February 16, 2017.

Public support for NATO has increased in Germany over the past few years, as noted in Figure 5.8.[118] However, only a minority of Germans (40 percent) would support their country using force to defend a NATO ally if it were to become engaged in a "serious military conflict" with Russia, making Germany less supportive than countries like France (53 percent would support) and the United States (62 percent would support).

In 2015, the German government pledged to increase defense spending and overhaul its security strategy in the coming years in response to Russian attempts to use "power politics and military force" to assert its interests.[119] Germany has recently led efforts to increase EU defense cooperation, which culminated in the signing of the PESCO

Figure 5.8
Favorability Ratings for NATO Among German Public, 2013–2017



[118] Bruce Stokes, "NATO's Image Improves on Both Sides of Atlantic," Pew Research Center, May 23, 2017.

[119] "Germany Says New Security Strategy Will Respond to Russia," Reuters, February 17, 2015.

defense pact by 25 EU member states in December 2017.[120] The participating countries (which include France, Italy, and Poland but do not include the United Kingdom) are set to begin several joint defense projects in 2018. An adviser to the EU High Representative for Foreign Affairs and Security Policy called PESCO a "game-changer" after years of stalled EU efforts on greater security cooperation.[121] PESCO allows member states to jointly develop military capabilities and invest in joint projects as part of a wider goal to enhance interoperability of European forces. These joint projects include standing up a European military training center and establishing common standards for military radio communications. Germany has partnered with Baltic states in programs to counter Russian disinformation, and its 2016 national security strategy criticized Russia for endangering the postwar security order and favoring strategic rivalry over partnership with the West.

The Baltic States

Few countries have been subject to more consistent Russian information manipulation over the past four to five years than the Baltics. With their significant Russian-language populations and given Russia's concern and resentment about NATO membership, Moscow has sought various means of shaping narratives in the Baltics. As elsewhere, however, it is not clear that these efforts have had measurable impact since 2014.

Attitudes Toward Russia in the Baltics

A common pattern in Estonia and Latvia is for opinions on foreign policy issues and attitudes toward Russia to be sharply divided along ethnic lines (native Estonian/Latvian and native Russian). Overall, 59 percent of Estonians and 43 percent of Latvians surveyed said they felt threatened by Russia in military terms in a 2016 poll.[122] Disaggregating the data by ethnicity shows significant differences between

[120] "Twenty-Five EU States Sign PESCO Defense Pact," 2017.

[121] Peel, 2017.

[122] Scholer, 2016.

native Estonians and Latvians and the Russian-speaking minorities in both countries: Between 70 percent and 80 percent of Latvian and Lithuanian speakers in these countries view Russia as a threat, as opposed to only a few percent of Russian speakers.[123]

Even among the ethnic Russian populations, however, surveys in the Baltics point to distinct limits on the effects of Russian disinformation. One study of attitudes in Estonia finds that ethnic Russian citizens tend to access a wider array of information than ethnic Estonians, in part because they trust almost no sources of information. Ethnic Russians, like all Estonians, are "tired of all the negativity" and more opposed to the pessimism of many news sources than the content. Multiple interviews on the ground showed an image of "the sober-minded nature of [Estonia's] Russian-speaking population" rather than any sense of virulent nationalism.[124]

A similar study in Latvia also found diverse attitudes and no clear pattern of Russian dominance of ethnic Russian attitudes. Only about half the ethnic Russians interviewed or surveyed for the study supported Russian narratives. Applying social science theories regarding the transition from attitudes to behavior, moreover, the study found little evidence that ethnic Russians in Latvia could be roused into violent or disruptive action by disinformation campaigns. "It would be difficult for Russia to mobilize a society," the study concluded, "which is socially and politically inactive, and does not know of, or support, pro-Russia organizations and individuals."[125]

More specifically, less than 14 percent of the ethnic Russians polled said they had a strong sense of "belonging to Russia," and only about 21 percent said that Russian "intervention to protect Russian speakers is necessary and justified." The polls strongly suggest that, as in so many contexts, it is the underlying social conditions that are the real

---

[123] Scholer, 2016.

[124] Jill Dougherty and Riina Kalijurand, "Estonia's 'Virtual Russian World': The Influence of Russian Media on Estonia's Russian Speakers," International Centre for Defense and Security, Estonia, October 2015.

[125] Martins Hirss, "The Extent of Russia's Influence in Latvia," National Defense Academy of Latvia, Working Paper No. 03/16, November 2016, pp. 3–4.

issue: 14.5 percent of those polled said "life in Latvia is very bad," and almost 30 percent agreed that the society discriminates against those who do not know Latvian. Some polls that distinguished households that specifically spoke Russian at home showed higher numbers—28 percent saying they felt a belonging to Russia, 41 percent saying Russian intervention was required to protect Russian speakers in Latvia, and over half believing Russia's claim that the Latvian government was pursuing a "restoration of fascism." Evidence suggests that economic variables, such as unemployment, play a major role in determining Russian speakers' views of the society.[126]

National Orientation and Security Policies

Defense spending in both Estonia and Latvia (and Lithuania) has been trending upward since 2013. Estonia has been spending at least 2 percent of GDP on defense for the past few years, and Latvia is within 0.3 percent of the 2-percent NATO guideline. Table 5.2 catalogs multiple initiatives since 2014 signaling a continued and indeed deepened intention on the part of the Baltics to sustain close partnerships with NATO and the European Union.

Most of the population in Estonia considers NATO their main security guarantee and supports NATO membership. Over the past few years, the public has become increasingly confident that NATO would provide military aid if Estonia were to be threatened with military aggression (although in 2017 only half of respondents believed NATO would provide direct military assistance, a slight increase from 2016).[127] However, native Estonians are far more likely to trust and support NATO than native Russian speakers. While 89 percent of native Estonian speakers approved of NATO troops' physical presence in Estonia in 2017, only 27 percent of Russian speakers approved.[128]

In January 2018 the Estonian prime minister lauded the strength of the relationships between Estonia and NATO and Estonia and the United States, pointing to the presence of U.S. troops in Estonia

---

[126] Hirss, 2016, pp. 10, 19.

[127] Juhan Kivirähk, "Public Opinion and National Defence," Tallinn: Estonian Ministry of Defense, Spring 2018, p. 56.

[128] Kivirähk, 2018, pp. 57–58.

Table 5.2
Recent Security Initiatives in the Baltics

Estonia	• 2014: Estonian President Toomas Hendrick Ilves stated that "The current security architecture in Europe, which relied on both the Helsinki Final Act and the Paris Charter, has now collapsed, following Russia's aggression in Ukraine."[a] • 2015: Estonian Air Force announced planned expansion of the Amari air base to allow for additional NATO aircraft. • 2016: Commander of Estonian defense forces, Lt General Riho Terras, stated that Patriot missile defense systems are needed in the Baltic states to deter a Russian invasion. • 2017: Estonian national security concept stated that Estonia will continue to work closely with NATO and the European Union in the face of Russia's unpredictable, aggressive and provocative activity. • 2017: Baltics signed a joint plan to simplify bureaucratic barriers and facilitate the movement of NATO forces in the region.
Latvia	• 2014: Riga (Latvia's capital) mayor Nils Usakovs claimed that Putin has brought stability to the region and is the best Russian president Latvia can have at the moment. • 2015: Latvia's national security concept stated that Russia's actions have created long-term negative effects on the national security of the Republic of Latvia. • 2016: Latvia increased its defense budget by 42%, though still below the 2% of GDP target set for NATO members. • 2016: Latvia's national defense concept stated that in recent years, Russia had employed a number of methods to erode the security of Latvia. 2012 iteration noted cooperation with Russia is a security and stability strengthening aspect of the Baltic Sea region. • 2016: Latvia promised to increase defense spending to 2% of GDP by 2018. • 2017: Baltics signed a joint plan to simplify bureaucratic barriers and facilitate the movement of NATO forces in the region.
Lithuania	• 2014: Since 2014, Lithuania's defense spending has steadily increased each year. • 2014: Lithuania established a rapid reaction force to address a potential hybrid warfare scenario by Russia. • 2014: Lithuania's national security threat assessment stated that one of the primary areas of threats emanates from Russian foreign policies. • 2016: Lithuania increased its defense budget by 34%, though still below the 2% of GDP target set for NATO members. • 2016: Lithuania permanently reinstated a 9-month conscription service to fully equip military units and prepare sufficient reserves.
Lithuania	• 2016: Lithuanian national security threat assessment cited Russia's imperialistic ambitions and aggressive foreign policy as one of the greatest national security threats to Lithuania. • 2017: Baltics signed a joint plan to simplify bureaucratic barriers and facilitate the movement of NATO forces in the region. • 2017: Lithuania's national security strategy stated that, "The main threat for the security of the Republic of Lithuania is posed by aggressive actions of the Russian Federation."[b] • 2017: Ahead of the 2017 Russian Zapad military exercise, Lithuania constructed a high wire fence along its border with Kaliningrad to help prevent provocations.

[a] Jeremy Bender, "Estonian President: Europe's Security Architecture 'Has Collapsed,'" *Business Insider*, September 19, 2014.
[b] "National Security Strategy," Republic of Lithuania, January 17, 2017.

(though the majority of NATO troops in Estonia are British), NATO's Enhanced Forward Presence, and the boost in the amount of military equipment given to Estonia by the United States in 2017.[129] Finally, given the 2007 cyberattacks against Estonia and Estonia's use of an online voting system, the country is invested in close cooperation with NATO on cybersecurity. The NATO Co-operation Cyber Defence Centre of Excellence was established in Tallinn in 2008.[130]

Estonia is among the 25 EU member states that signed the PESCO defense agreement in December 2017.[131] PESCO allows member states to jointly develop military capabilities and invest in projects as part of a wider goal to enhance interoperability of European forces. Estonia suggested adding an obligation to simplify European military transport to the joint notification, which was accepted. According to Estonian Minister of Defense Jüri Luik, minimizing the red tape and bureaucracy involved in the movement of units and supplies promotes the objectives of both the European Union and NATO.[132]

A Canadian-led NATO multinational battlegroup was deployed to Latvia in 2017.[133] More than half (59 percent) of respondents in a November 2016 Latvian Ministry of Defense–sponsored poll agreed that the presence of NATO troops in Latvia increases Latvian security [the decision to send the multinational battlegroup to Latvia was made in July 2016].[134] Almost half of respondents believed that the security situation has improved since 2015. The main reasons given for this improvement were the presence of NATO in Latvia, improved military training, and the purchase of equipment and technologies.

---

129 Turak, 2018.

130 "Estonia and NATO," Republic of Estonia Ministry of Foreign Affairs, July 3, 2017.

131 "Twenty-Five EU States Sign PESCO Defense Pact," 2017.

132 "Deepening of Defence Cooperation in the EU Strengthens Europe's Security," press release, Foreign Affairs Council, November 13, 2017.

133 "Secretary General Marks Deployment of NATO Battlegroups During Visit to Latvia," press release, NATO, June 19, 2017.

134 "Residents' Poll on State Defence Issues," Ministry of Defence of the Republic of Latvia, 2016.

In the past few years, Latvia has been involved in several initiatives to enhance cooperation between various EU member states. Latvia is among the 25 EU member states that signed the PESCO defense agreement in December 2017. In 2017, Latvia and Norway signed memoranda of understanding to cooperate on various economic and climate issues.[135] Both Latvia and Estonia are participants in the Interreg Baltic Sea Region Programme 2014–2020, an EU-funded program to encourage greater cooperation and innovation among countries in the region.[136] In 2016, Latvia hosted the fifth summit of heads of government of Central and Eastern European Countries and China (16+1).[137]

Poland

Poland is struggling with a radical far-right movement that appears to be increasingly emboldened by the rise to power of a far-right populist party (Law and Justice party, PiS) in 2015. Polish domestic and foreign policy has been significantly altered by the PiS, resulting in strained relations with the European Union and raising concerns over new Polish defense plans. However, Polish support for NATO is the highest it has been in a decade, and the percentage of Poles who believe they should come to the defense of a NATO ally if it were to become engaged in a military conflict with Russia has increased significantly since 2015. These increases are likely driven by the pronounced fear of Russia and distrust of President Putin among the Polish public.

---

[135] "Closer Cooperation with Latvia," Mission of Norway to the European Union, December 14, 2017.

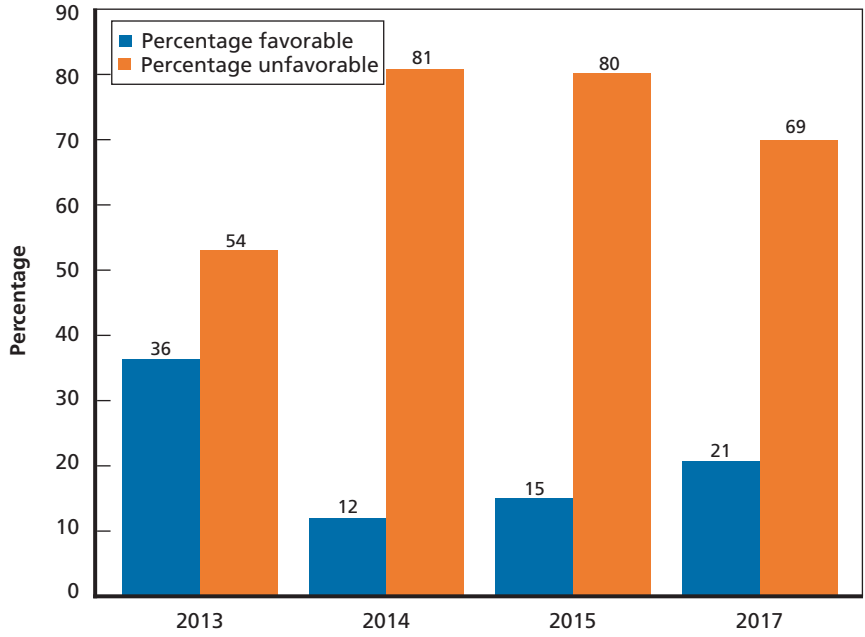
[136] The program is an agreement between EU member states Denmark, Estonia, Finland, Latvia, Lithuania, Poland, Sweden, and the northern parts of Germany, as well as partner countries Norway, Belarus, and the northwest regions of Russia ("About the Programme," Interreg Baltic Sea Region, fact sheet, Rostock, Germany, undated).

[137] The 16+1 is an initiative by the People's Republic of China to expand cooperation with 11 EU member states and 5 Balkan countries (Albania, Bosnia and Herzegovina, Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Macedonia Montenegro, Poland, Romania, Serbia, Slovakia, and Slovenia). Ministry of Foreign Affairs of the Republic of Latvia, "16+1 Summit Has Concluded," press release, February 22, 2017.

Attitudes Toward Russia in Poland

As indicated in the 2017 Pew Global Attitudes Survey,[138] the percentage of the Polish public that views Russia favorably has increased by 9 percentage points since 2014, though it still remains well below 2013 levels (see Figure 5.9). Sixty-five percent of Poles surveyed believe Russia poses a major threat to Poland (and 25 percent believe Russia poses a minor threat); only 5 percent said Russia did not pose a threat.[139] Significantly more Poles are confident that Trump would do the right thing in world affairs (23 percent) than they are that Putin would do the right thing (4 percent).

Figure 5.9
Favorability Ratings of Russia Among Polish Public, 2013–2017



[138] Vice, 2017.

[139] Unfortunately, Pew began asking this question in only 2017.

National Orientation and Security Policies

Poland's defense spending as a percentage of its GDP has stayed between 1.8 percent and 2.2 percent since the mid-1990s.[140] In October 2017, Poland formalized plans to gradually increase defense spending to 2.5 percent of GDP by 2030.[141]

Poland remains a committed member of NATO, hosting an American-led NATO battle group and recently hosting major NATO defensive exercises.[142] However, under the PiS, Poland is attempting to become more self-sufficient; the Polish defense minister stated that the goal was for Poland to be able to defend itself within 12 years. One official within the PiS government anonymously expressed anxiety over this objective, saying that it would send a negative message to NATO allies. About a quarter of Poland's top military officials have resigned since PiS came to power, due to unspecified policy disagreements with PiS leadership.[143] Poland has recently moved its most capable tanks to Warsaw, to be closer to Russia. Military experts have warned that this is a dangerous move—the Warsaw base does not currently have the necessary infrastructure or personnel to support these more sophisticated tanks, meaning that for a period of about two years (the time it is anticipated to take to establish the necessary support at Warsaw), these tanks are essentially useless. In the case of a surprise attack, Poland would not be able to mobilize and deploy these tanks.[144]

As noted in Figure 5.10, Polish support for NATO in 2017 is at the highest point it has been since 2007, when Pew began collecting data.[145] The percentage of Poles who would support their country using

---

[140] "Military Expenditure by Country as Percentage of Gross Domestic Product," 2017.

[141] "Polish President Signs Defence Spending Boost into Law," Radio Poland, October 23, 2017.

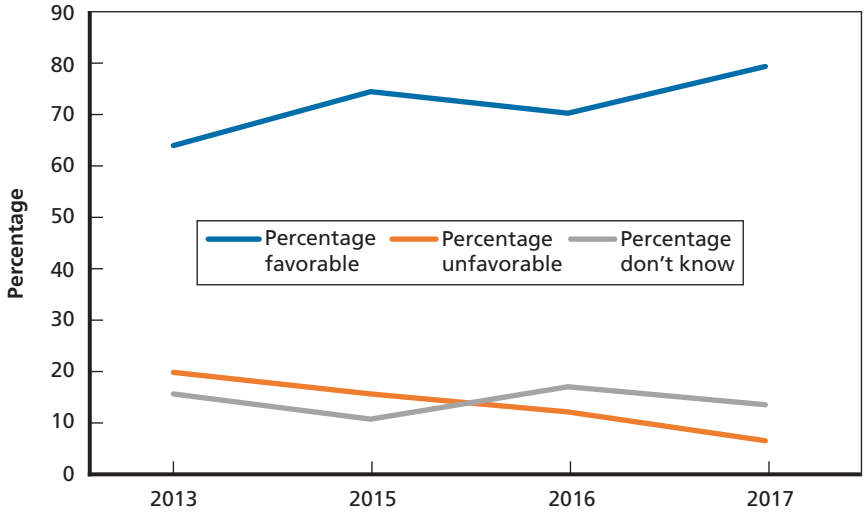
[142] Cheryl Pellerin, "Poland, a Valued NATO Member, Leads by Example, Mattis Says," press release, U.S. Department of Defense, September 22, 2017; "Poland, NATO Launch Defensive Exercises amid Security Concerns," CBS News, September 21, 2017.

[143] Lidia Kelly, "Poland Plans Trump-Era Defense Spending Splurge, Critics Say 'Unrealistic,'" Reuters, June 16, 2017.

[144] Kelly, 2017.

[145] Stokes, 2017.

Figure 5.10
Favorability Ratings for NATO Among Polish Public, 2013–2017



force to defend a NATO ally if it were to become engaged in a "serious military conflict" with Russia significantly increased between 2015 and 2017, as did the percentage who believed the United States would come to the defense of a NATO ally (increased from 49 percent in 2015 to 57 percent in 2017). Unsurprisingly, Pew found that countries that considered Russia more of a threat generally also had a higher level of NATO solidarity and support.[146]

While 76 percent of Poles agree that, overall, their country's membership in the European Union is a positive thing,[147] Poland's relationship with the European Union has become increasingly tense over the past few years. The refugee issue has been a serious point of tension between Poland and the European Union; in December 2017,

[146] Stokes, 2017, pp. 8.

[147] "Majority of Young People in Central and Eastern Europe Strongly Backs the EU," Bertelsmann Stiftung, March 21, 2017.

the European Commission (EC) took Poland (as well as Hungary and the Czech Republic) to the EU Court of Justice over the countries' refusal to accept the EU refugee resettlement plan. A small majority (51 percent) of Poles recently said that Poland should continue to refuse Muslim refugees even if it resulted in losing EU membership.[148]

The PiS-led government's recent democratic rollbacks have prompted threatened reprisals of an unprecedented severity from the EC (the EU executive arm), which has put serious strain on Poland's relationship with the European Union. The EC began an investigation into rule of law violations in Poland in January 2016. The Polish government rejected the EC's recommendations to improve rule of law in Poland as interference in sovereign Polish affairs. In December 2017, the EC proposed invoking Article 7 of the Treaty of the European Union (intended to ensure that EU member states respect human dignity and democracy) against Poland, which would be an unprecedented disciplinary step. If this proposal were to escalate and receive unanimous support from other EU members (which is unlikely), Poland could lose its voting rights.[149]

Summary of Outcome Evidence

If the goal of the recent Russian campaign has been to affect strategic positioning of states and populations and boost support for policies Russia desires, that effort appears to be largely failing. One scholar who is extremely concerned about Russian disinformation efforts nonetheless argued that "so far, the impact of Russian active measures in Europe appears to have been somewhat hit-and-miss—with an emphasis on 'miss.' Certainly, none of the past year's elections have yielded outcomes favorable to the Kremlin; in fact, European voters . . . have been mostly hewing to the main." Some egregious examples of Russian fake news, such as the "Our Lisa" story about a

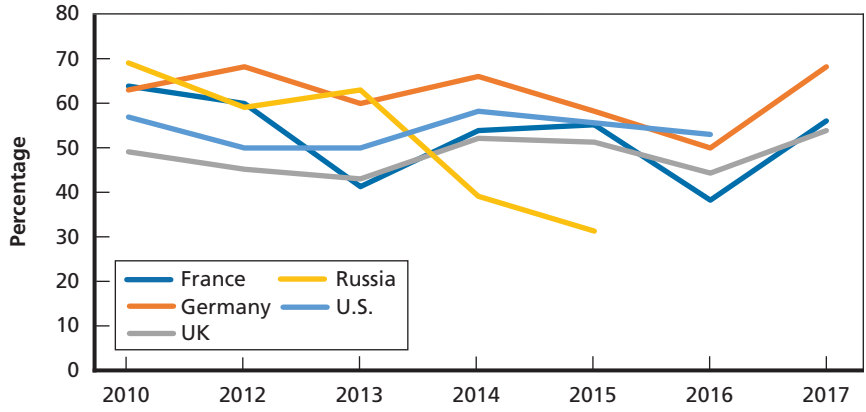
[148] Results from a July 2017 poll (Polish language) summarized in Remi Adekoya, "Why Poland's Law and Justice Party Remains So Popular," *Foreign Affairs*, November 3, 2017.

[149] Marek Strzelecki and Ewa Krukowska, "EU Sanctions Risk for Poland Rises on Democratic Backsliding," Bloomberg, December 20, 2017.

Russian-German girl who was falsely reported to have been raped by Arab migrants in January 2016, have generated backlash and general mistrust of any pro-Russian reports. European media have rallied to oppose Russian influence and form new mechanisms for fact checking. The German government, as one example, has responded with dozens of measures—including expanding its cyber resilience and media monitoring efforts. In the meantime, "NATO and the EU, far from crumbling into irrelevance, are experiencing a renaissance of purpose."[150]

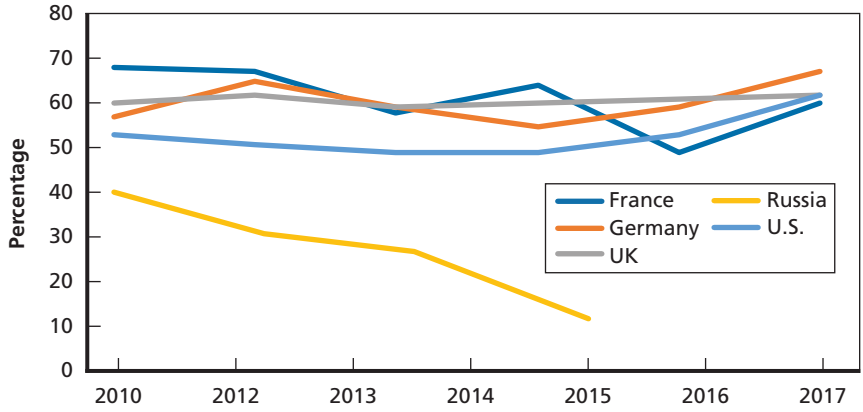
As one example, beyond the specific countries surveyed above, Figures 5.11 and 5.12 show current trends in favorability ratings for two key institutions that Russia appears to have tried to undermine: The European Union and NATO. In both cases, favorability in key European countries and the United States has *risen* over the past year, after several years of stagnation or slight decline.

Figure 5.11
Percentage of Various Publics with Favorable View of European Union



[150] Quotations in this paragraph are from Constanze Stelzenmüller, "The Impact of Russian Interference on Germany's 2017 Elections," testimony before the U.S. Senate Select Committee on Intelligence, June 28, 2017.

Figure 5.12
Percentage of Various Publics with Favorable View of NATO



Evidence from across Europe on faith in institutions more generally shows a somewhat similar pattern.[151] Between 2016 and 2017, for example, one major survey found that support for the European Union rose 11 points, and support for respondents' national governments rose nine points. Measures of trust in other institutions, such as the court system and the media, remained relatively stable, though there is significant variation among countries, largely attributable to specific socioeconomic or political developments.

One recent study of Russian interference in 27 different electoral events (elections and referendums) going all the way back to 1991 found little evidence of success. "Russia's efforts have made little difference," it concluded. In the post–Cold War years from 1991 to 2014, only four of 11 elections tilted as Russia hoped, and only one outcome (Ukraine in 1994) may have been attributable to Russian actions. Since 2015, the study found, Russia has tried to affect 16 elections; two (Brexit and the Czech Republic in 2017) reflected Moscow's wishes, and seven "partly" did so (when, for example, nationalist anti-EU parties received a larger share of the vote than before). In all those cases, moreover, powerful alter-

[151] This evidence is drawn from EC, "Special Eurobarometer 461: Designing Europe's Future," April 2017.

native variables were at work that make it impossible to ascribe unique effect to Russia's efforts. Russia "hasn't gotten much for its efforts," this study's scholars conclude, "and these efforts have often backfired."[152] One study that specifically focused on the impact of Russian social media in the 2014 Ukraine election found that "Russian state-controlled television has very uneven effects" and that it worked only on "receptive ears"—those who were already sympathetic to Russian messages.[153]

The reactions to and counterproductive results of Russian disinformation efforts run deeper, to the essential network of contacts by which Russia can exercise influence. Pro-Russian interest groups in Germany, for example, have lost influence "because so many German companies have been burned doing business in Russia." Partly as a result, German exports to Russia have been cut in half—from 4 percent of German exports to 2 percent—just between 2015 and 2017.[154]

In terms of geostrategic orientation, regionwide activities show many of the same trends as national action—a toughening posture toward Russia. Table 5.3 outlines several of the major NATO initiatives on this score since 2014.

To date, therefore, the dominant Russian efforts have been to make use of existing attitudes, not drive major changes in them. While there have been measurable *output* effects of Russian activities, such as numbers of Facebook likes or tweets, the best available evidence regarding geopolitical *outcomes* suggests that Moscow's actions have had limited effectiveness.

The only major outcome trend running in a favorable direction for Russia is public attitudes, but this appears to be an artifact of support for political parties that have expressed some sympathy for Russia. Otherwise, Russia does not appear to have achieved significant mea-

---

[152] Lucan Ahmad Way and Adam Casey, "Russia Has Been Meddling in Foreign Elections for Decades. Has It Made a Difference?" *Washington Post*, January 8, 2018. The comprehensive study is Way and Casey, "Is Russia a Threat to Western Democracy? Russian Intervention in Foreign Elections, 1991–2017," draft memo prepared for conference on Global Populisms as a Threat to Democracy? Stanford University, November 3–4, 2017.

[153] Leonid Peisakhin and Arturas Rozenas, "When Does Russian Propaganda Work—and When Does It Backfire? Here's What We Found." *Washington Post*, April 3, 2018.

[154] Stelzenmüller, 2017.

Table 5.3
NATO Collective Initiatives Since 2014

2014	• NATO agreed to establish a Very High Readiness Joint Task Force to have the capability to better respond to a Ukraine scenario. • NATO suspended all practical civilian and military cooperation with Russia within the NATO-Russia Council. • NATO's Strategic Communications Centre of Excellence was developed and received its first task: to study Russia's information campaign against Ukraine. • NATO stated that the developments in and around Ukraine are seen to constitute a threat to neighboring allied countries, with serious implications for security and stability.
2016	• Twenty-three NATO allies increased their defense expenditure in real terms by 3.8%, which added up to $10 billion (U.S.). • NATO agreed to send four multinational battalions to the Baltics and Poland as a deterrence force against Russian aggression. • NATO tripled the size of the NATO Response Force to 40,000 and set up eight small headquarters (NATO Force Integration Units) to facilitate training and reinforcements.
2017	• According to NATO's annual defense report, NATO allies in Europe and Canada will collectively increase defense spending by 4.3% in 2017.

surable results in key outcomes it might be seeking in the West: popular support for sympathetic right-wing parties (beyond the general trend already in evidence), hostility to political institutions, geopolitical orientation favoring Russia, and weakened security policies. In fact, Russia's use of hostile social manipulation has generated a profound reaction from the United States and Europe in ways that, on balance, may have created a less favorable strategic context for Moscow.

These conclusions, based as they are on Russian activities to date, reflect only the results of existing technologies. Our research on the social manipulation programs of both Russia and China reveals well-funded, increasingly sophisticated efforts to push the boundaries of the field and improve its effectiveness over time. Research underway in this project on the future of such technologies, moreover, points to the potential for a dangerous marriage of virtual realities, artificial intelligence, cyberintrusions, and social media outreach that could create remarkably influential campaigns. Our research on the effectiveness of Russian efforts to date, therefore, supports two conclusions: The effects of existing social manip-

ulation campaigns should be kept in perspective—and the United States has a possibly narrow window of opportunity to deal with this challenge before it potentially becomes dramatically more dangerous.

CHAPTER SIX

Hostile Social Manipulation: The Experience to Date—Conclusions and Implications

Our research into the character and evolving nature of hostile social manipulation supports several broad conclusions.

First, *the United States needs an updated framework for organizing its thinking about the complex issues involved with manipulation of infospheres by foreign powers determined to gain competitive advantage*. Chapter Two offers such a revised framework, in an effort to put social manipulation into a broader context of information competition. One challenge is that many concepts and terms overlap with one another in confusing ways; cybertools, for example, can be employed as part of social manipulation efforts or in diverse ways—directing attacks on infrastructure targets, for example. Traditional military concepts such as information operations, psychological operations, and military support to information operations do not begin to capture the full scope of hostile social manipulation. A coherent framework for organizing the various components of the challenge is the first step toward improved policy.

Second, it is now clear that *leading autocratic states have begun to employ information channels for competitive advantage; these plans remain in their initial stages and could unfold in several ways*. States such as Russia and China appear to view such techniques as a source of leverage relative to open societies. They believe themselves to be engaged in an information war with the West—one begun by the United States and its friends and allies—and have begun to invest significant resources in such tools. They see many forms of information competition as parts of an overarching, holistic competitive space and pay less

attention to precise definitional categories or institutional silos than do Western governments. They are investing hundreds of millions of dollars in the effort and assembling considerable experience with this tool of statecraft. Though some of the initial Russian political efforts were haphazard and amateur, that is not likely to remain true for long. Both countries are dedicated to controlling their domestic information environment and using information tactics to gain increasing leverage over other countries.

Third, this research suggests that *efforts at social manipulation are effective to the degree that vulnerabilities in a society allow them to be effective*. Such techniques can seldom create from whole cloth the situations that allow an aggressor to manipulate political life; they can only take advantage of realities being created by underlying trends. This has been the story of Russian and Chinese efforts to date—searching for seams and gaps in the social and information fabric of other countries.

Our research also suggests that these campaigns remain in their preliminary stages, have so far had relatively marginal effects, and may reflect far less coherent strategy in Moscow and Beijing than is typically assumed. A fourth broad finding is that *there is, as yet, little conclusive evidence about the actual impact of hostile social manipulation to date*. Significant gaps remain in our awareness of what has happened and how effective current social manipulation campaigns have been. Neither those trying to track the issue nor those who have been using these techniques are confident about its degree of effectiveness. The evidence does not so far support the proposition that either country has been able to achieve significant effects in regard to its major objectives—changes in the orientation of regional countries, reduced efforts to counteract their influence, measurable fragmentation of other countries' political or social systems attributable to social manipulation.

Indeed, their efforts appear to have been counterproductive in some ways. There is reason to believe that exaggerated claims of especially Russian effectiveness have actually provided more strategic value to Moscow and Beijing than the direct effects of the manipulation. The United States and its friends and allies would benefit by broadcasting the constraints as well as successes of hostile social manipulation.

A critical distinction emerged in our research between the *outputs* of these campaigns—numbers of posts, tweets, clicks, views, likes, and so on—and their *outcomes* in terms of the actual effect of that activity on attitudes or behavior. There is a tremendous amount of data on outputs and almost no meaningful empirical evidence on outcomes. In fact, according to many metrics, the disinformation campaigns of one of the two actors examined in this study—Russia—have *not* been having significant success. Even in cases where outcomes have matched Russia's objectives, Moscow has not been inventing the grievances that produced a few recent electoral or referendum outcomes—it has only been adding its voice to many others saying largely the same things. It is difficult to separate out the unique effect of each additional voice. One of the main imperatives going forward is for additional research into such questions.

Our research into the evolution of future technologies suggests that this pattern may not persist—it may reflect a temporary reprieve rather than a permanent limit on the effectiveness of what could be termed "virtual societal aggression." Our fifth finding is, therefore, that *despite the apparent limited effects to date, the marriage of the hostile intent of several leading powers and the evolution of several interrelated areas of information technology has the potential to vastly increase the effectiveness and reach of these techniques over time*. Such technologies as targeted marketing, including opt-in programs through which consumers share the most intimate details of their location, thought process, and emotional state; artificial intelligence and related fields such as machine learning; virtual and augmented reality; high-fidelity video and audio capture and impersonation; dynamic content creation and affective computing; the confluence between surveillance technologies, social credit systems, and computational propaganda; and the emergence of an "internet of things" in which data are being gathered from and shared among most things people interact with in daily life are creating the potential for much more sophisticated campaigns of social manipulation. In the meantime, these emerging practices are muddying the relationship of information, awareness, and social and political action, raising some of the most profound questions democracies have ever faced.

This remains a provisional finding, based on evidence about the *potential* effects of these technologies. It is not a conclusive finding that such technologies *will* allow malign actors to achieve dramatically greater effects than has so far been the case. Various responses underway—from social media companies as well as governments and nongovernmental organizations working to counter disinformation—could slow the trend. But there is sufficient evidence to sustain intense efforts to find out more about the possible effects of these technologies and to begin vigilance about how they are evolving. If the risks of such technologies are, in fact, valid, leading democracies may have a limited window of opportunity to develop resilience and active defenses against such measures before they become truly dangerous. Widespread, increasingly influential and damaging campaigns of hostile social manipulation attack the very essence of free societies—the relationship between facts, knowledge, belief, and political behavior. As we have seen, these techniques are not magic wands, and there are significant constraints on efforts to fine-tune the beliefs of any population. But the risks are significant enough to warrant continued close attention and initial policy responses to bound the danger. The second report in this study examines such future risks in detail.

The sixth conclusion of this analysis is that *the United States and other democracies urgently need to support rigorous and in-depth research on the issue to gain a better understanding of many of the dynamics related to social manipulation*. Simply put, too many basic relationships are poorly understood, and more research is called for to better grasp the true level of risk, the most effective types of manipulation, and the most powerful responses. The box lists several promising avenues for inquiry that emerge from our research.

This report catalogs a growing commitment to tools of social manipulation by leading U.S. competitors. As we argue, the threat—at least as it exists today—should not be blown out of proportion. So far, most of these campaigns appear to have had limited effects in terms of concrete geopolitical outcomes that either Russia or China is seeking. But there is abundant evidence that both see information competition as an integral part, perhaps the leading part, of an unending, intensive competition. Both are investing significant resources in building

Proposed Research Topics

- Ways and situations in which incoming information on social/political subjects has the most and least resonance and persuasiveness; relationship between baseline social, political, and economic trends and informational variables
- Role of "influencers" or social hubs in personal networks in shaping persuasiveness of information
- Factors affecting appetite for accuracy in information consumption
- Factors that reduce the appeal of misleading or falsified but sensational or ideologically enticing information
- Differences between changing character of the infosphere itself and outside activity in shaping perceptions
- True role of information silos in constraining information intake; effective mechanisms to broaden silos
- Relative effect of various sources of incoming information on beliefs and behavior: advertisements, news stories, opinions of friends in network, and other

extensive capabilities in this realm and have begun to acquire extensive experience in their employment. If combined with emerging technologies that significantly enhance the impact of such campaigns—a possibility we assess in the next report—the results could pose one of the most significant dangers in history to open democracies. The findings in this report alone are sufficient to suggest that the U.S. government should take a number of immediate steps, including developing a more formal and concrete framework for understanding the issue and funding additional research to understand the scope of the challenge.

Bibliography

"独家：用中国社交网 在美华裔组建特朗普支持团," Sina, May 11, 2016. As of May 6, 2019:
http://news.sina.com.cn/w/zg/2016-05-11/doc-ifxryhhh1925752.shtml

"About the Programme," Interreg Baltic Sea Region, fact sheet, Rostock, Germany, undated. As of May 10, 2019:
http://www.interreg-baltic.eu/about-the-programme.html

Abramowitz, Michael J., "Stop the Manipulation of Democracy Online," *New York Times*, December 11, 2017. As of April 19, 2019:
https://www.nytimes.com/2017/12/11/opinion/fake-news-russia-kenya.html

Adamsky, Dimitry, "Cross-Domain Coercion: The Current Russian Art of Strategy," Proliferation Papers No. 54, Security Studies Center, Institut Francais des Relations Internationales, November 2015.

Adekoya, Remi. "Why Poland's Law and Justice Party Remains So Popular," *Foreign Affairs*, November 3, 2017.

Ai Weiwei, "China's Paid Trolls: Meet the 50-Cent Party," *New Statesman*, October 17, 2012. As of April 29, 2019:
https://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party

Albright, Jonathan, "Trolls on Twitter: How Mainstream and Local News Outlets Were Used to Drive a Polarized News Agenda," Berkman Klein Center for Internet and Society at Harvard University, February 15, 2018. As of April 17, 2019:
https://medium.com/berkman-klein-center/trolls-on-twitter-how-mainstream-and-local-news-outlets-were-used-to-drive-a-polarized-news-agenda-e8b514e4a37a

Allcott, Hunt, and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives*, Vol. 31, No. 2, Spring 2017. As of April 17, 2019:
http://web.stanford.edu/~gentzkow/research/fakenews.pdf

Allenby, Braden R., "The Age of Weaponized Narrative," *Issues in Science and Technology*, Summer 2017.

Allen-Ebrahimian, Bethany, "Did China Just Ban Maroon 5?" *Foreign Policy*, July 16, 2015.

———, "Chinese Police Are Demanding Personal Information from Uighurs in France," *Foreign Policy*, March 2, 2018a. As of April 30, 2019: http://foreignpolicy.com/2018/03/02/chinese-police-are-secretly-demanding-personal-information-from-french-citizens-uighurs-xinjiang/

———, "China's Long Arm Reaches into American Campuses," *Foreign Policy*, March 7, 2018b. As of May 5, 2019: http://foreignpolicy.com/2018/03/07/chinas-long-arm-reaches-into-american-campuses-chinese-students-scholars-association-university-communist-party/

Alliance for Securing Democracy, *Securing Democracy Dispatch*, December 18, 2017.

America's Continued Commitment to European Security: Operation Atlantic Resolve, U.S. Department of Defense Special Reports, undated. As of May 7, 2019: https://dod.defense.gov/News/Special-Reports/0218_Atlantic-Resolve

Anbin, Shi, and Peiyan Wang, "Stealth Propaganda: Concepts Evolution, Strategy" ["隐性宣传：概念·演进·策略"], *International Communications*, January 2016.

Anderlini, Jamil, and Jamie Smyth, "West Grows Wary of China's Influence Game," *Financial Times*, December 19, 2017. As of April 29, 2019: https://www.ft.com/content/d3ac306a-e188-11e7-8f9f-de1c2175f5ce

"An Ex St. Petersburg 'Troll' Speaks Out: Russian Independent TV Network Interviews Former Troll at the Internet Research Agency," *Meduza*, October 15, 2017. As of April 17, 2019: https://meduza.io/en/feature/2017/10/15/an-ex-st-petersburg-troll-speaks-out

"An Examination of International Public Opinion on One Belt One Road" ["一带一路"议题的国际舆情分析"], *International Communications*, May 2017.

"Anonymous Ukraine Klitschko E-mails and Nuland/Pyatt Dialogue Prove US-Backed Coup," Sputnik (then Voice of Russia), February 25, 2014.

Arabie, P., and Y. Wind, "Marketing and Social Networks," in *Advances in Social Networks Analysis*, S. Wasserman and J. Galackiewicz, eds., London: Sage Publications, 1994, pp. 254–273.

"Are HIV/AIDS Conspiracy Beliefs a Barrier to HIV Prevention Among African Americans?" *Journal of Acquired Immune Deficiency Syndromes*, Vol. 38, No. 2, February 1, 2005, pp. 213–218.

Arquilla, John, and David Ronfeldt, "A New Epoch—and Spectrum—of Conflict," in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND Corporation, MR-880-OSD/RC, 1997. As of April 19, 2019: https://www.rand.org/pubs/monograph_reports/MR880.html

———, *The Emergence of Noopolitik: Toward an American Information Strategy*, Santa Monica, Calif.: RAND Corporation, MR-1033-OSD, 1999. As of April 19, 2019: https://www.rand.org/pubs/monograph_reports/MR1033.html

Auchard, Eric, and Joseph Menn, "Facebook Cracks Down on 30,000 Fake Accounts in France," Reuters, April 13, 2017. As of May 9, 2019: https://www.reuters.com/article/us-france-security-facebook/facebook-cracks-down-on-30000-fake-accounts-in-france-idUSKBN17F25G

"Authorities Deny Rumor of Ban on Incense, Ghost Money Burning," *Central News Agency* (Taiwan), July 21, 2017.

Baldwin, Clare, and Kristina Cooke, "How Sony Sanitized the New Adam Sandler Movie to Please Chinese Censors," Reuters, July 24, 2015. As of April 29, 2019: https://www.reuters.com/investigates/special-report/china-film/

Bao Yu, "The Political Network Marketing Strategies of Islamic State Towards Western Countries," *Journal of Jiangnan Social University*, June 2016, pp. 17–21.

Baraniuk, Chris, "Beware the Brexit Bots: The Twitter Spam out to Swing Your Vote," *New Scientist*, June 22, 2016. As of May 8, 2019: https://www.newscientist.com/article/2094629-beware-the-brexit-bots-the-twitter-spam-out-to-swing-your-vote/

Barbash, Fred, "U.S. Ties 'Klan' Olympic Hate Mail to KGB," *Washington Post*, August 7, 1984. As of August 19, 2019: https://www.washingtonpost.com/archive/politics/1984/08/07/us-ties-klan-olympic-hate-mail-to-kgb/80918fe8-fcf0-46cf-bb58-726ee46d8ce9/?utm_term=.df5d65145eb9

Baym, Nancy K., "Data Not Seen: The Uses and Shortcomings of Social Media Metrics," *First Monday*, Vol. 18, No. 10, October 7, 2013

Beauchamp-Mustafaga, Nathan, and Michael Chase, *The Chinese Military and Social Media: A New Tool for Peacetime and Wartime Propaganda at Home and Abroad*, Washington, D.C.: John Hopkins SAIS, forthcoming.

Beauchamp-Mustafaga, Nathan, Cristina Garafola, Astrid Cevallos, and Arthur Chan, "China Signals Resolve with Bomber Flights over the South China Sea," *War on the Rocks*, August 2, 2016. As of April 29, 2019: https://warontherocks.com/2016/08/china-signals-resolve-with-bomber-flights-over-the-south-china-sea/

Beauchamp-Mustafaga, Nathan, Derek Grossman, and Logan Ma, "Chinese Bomber Flights Around Taiwan: For What Purpose?" *War on the Rocks*, September 13, 2017. As of April 29, 2019: https://warontherocks.com/2017/09/chinese-bomber-flights-around-taiwan-for-what-purpose/

Bechev, Dimitar, *Russia's Influence in Bulgaria*, Brussels: New Direction: The Foundation for European Reform, May 12, 2015. As of April 24, 2019: http://europeanreform.org/files/ND-report-RussiasInfluenceInBulgaria-preview-lo-res_FV.pdf

Beech, Hannah, "Communist Chinese Rap 'This Is China' Attacks Western Media," *Time*, June 20, 2016.

Beesley, Arthur, "EU Sets Timetable for Tighter Military Coordination," *Financial Times*, June 22, 2017. As of May 8, 2019: https://www.ft.com/content/1c8aaeec-5782-11e7-80b6-9bfa4c1f83d2

Beijing Municipal Committee United Front Department, "The Historical Status and Practical Role of the United Front" ["统一战线的历史地位和现实作用"], *China United Front*, October 2012.

Bender, Jeremy, "Estonian President: Europe's Security Architecture 'Has Collapsed,'" *Business Insider*, September 19, 2014. As of May 10, 2019: www.businessinsider.com/europes-security-architecture-has-collapsed-2014-9?IR=T

Benner, Thorsten, Jan Gaspers, Mareike Ohlberg, Lucrezia Poggetti, and Kristin Shi-Kupfer, "Authoritarian Advance: Responding to China's Growing Political Influence in Europe," Global Public Policy Institute and Mercator Institute for China Studies, February 2018. As of April 28, 2019: https://www.merics.org/sites/default/files/2018-02/GPPi_MERICS_Authoritarian_Advance_2018_1.pdf

Berkowitz, Bruce D., "Warfare in the Information Age," in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND Corporation, MR-880-OSD/RC, 1997. As of April 19, 2019: https://www.rand.org/pubs/monograph_reports/MR880.html

Berman, Richard, "China's Rising Threat to Hollywood," *Politico*, October 4, 2016. As of April 29, 2019: https://www.politico.com/agenda/story/2016/10/china-hollywood-movies-threat-000216

Bernays, Edward, *Propaganda*, New York: IG Publishing, 2005, originally published 1928.

———, *Crystallizing Public Opinion*, New York: IG Publishing, Reprint Edition 2011.

Bernstein, Richard, "The Brands That Kowtow to China," *New York Review of Books*, March 2, 2018. As of May 5, 2019:
http://www.nybooks.com/daily/2018/03/02/the-brands-that-kowtow-to-china/

Besemeres, John, *A Difficult Neighbourhood: Essays on Russia and East-Central Europe Since World War II*, Canberra: Australian National University Press, 2016.

Bi Lifu, "Innovating Foreign Propaganda in Ports and Improving Inner Mongolia's Image," *Theory Construction*, 2009.

Bialik, Kristen, "Putin Remains Overwhelmingly Unfavorable in the United States," Pew Research Center, March 26, 2018. As of October 12, 2018:
http://www.pewresearch.org/fact-tank/2018/03/26/
putin-remains-overwhelmingly-unpopular-in-the-united-states/

Biden, Joe, and Michael Carpenter, "How to Stand Up to the Kremlin," *Foreign Affairs*, December 2017.

Bittman, Ladislav, *The KGB and Soviet Disinformation: An Insider's View*, Washington, D.C.: Pergamon-Brassey's, 1985.

Blackwill, Robert, and Kurt Campbell, *Xi Jinping on the Global Stage: Chinese Foreign Policy Under a Powerful but Exposed Leader*, Council Special Report No. 74, New York: Council on Foreign Relations, February 25, 2016.

Blackwill, Robert D., and Philip H. Gordon, "Containing Russia, Again," *Foreign Affairs*, January 18, 2018. As of May 7, 2019:
https://www.foreignaffairs.com/articles/russian-federation/2018-01-18/
containing-russia-again

Bland, Ben, "China Censorship Drive Splits Leading Academic Publishers," *Financial Times*, November 4, 2017.

"BM Not My President Rally," Twitter post, U.S. House of Representatives Permanent Select Committee on Intelligence, 2017. As of April 19, 2019:
https://democrats-intelligence.house.gov/uploadedfiles/6056284937087.pdf

Bodner, Matthew, Matthew Kupfer, and Bradley Jardine, "Welcome to the Machine: Inside the Secretive World of RT," *Moscow Times*, June 1, 2017. As of April 24, 2019:
https://www.themoscowtimes.com/2017/06/01/
welcome-to-the-machine-inside-the-secretive-world-of-rt-a58132

Boghardt, Thomas, "Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence*, Vol. 53, No. 4, December 2009. As of April 19, 2019:
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/
csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20
USA-17Dec.pdf

Bolsover, Gillian, "Computational Propaganda in China: An Alternative Model of a Widespread Practice," Computational Propaganda Research Project, University of Oxford, Oxford, UK, April 2017. As of April 30, 2019: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-China.pdf

Botsman, Rachel, "Big Data Meets Big Brother As China Moves to Rate Its Citizens," *Wired*, October 21, 2017. As of May 5, 2019: http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Boxell, Levi, Matthew Gentzkow, and Jesse M. Shapiro, "Is Media Driving Americans Apart?" *New York Times*, December 6, 2017.

Bradshaw, Samantha, and Philip N. Howard, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation," Working Paper No. 2017.12, Oxford, UK: Project on Computational Propaganda, 2017.

Brady, Anne-Marie, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China*, Lanham, Md.: Rowman and Littlefield Publishers, 2008.

———, ed., *China's Thought Management*, New York: Routledge, 2012.

———, "China's Foreign Propaganda Machine," *Journal of Democracy*, Vol. 26, No. 4, October 2015. As of May 6, 2019: https://muse.jhu.edu/article/595922

———, *Magic Weapons: China's Political Influence Activities Under Xi Jinping*, Washington, D.C.: Wilson Center, 2017.

Breland, Ali, "Thousands Attended Rally Organized by Russia on Facebook," *The Hill*, October 31, 2017.

"British Troops Land in Estonia for Nato Mission to Deter Russia," *The Guardian*, March 18, 2017. As of May 8, 2019: https://www.theguardian.com/uk-news/2017/mar/18/british-troops-land-in-estonia-for-nato-mission-to-deter-russia

Britt, Lawrence, (pseudonym for Ladislav Bittman), testimony before U.S. Senate Subcommittee on Internal Security, Washington, D.C., May 5, 1971, as referenced in Max Holland, "The Propagation and Power of Communist Security Services Dezinformatsiya," *International Journal of Intelligence and Counterintelligence*, Vol. 19, No. 1, 2006, p. 24.

Broderick, Ryan, "Trump Supporters Online Are Pretending to Be French to Manipulate France's Election," Buzzfeed News, January 24, 2017. As of May 8, 2019: https://www.buzzfeed.com/ryanhatesthis/inside-the-private-chat-rooms-trump-supporters-are-using-to?utm_term=.yqWz6gPnR#.nl1OWVZ83

Bruter, Michael, and Sarah Harrison, *The Impact of Brexit on Consumer Behavior*, Lansons, London School of Economics, and Opinium, June 9, 2016.

Buckley, Chris, "China Takes Aim at Western Ideas," *New York Times*, August 19, 2013. As of April 28, 2019:
http://www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hard-line-in-secret-memo.html

Buckley, Chris, and Jane Perlez, "By Buying Hong Kong Paper, Alibaba Seeks to Polish China's Image," *New York Times*, December 13, 2015. As of May 6, 2019:
https://www.nytimes.com/2015/12/14/world/asia/alibaba-south-china-morning-post-hong-kong.html

Bumiller, Elizabeth, and Michael Wines, "Test of Stealth Fighter Clouds Gates Visit to China," *New York Times*, January 11, 2011.

Burgess, Matt, "Here's the First Evidence Russia Used Twitter to Influence Brexit," *Wired*, November 10, 2017.

Bytwerk, Randall L., "Believing in 'Inner Truth': The *Protocols of the Elders of Zion* in Nazi Propaganda, 1933–1945," *Holocaust and Genocide Studies*, Vol. 29, No. 2, 2015.

Cadell, Cate, "China Investigates Top Local Social Media Sites in Push to Control Content," Reuters, August 10, 2017. As of April 29, 2019:
https://www.reuters.com/article/us-china-cyber/china-investigates-top-local-social-media-sites-in-push-to-control-content-idUSKBN1AR07K

Cai Huifu, Wang Lin, Sheng Peilin, Yu Qi, Liu Xuemei, and Zheng Yu, "Research into News and Public Opinion Warfare During the Iraq War," *China Military Science*, August 2003, pp. 28–34.

Cai Yintong, "Study Abroad Students: An Important Force for People-to-People External Propaganda" ["留学生: 民间外宣的重要力量"], *International Communications*, March 2009.

Capon, Felicity, "Chinese Propaganda Cartoon Promotes Five Year Plan," *Newsweek*, October 27, 2015. As of April 30, 2019:
http://www.newsweek.com/chinachinese-propaganda-videochina039s-five-year-plancommunist-598015

Central Intelligence Agency, *Political Information: The Role of TASS in Soviet Propaganda Activities, Shanghai*, Information Report, December 13, 1948. As of April 17, 2019:
https://www.cia.gov/library/readingroom/docs/CIA-RDP82-00457R002100650004-7.pdf

———, translation of: S. Simoni, "Soviet Anti-Semitism and the Prague Trial," Yedioth Hayom, 1952. As of April 17, 2019:
https://www.cia.gov/library/readingroom/docs/CIA-RDP65-00756R000500130006-7.pdf

———, "Tass: Its Role, Structure, and Operations," June 1959.

——— "Soviet Broadcasts to Middle East–South Asian Countries," February 4, 1980. As of April 17, 2019:
https://www.cia.gov/library/readingroom/docs/CIA-RDP84-00868R000100060056-8.pdf

———, "The Soviet Foreign Propaganda Apparatus: A Research Paper," 1986a. As of April 17, 2019:
https://www.cia.gov/library/readingroom/docs/CIA-RDP88G01116R000800900003-2.pdf

———, "Moscow Drops Clandestine Radio, Sustains Criticism of Tehran," *FBIS Trends* newsletter, December 10, 1986b. As of April 17, 2019:
https://www.cia.gov/library/readingroom/docs/CIA-RDP09-00997R000100350002-9.pdf

Chapple, Amos, "War of Words over Ukraine 'Combat' Photo," Radio Free Europe Radio Liberty, August 25, 2016. As of April 24, 2019:
https://www.rferl.org/a/ukraine-war-photographer-real-or-fake-controversy-muravskiy/27946182.html

Charlton, Angela, and Matthew Bodner, "Russian Meddling Abroad: Does Putin Pull All the Strings?" Associated Press, September 15, 2018.

"Chast' Pervaja. Zoloto Trollej," Anonymous International, May 26, 2014.

Chen, Adrian, "The Agency," *New York Times Magazine*, June 2, 2015. As of April 17, 2019:
https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Chen Hui-hui, "Commentary Analysis on 'Artificial Intelligence Technology Manipulating The US Election' Research Report," *Information Security and Communications Privacy*, July 2017.

Chen Jie, "Build a Military Foreign Propaganda Shock Brigade" ["打造军事外宣队的突击队"], *Military Correspondent*, June 2015, pp. 53–54.

Chen Lin, "Effectively Strengthen Internet Propaganda and Management Work to Create Sound Internet Public Opinion and Cultural Environment for Society," *Tibet Daily*, May 26, 2012.

Chen Zheng, "Analysis of Information on Social Media for German Audience" ["德国受众社交媒体获取信息情况分析"], *International Communications*, August 2013.

Chen Zhengzhong, "Preliminary Thoughts About Strengthening Cyber News Media in Wartime," *Military Correspondent*, July 2014.

Cheng, Dean, "Chinese Lessons from the Gulf Wars," in Andrew Scobell, David Lai, and Roy Kamphausen, eds., *Chinese Lessons from Other Peoples' Wars*, Carlisle, Pa.: Strategic Studies Institute, 2011.

———, "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response," Heritage Foundation, Backgrounder No. 2745, November 21, 2012.

———, "Winning Without Fighting: The Chinese Psychological Warfare Challenge," Heritage Foundation, Backgrounder No. 2821, July 11, 2013.

Chessen, Matt, "Understanding the Psychology Behind Computational Propaganda," in Shawn Powers and Markos Kounalakis, eds., *Can Public Diplomacy Survive the Internet?: Bots, Echo Chambers, and Disinformation,* Advisory Commission on Public Diplomacy, May 2017.

Chin, Josh, and Gillian Wong, "China's New Tool for Social Control: A Credit Rating for Everything," *Wall Street Journal*, November 28, 2016. As of May 5, 2019:
https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590

"China Invents the Digital Totalitarian State," *The Economist*, December 17, 2016. As of May 5, 2019:
https://www.economist.com/news/briefing/21711902-worrying-implications-its-social-credit-project-china-invents-digital-totalitarian

"China Is Spending Billions to Make the World Love It," *The Economist*, March 23, 2017.

"China's Biggest Search Engine Baidu Looks Into 3 Billion Fake News Claims a Year," Bloomberg, October 10, 2017.

"China's Five-Year Plan Now Has Its Own Psychedelic Music Video," *Wall Street Journal*, October 27, 2015.

"China's New Cultural Revolution," *Wall Street Journal*, January 4, 2012. As of April 28, 2019:
https://www.wsj.com/articles/SB10001424052970203550304577138270191788832

"China's Operation Australia," *Sydney Morning Herald*, 2017. As of April 28, 2019:
http://www.smh.com.au/interactive/2017/chinas-operation-australia/

"China's Propaganda Department Not Good Enough at Propaganda—Gov't," *Hong Kong Free Press*, June 9, 2016.

Chinese Academy of Military Science Military Strategy Department, ed., *Science of Military Strategy* [战略学], 3rd edition, Beijing: Academy of Military Science Press, 2013.

"Chinese-Americans Are Becoming Politically Active," *The Economist*, January 19, 2017. As of May 6, 2019:
https://www.economist.com/news/united-states/21715066-long-slumbering-voter-block-awakes-chinese-americans-are-becoming-politically-active

"Chinese Embassy in US Now on Facebook," *China Daily*, February 13, 2018. As of May 6, 2019:
http://usa.chinadaily.com.cn/a/201802/13/WS5a82001da3106e7dcc13c618.html

Choi Chi-yuk, "Voice of America Fires Three Staff over Explosive Guo Wengui Interview," *South China Morning Post*, November 15, 2017.

Chong, Zoey, "Up to 48 Million Twitter Accounts Are Bots, Study Says," CNET, March 14, 2017.

Chung, Jae Ho, "China's Evolving Views of the Korean-American Alliance, 1953–2012," *Journal of Contemporary China*, Vol. 23, No. 87, 2014, pp. 425–442.

CIA—*See* Central Intelligence Agency.

"CIA Study: Soviet Covert Action and Propaganda," in U.S. House of Representatives, Permanent Select Committee on Intelligence, Subcommittee on Oversight, *Soviet Covert Action (The Forgery Offensive)*, Washington, D.C.: U.S. Government Printing Office, 1980.

Cialdini, Robert B., *Pre-Suasion: A Revolutionary Way to Influence and Persuade*, New York: Simon and Schuster, 2016.

Cieply, Michael, "Deal Expands Chinese Influence on Hollywood," *New York Times*, May 20, 2012.

"Closer Cooperation with Latvia," Mission of Norway to the European Union, December 14, 2017. As of May 10, 2019:
https://www.norway.no/en/missions/eu/about-the-mission/news-events-statements/news2/closer-cooperation-with-latvia/

Cloud, David S., "Facebook Tells Congress That 126 Million Americans May Have Seen Russia-Linked Ads," *Los Angeles Times*, October 31, 2017.

Cobb, Michael D., Brendan Nyhan, and Jason Reifler, "Beliefs Don't Always Persevere: How Political Figures Are Punished When Positive Information About Them Is Discredited," *Political Psychology*, December 28, 2012.

Coca, Nithin, "The High-Tech War on Tibetan Communication," *Engadget*, June 27, 2015. As of May 5, 2019:
https://www.engadget.com/2017/06/27/the-high-tech-war-on-tibetan-communication/

Cole, J. Michael, "China Intensifies Disinformation Campaign Against Taiwan," *Taiwan Sentinel*, January 19, 2017a.

———, "Will China's Disinformation War Destabilize Taiwan?" *National Interest*, July 30, 2017b.

Coleman, E. Gabriella, "Phreaks, Hackers, and Trolls: The Politics of Transgression and Spectacle," in Michael Mandiberg, ed., *The Social Media Reader*, New York: New York University Press, 2012.

Collins, Ben, Andrew Desiderio, Spencer Ackerman, Gideon Resnick and Joseph Cox, "House Drops Motherlode of Russian Propaganda," *Daily Beast,* November 1, 2017.

Committee to Investigate Russia, "Morgan Freeman Warns Russia Is Waging War on the U.S.," September 18, 2017.

Confessore, Nicholas, Gabriel J. X. Dance, Richard Harris, and Mark Hansen, "The Follower Factory," *New York Times*, January 27, 2018. As of May 6, 2019: https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html

Congressional Record, "Soviet Active Measures in the United States: An Updated Report by the FBI," December 9, 1987.

Cook, John, Ullrich Ecker, and Stephan Lewandowsky, "Misinformation and How to Correct It," in Robert Scott and Stephan Kosslyn, eds., *Emerging Trends in the Social and Behavioral Sciences*, New York: John Wiley and Sons, 2015.

Cook, Sarah, "Resisting Beijing's Global Media Influence," *The Diplomat*, December 10, 2015.

———, "Chinese Government Influence on the U.S. Media Landscape," testimony before the U.S–China Economic and Security Review Commission, May 4, 2017a.

———, "China's Party Congress Hints at Media Strategy for a 'New Era,'" *The Diplomat*, November 4, 2017b.

Cooke, Kristina, "China News Agency Leases Plum Times Square Ad Space," Reuters, July 26, 2011. As of May 6, 2019: https://www.reuters.com/article/industry-us-media-xinhua-timessquare/china-news-agency-leases-plum-times-square-ad-space-idUSTRE76P71T20110726

"Could This Be the Digital Ad Industry's Magic Bullet? Connecting Online Ads to Offline Sales," *VentureBeat*, March 16, 2015. As of October 24, 2017: https://venturebeat.com/2015/03/16/could-this-be-the-digital-ad-industrys-magic-bullet-connecting-online-ads-to-offline-sales/

Crain, M., "The Limits of Transparency: Data Brokers and Commodification," *New Media & Society*, Vol. 20, No. 1, 2016.

"Crimean 'Nazi' Billboard Highlights Propaganda Problem: U.S.," CBS News, March 10, 2014.

Crossley, Lucy, "The 'Aggrieved Housewife', the Soldier's Mother' and the 'Kiev Resident': Did Russian Television 'Use Actress to Portray FIVE Different Women' As It Reported Normal Ukrainians Backed Kremlin," *Daily Mail*, March 5, 2014. As of April 24, 2019: http://www.dailymail.co.uk/news/article-2574131/How-Russian-television-used-actress-pretend-five-different-people-opposed-revolution-reported-normal-Ukrainians-backed-Kremlin.html

Davies, Jessica, "*Le Monde* Identifies 600 Unreliable Websites in Fake-News Crackdown," *Digiday*, January 25, 2017. As of May 9, 2019: https://digiday.com/uk/le-monde-identifies-600-unreliable-websites-fake-news-crackdown/

Dean, L. G., G. L. Vale, K. N. Laland, E. Flynn, and R. L. Kendal, "Human Cumulative Culture: A Comparative Perspective," *Biological Reviews*, Vol. 89, No. 2, 2014, pp. 284–301.

"Deepening of Defence Cooperation in the EU Strengthens Europe's Security," press release, Foreign Affairs Council, November 13, 2017. As of May 10, 2019: https://www.eu2017.ee/news/press-releases/deepening-defence-cooperation-eu-strengthens-europes-security

"Defence Budget Increases for the First Time in Six Years," press release, United Kingdom Ministry of Defence, April 1, 2016. As of May 8, 2019: https://www.gov.uk/government/news/defence-budget-increases-for-the-first-time-in-six-years

"Defence Secretary Steps up UK Commitments to NATO," press release, United Kingdom Ministry of Defence, June 29, 2017. As of May 8, 2019: https://www.gov.uk/government/news/defence-secretary-steps-up-uk-commitments-to-nato

De Pinto, Jennifer, Fred Backus, Kabir Khanna, and Anthony Salvanto, "Republicans Blame Bill, Not Trump, for Health Care," CBS News, March 29, 2017. As of May 7, 2019: https://www.cbsnews.com/news/republicans-health-care-trump-approval-russia-election-meddling-cbs-news-poll/?ftag=CNM-00-10aab7e&linkId=35962703

Desigaud, Clementine, Philip N. Howard, Samantha Bradshaw, Bence Kollanyi, and Gillian Bolsolver, "Junk News and Bots During the French Presidential Election: What Are French Voters Sharing over Twitter in Round Two?" Data Memo 2017.4, Oxford, UK: Project on Computational Propaganda, Oxford Internet Institute, University of Oxford, May 4, 2017.

DFR Lab, "#FakeNews: Made in China," *Medium*, November 25, 2017.

Diaz, Itxu, "Venezuela and Russia Teamed Up to Push Pro-Catalan Fake News," *Daily Beast*, November 28, 2017.

Digital Forensics Research Lab, "Putin's Online Cheerleaders: The 'Patriots' Behind Pro-Kremlin, Anti–Morgan Freeman Memes," The Atlantic Council, October 17, 2017.

———, "Russia's Full Spectrum Propaganda: A Case Study in How Russia's Propaganda Machine Works," The Atlantic Council, January 23, 2018.

Ding Chunguang and Ma Gensheng, "Effectively Controlling Lively Spokesmen—on the Control of the Dissemination of Major Military News," *Military Correspondent*, April 2011.

"Document 9: A ChinaFile Translation," ChinaFile, November 8, 2013. As of April 28, 2019:
http://www.chinafile.com/document-9-chinafile-translation

Doland, Angela, "Watch the Chinese Propaganda Ad Playing 120 Times a Day in Times Square," *AdAge*, July 27, 2016. As of May 6, 2019:
http://adage.com/article/global-news/a-mind-numbing-chinese-propaganda-ad-playing-times-square-120-times-a-day/305198/

Dotson, John, "The United Front Work Department in Action Abroad: A Profile of the Council for the Promotion of the Peaceful Reunification of China," *China Brief*, February 13, 2018. As of April 29, 2019:
https://jamestown.org/program/united-front-work-department-action-abroad-profile-council-promotion-peaceful-reunification-china/

Dou, Eva, "Jailed for a Text: China's Censors Are Spying on Mobile Chat Group," *Wall Street Journal*, December 8, 2017.

Dougherty, Jill, "Everyone Lies: The Ukraine Conflict and Russia's Media Transformation," Discussion Paper Series, Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School, July 2014.

Dougherty, Jill, and Riina Kalijurand, "Estonia's 'Virtual Russian World': The Influence of Russian Media on Estonia's Russian Speakers," International Centre for Defense and Security, Estonia, October 2015.

Dredge, Stuart, "More Than One-Fifth of Britons Will Use Twitter This Year, Claims Report," *The Guardian*, February 20, 2014. As of May 8, 2019:
https://www.theguardian.com/technology/2014/feb/20/twitter-uk-active-users-2014

Dreyer, June Teufel, "A Weapon Without War: China's United Front Strategy," Foreign Policy Research Institute, February 6, 2018. As of April 29, 2019:
https://www.fpri.org/article/2018/02/weapon-without-war-chinas-united-front-strategy/

Druckman, James, "On the Limits of Framing Effects: Who Can Frame?" *Journal of Politics*, Vol. 63, No. 4, 2001.

Duhigg, Charles, "How Companies Learn Your Secrets," *New York Times*, February 16, 2012.

Durham, W. H., *Coevolution: Genes, Culture, and Human Diversity*, Palo Alto, Calif.: Stanford University Press, 1991.

Eagly, Alice H., and Shelly Chaiken, "An Attribution Analysis of Communicator Characteristics on Opinion Change: The Case of Communicator Attractiveness," *Journal of Personality and Social Psychology*, Vol. 32, No. 1, 1975, pp. 136–144.

———, "Attitude Structure and Function," in D. T. Gilbert, S. T. Fiske, and G. Lindzey, eds., *The Handbook of Social Psychology* (4th ed.), New York: Oxford University Press, 1998, pp. 269–322.

EC—*See* European Commission.

Edwards, George C. III, *On Deaf Ears: The Limits of the Bully Pulpit*, New Haven, Conn.: Yale University Press, 2003.

Edwards, Kari, and Edward E. Smith, "A Disconfirmation Bias in the Evaluation of Arguments," *Journal of Personality and Social Psychology*, Vol. 71, No. 1, 1996, pp. 5–24.

Elder, Miriam, "Polishing Putin: Hacked Emails Suggest Dirty Tricks by Russian Youth Groups," *The Guardian*, February 7, 2012. As of April 24, 2019: https://www.theguardian.com/world/2012/feb/07/putin-hacked-emails-russian-nashi

Ellul, Jacques, *Propaganda*, New York: Vintage Books, 1965.

Enge, E., "Influencer Marketing—What It Is and Why You Need to Be Doing It," blog post, *Moz Blog*, March 6, 2012. As of October 24, 2017: https://moz.com/blog/influencer-marketing-what-it-is-and-why-you-need-to-be-doing-it

Erlanger, Steven, "What is RT?" *New York Times,* March 8, 2017.

"Estonia and NATO," Republic of Estonia Ministry of Foreign Affairs, July 3, 2017. As of May 10, 2019: http://vm.ee/en/estonia-and-nato

"EU Referendum Results," BBC News, 2016. As of May 8, 2019: http://www.bbc.com/news/politics/eu_referendum/results

European Commission, "Special Eurobarometer 461: Designing Europe's Future," April 2017.

Evans, W. D., J. Uhrig, K. Davis, and L. McCormack, "Efficacy Methods to Evaluate Health Communication and Marketing Campaigns," *Journal of Health Communication*, Vol. 14, No. 4, 2009, pp. 315–330.

"Eyes Wide Shut: Strengthening of Russian Soft Power in Serbia: Goals, Instruments, and Effects," Center for Euro-Atlantic Studies, May 2016. As of April 24, 2019: https://www.ceas-serbia.org/images/publikacije/CEAS_Studija_-_%C5%A0irom_zatvorenih_o%C4%8Diju__ENG.pdf

"Exhibit B," U.S. House of Representatives Permanent Select Committee on Intelligence, 2017. As of April 23, 2019: https://democrats-intelligence.house.gov/uploadedfiles/exhibit_b.pdf

"Face the Nation," CBS, February 4, 2018. As of April 29, 2019: https://www.cbsnews.com/news/face-the-nation-february-4-2018-transcript/

"Fake Swedish Letter in Russian Media," blog post, *StopFake*, September 15, 2015. As of April 24, 2019: https://www.stopfake.org/en/fake-swedish-letter-in-russian-media/

"Fake 'Swedish' Letter Spread in Russian Media," Radio Sweden, September 13, 2015. As of April 24, 2019:
http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6254260

Fan, Jiayang, "How China Wants to Rate Its Citizens," *New Yorker*, November 3, 2015. As of May 5, 2019:
https://www.newyorker.com/news/daily-comment/how-china-wants-to-rate-its-citizens

Faris, Robert M., Hal Roberts, Bruce Etling, Nikki Bourassa, Ethan Zuckerman, and Yochai Benkler, "Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election," research paper, Berkman Klein Center for Internet and Society, Harvard University, August 2017. As of May 8, 2019:
https://dash.harvard.edu/bitstream/handle/1/33759251/2017-08_electionReport_0.pdf?sequence=9

Farrell, Henry, "American Democracy Is an Easy Target," *Foreign Policy*, January 17, 2018. As of May 8, 2019:
http://foreignpolicy.com/2018/01/17/american-democracy-was-asking-for-it/

Farrely, M. C., K. C. Davis, M. L. Haviland, P. Messeri, and C. G. Healton, "Evidence of a Dose-Response Relationship Between 'Truth' Antismoking Ads and Youth Smoking Prevalence," *American Journal of Public Health*, Vol. 95, 2005, pp. 425–431.

Faughnder, Ryan, "China-Owned AMC Seals Deal to Buy Carmike Cinemas, Making It the Largest Theater Chain in U.S.," *Los Angeles Times*, November 15, 2016.

Fazio, Lisa K., Nadia M. Brasier, B. Keith Payne, and Elizabeth J. Marsh, "Knowledge Does Not Protect Against Illusory Truth," *Journal of Experimental Psychology*, Vol. 144, No. 5, 2015, pp. 993–1002.

Fazio, Russell H., and Richard E. Petty, eds., *Attitudes: Their Structure, Function, and Consequences*, New York: Psychology Press/Taylor & Francis, 2008.

Ferrara, Emilio, "Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election," *First Monday*, Vol. 22, No. 8, August 2017. As of May 8, 2019:
http://firstmonday.org/ojs/index.php/fm/article/view/8005/6516

Flynn, D. J., Brendan Nyhan, and Jason Reifler, "The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics," *Advances in Political Psychology*, Vol. 38, Supplement 1, 2017, pp. 128–129.

Forbidden Feeds: Government Controls on Social Media in China, New York: PEN America, March 13, 2018. As of May 5, 2019:
https://pen.org/wp-content/uploads/2018/06/PEN-America_Forbidden-Feeds-report-6.6.18.pdf

Forsythe, Michael, "He Tweeted About Chinese Government Corruption. Twitter Suspended His Account," *New York Times*, April 26, 2017a.

———, "Billionaire Who Accused Top Chinese Officials of Corruption Asks U.S. for Asylum," *New York Times*, September 7, 2017b.

Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy, Washington, D.C.: Freedom House, 2017.

Frenkel, Sheera, "'Troll Farms' Are Relentless at Sharing on Instagram," *New York Times,* December 18, 2017.

Frenkel, Sheera, and Daisuke Wakabayashi, "After Florida School Shooting, Russian 'Bot' Army Pounced," *New York Times*, February 19, 2018.

Friedlander, Blaine, "Taiwan Elects Its Second Cornell Alumnus As President," *Cornell Chronicle*, January 29, 2016. As of May 5, 2019: http://news.cornell.edu/stories/2016/01/taiwan-elects-its-second-cornell-alumnus-president

Fritz, Ben, and John Horn, "Reel China: Hollywood Tries to Stay on China's Good Side," *Los Angeles Times*, March 16, 2011. As of April 29, 2019: http://articles.latimes.com/2011/mar/16/entertainment/la-et-china-red-dawn-20110316

"'F**k the EU': Snr US State Dept. Official Caught in Alleged Phone Chat on Ukraine," RT, February 6, 2014. As of April 24, 2019: https://www.rt.com/news/nuland-phone-chat-ukraine-927/

"Further Present a Real Tibet to the World—Sixth Discussion on Earnestly Studying and Implementing Spirit of Comrade Li Changchun's Important Speech," *Tibet Daily*, August 5, 2012.

Gal, David, and David Rucker, "When in Doubt, Shout! Paradoxical Influences of Doubt on Proselytizing," *Psychological Science*, Vol. 21, No. 11, 2010, pp. 1701–1707.

Galeotti, Mark, "'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't," in Agnieska Pikulicksa-Wilczewska and Richard Sakwa, eds., *Ukraine and Russia: People, Politics, Propaganda, and Perspectives,* Bristol, UK: E-International Relations Publishing, 2015.

Gallup, "Russia," survey results, undated. As of January 31, 2018: http://news.gallup.com/poll/1642/russia.aspx

———, "Confidence in Institutions," survey results, 2017. As of May 7, 2019: http://news.gallup.com/poll/1597/confidence-institutions.aspx

Gao, Mengzi, "Chinese Trump Supporters Thank WeChat," *Voices of New York*, November 11, 2016. As of May 6, 2019: https://voicesofny.org/2016/11/chinese-trump-supporters-thank-wechat/

Gao Han, "Russia Today: Russia's External Propaganda Aircraft Carrier" ["今日俄罗斯": 俄罗斯的"外宣航母"], *Modern Audiovisual*, May 2016. As of April 29, 2019:
http://www.globalview.cn/html/global/info_10863.html

Garcia, D., "Social Media Mavens Wield 'Influence,' and Rake in Big Dollars," CNBC Tech, August 12, 2017. As of August 24, 2017:
https://www.cnbc.com/2017/08/11/social-media-influencers-rake-in-cash-become-a-billion-dollar-market.html

Garmazhapova, Aleksandra, "Gde Zhivut Trolli. I Kto ih Kormi,t," *Novaya Gazeta*, September 9, 2013. As of April 24, 2019:
https://www.novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit

Geng, Olivia, "'Very Big Muscles': Chinese Propaganda Video Lavishes Praise on Putin," blog post, *Wall Street Journal*, May 8, 2015. As of April 30, 2019:
https://blogs.wsj.com/chinarealtime/2015/05/08/very-big-muscles-chinese-propaganda-video-lavishes-praise-on-putin

"German Intelligence Unmasks Alleged Covert Chinese Social Media Profiles," Reuters, December 10, 2017.

"Germany Says New Security Strategy Will Respond to Russia," Reuters, February 17, 2015. As of May 10, 2019:
https://www.reuters.com/article/us-germany-security/germany-says-new-security-strategy-will-respond-to-russia-idUSKBN0LL1BK20150217

Ghosh, Dipayan, and Ben Scott, "#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet," New America, Public Interest Technology Program, January 2018.

Giles, Keir, "Indicators and Warnings for Detecting Information Threats," YouTube video of remarks at the Riga StratCom Dialogue: Perception Matters, NATO StratCom Center of Excellence, Riga, Latvia, August 20–21, 2015. As of April 17, 2016:
https://www.youtube.com/watch?v=RW3DHoQYayM

———, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, London: Chatham House, March 2016a.

———, *Handbook of Russian Information Warfare,* Research Division, NATO Defense College, November 2016b.

Glaser, April, "Twitter Admits There Were More Than 50,000 Russian Bots Trying to Confuse American Voters Before the Election Campaign," *Slate*, January 19, 2018. As of April 24, 2019:
https://slate.com/technology/2018/01/twitter-admits-there-were-more-than-50-000-russian-bots-confusing-u-s-voters-in-2016.html

Glaser, Bonnie, and Matthew P. Funaiole, "Xi Jinping's 19th Party Congress Speech Heralds Greater Assertiveness in Chinese Foreign Policy," Center for Strategic and International Studies, October 26, 2017. As of April 28, 2019: https://www.csis.org/analysis/xi-jinpings-19th-party-congress-speech-heralds-greater-assertiveness-chinese-foreign-policy

Glatz, Rainer L., and Martin Zapfe, "Ambitious Framework Nation: Germany in NATO," German Institute for International and Security Affairs, September 2017. As of May 10, 2019: https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C35_glt_zapfe.pdf

Gorman, Jack, and Sara Gorman, *Denying to the Grave: Why We Ignore the Facts That Will Save Us*, 2016.

Gorton, William A., "Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy," *New Political Science*, Vol. 38, No. 1, 2016.

Gorwa, Robert, and Douglas Guilbeault, "Understanding Bots for Policy and Research: Challenges, Methods, and Solutions," Prague: Conference of the International Communication Association, May 2018. As of April 24, 2019: https://arxiv.org/pdf/1801.06863.pdf

Grassegger, Hannes, and Mikael Krogerus, "Weaken from Within," *New Republic*, November 2, 2017.

Green, D. P., and A. S. Gerber, "Voter Mobilization, Experimentation, and Translational Social Science," *Perspectives in Politics*, Vol. 14, 2016, pp. 738–749.

Greenberg, Andy, "Hackers Hit Macron with Huge Email Leak Ahead of French Election," *Wired*, May 5, 2017. As of April 24, 2019: https://www.wired.com/2017/05/macron-email-hack-french-election/

Greenberg, Andy, "Don't Pin the Macron Email Hack on Russia Just Yet," *Wired*, May 8, 2017b. As of April 24, 2019: https://www.wired.com/2017/05/dont-pin-macron-email-hack-russia-just-yet/

Groot, Gerry, "The Long Reach of China's United Front Work," *Lowy Interpreter*, November 6, 2017a.

———, "United Front Work After the 19th Party Congress," *China Brief*, December 22, 2017b. As of April 29, 2019: https://jamestown.org/program/united-front-work-19th-party-congress

Grundy, Tom, "Did China's State-Run News Agency Purchase Twitter Followers?" *Hong Kong Free Press*, April 14, 2015. As of May 6, 2019: https://www.hongkongfp.com/2015/04/14/did-chinas-state-run-news-agency-purchase-twitter-followers/

Guo, Eileen, "How WeChat Spreads Rumors, Reaffirms Bias, and Helped Elect Trump," *Wired*, April 20, 2017. As of May 6, 2019: https://www.wired.com/2017/04/how-wechat-spreads-rumors-reaffirms-bias-and-helped-elect-trump/

Győri, Lóránt, Peter Krekó, Jakub Janda, and Bernhard Weidinger, *Does Russia Interfere in Czech, Austrian, and Hungarian Elections?* Political Capital, European Values, in cooperation with Dokumentations Archiv des österreichischen Widerstandes, 2017.

Haidt, Jonathan, *The Righteous Mind: Why Good People Are Divided by Politics and Religion*, New York: Vintage Books, 2013.

Haines, John R., "Distinguishing the True from the False: Fakes and Forgeries in Russia's Information War Against Ukraine," Foreign Policy Research Institute, September 28, 2016. As of April 24, 2019: https://www.fpri.org/article/2016/09/distinguishing-true-false-fakes-forgeries-russias-information-war-ukraine/#_ftn49

Halliday, Josh, "BBC World Service Fears Losing Information War As Russia Today Ramps Up Pressure," *The Guardian,* December 21, 2014.

Halper, Stephan, *China: The Three Warfares*, Washington, D.C.: Office of Net Assessment, 2013.

Hamilton, Clive, *Silent Invasion: China's Influence in Australia*, Richmond, Australia: Hardie Grant, 2018.

Han Song and Ping Chuan, "Grasp Important Points, Explain Difficult Points, Decipher Confusion Points: How to Explain 3rd Plenum Meeting of 18th Party Congress to Foreigners" ["抓重点 解难点 释疑点——如何做好十八届三中全会的对外解读"], *International Communications*, January 2014.

Harrell, Margaret C., and Melissa A. Bradley, *Data Collection Methods: Semi-Structured Interviews and Focus Groups*, Santa Monica, Calif.: RAND Corporation, TR-718-USG, 2009. As of April 17, 2019: https://www.rand.org/pubs/technical_reports/TR718.html

Harrington, Kent, "Will China Weaponize Social Media?" *Project Syndicate*, February 5, 2018. As of July 10, 2019: https://www.project-syndicate.org/commentary/xi-jinping-china-foreign-influence-campaigns-by-kent-harrington-2018-02

Hatmaker, Taylor, "Here's How Russia Targeted Its Fake Facebook Ads and How Those Ads Performed," *Tech Crunch*, November 1, 2017. As of April 17, 2019: https://techcrunch.com/2017/11/01/list-russian-ads-facebook-instagram/

Heath, Timothy, "Beijing's Influence Operations Target Chinese Diaspora," *War on the Rocks*, March 1, 2018. As of April 30, 2019: https://warontherocks.com/2018/03/beijings-influence-operations-target-chinese-diaspora/

Hellman, Maria, and Charlotte Wagnsson, "How Can European States Respond to Russian Information Warfare? An Analytical Framework," *European Security*, Vol. 26, No. 2, 2017, pp. 156–157.

Helm, Toby, "Third of EU Referendum Voters Won't Make up Their Minds Until Week Before Poll," *The Guardian*, June 11, 2016. As of May 8, 2019: https://www.theguardian.com/politics/2016/jun/11/brexit-eu-referendum-vote-last-minute-decision-decide-lse

Helmus, Todd, Christopher Paul, and Russell W. Glenn, *Enlisting Madison Avenue: The Marketing Approach to Earning Popular Support in Theaters of Operation*, Santa Monica, Calif.: RAND Corporation, MG-607-JFCOM, 2007. As of April 17, 2019: https://www.rand.org/pubs/monographs/MG607.html

Henchowitz, Anne, "Thousands of Local Internet Propaganda Emails Leaked," *China Digital Times*, December 3, 2014.

Hernandez, Javier C., and Melissa Eddy, "China Denies Using LinkedIn to Recruit German Informants," *New York Times*, December 11, 2017.

Hirss, Martins, "The Extent of Russia's Influence in Latvia," National Defense Academy of Latvia, Working Paper No. 03/16, November 2016.

Holland, Max, "The Propagation and Power of Communist Security Services Dezinformatsiya," *International Journal of Intelligence and Counterintelligence*, Vol. 19, No. 1, 2006.

Horvitz, Josh, "China's Military Has Released a Rap Video in Order to Lure More Recruits," *Quartz*, May 3, 2016.

Horwitz, Josh, "A Chinese Student's Commencement Speech Praising "Fresh Air" and Democracy Is Riling China's Internet," *Quartz*, May 23, 2017a. As of May 5, 2019: https://qz.com/989454/a-chinese-students-commencement-speech-at-the-university-of-maryland-praising-fresh-air-and-democracy-is-riling-chinas-internet/

———, "Australian Professors and Universities Are Being Shamed into Apologizing for Offending Chinese Students," *Quartz*, August 29, 2017b.

"Hotels Turn Away South Koreans, Chinese Smash Goods as Missile Row Widens," Radio Free Asia, March 13, 2017.

Hou Dongsheng, "Comparison and Analysis of Foreign Propaganda Related to Tibet Between Chinese Government and Dalai Lama Clique" ["中国政府与达赖集团在涉藏外宣上的比较和分析"], *Journal Of Chongqing Institute of Socialism*, June 2012.

Howard, Philip N., Gillian Bolsover, Bence Kollanyi, Samantha Bradshaw, and Lisa-Maria Neudert, "Junk News and Bots During the U.S. Election: What Were Michigan Voters Sharing over Twitter?" Data Memo 2017.1, Oxford, UK: Project on Computational Propaganda, Oxford Internet Institute, University of Oxford, March 26, 2017.

Howard, Philip N., and Bence Kollanyi, "Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum," Research Note 2016.1, Oxford, UK: Project on Computational Propaganda, 2016. As of April 19, 2019:
http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2016/06/COMPROP-2016-1.pdf

Hu Jintao, "Resolutely Follow the Cultural Development Path of Socialism with Chinese Characteristics, Work to Build a Socialist Strong Culture Country" ["坚定不移走中国特色社会主义文化发展道路努力建设社会主义文化强国"], *Seeking Truth*, January 1, 2012.

Hu Xiaojian, "Decoding the U.S. 'Murphy-Portman Counter-Propaganda Bill,'" *International Study Reference*, July 2017, pp. 26–29.

Hu Yu and Lu Jun, "Experiences and Thoughts on Construction of Central-Level State-Owned Enterprises Image Abroad" ["央企海外形象建设的经验与思考"], *International Communications*, October 2016.

Huang Chien and Hsieh Chun-lin, "Prosecutors: China Paid Wang for Propaganda," *Taipei Times*, January 3, 2018. As of May 6, 2019:
http://www.taipeitimes.com/News/front/archives/2018/01/03/2003685092/1

Huang Dahui, "Analyzing the Abe Government's Foreign Propaganda Strategy" ["试析安倍政府的对外宣传战略"], *Contemporary International Relations*, June 2017.

Huang, Zheping, "China's Craziest English-Language Propaganda Videos Are Made by One Mysterious Studio," *Quartz*, October 27, 2015. As of April 30, 2019:
https://qz.com/533850/chinas-craziest-english-language-propaganda-videos-are-made-by-one-mysterious-studio/

———, "China Wants to Build a Credit Score That Dings Online Chat Group Users for Their Political Views," *Quartz*, September 8, 2017. As of May 5, 2019:
https://qz.com/1072660/china-wants-to-build-a-credit-score-that-dings-online-chat-group-users-for-their-political-views/

Hutchings, Stephen, and Joanna Szostek, "Dominant Narratives in Russian Political and Media Discourse During the Ukraine Crisis," in Agnieska Pikulicksa-Wilczewska and Richard Sakwa, eds., *Ukraine and Russia: People, Politics, Propaganda, and Perspectives,* Bristol, UK: E-International Relations Publishing, 2015.

Hvistendal, Mara, "Inside China's Vast New Experiment in Social Ranking," *Wired*, December 14, 2017. As of May 5, 2019: https://www.wired.com/story/age-of-social-credit/

"Inside China's Secret 'Magic Weapon' for Worldwide Influence," *Financial Times*, October 26, 2017.

Isaac, Mike, "Facebook Said to Create Censorship Tool to Get Back into China," *New York Times*, November 22, 2016. As of April 29, 2019: https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html

Ives, Mike, "Chinese Student in Maryland Is Criticized at Home for Praising U.S.," *New York Times*, May 23, 2017. As of May 5, 2019: https://www.nytimes.com/2017/05/23/world/asia/chinese-student-fresh-air-yang-shuping.html

Jain, Shailendra Pratap, and Steven S. Posavac, "Prepurchase Attribute Verifiability, Source Credibility, and Persuasion," *Journal of Consumer Psychology*, Vol. 11, No. 3, 2001, pp. 169–180.

Jamieson, Kathleen Hall, "Messages, Micro-Targeting, and New Media Technologies," *The Forum*, Vol. 11, No. 3, January 2013, pp. 429–435. As of April 17, 2019: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1363&context=asc_papers

———, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President*, New York: Oxford University Press, 2018.

Jenkins, Tricia, "What Did Russian Trolls Want in 2016?" blog post, *War on the Rocks*, May 22, 2018. As of April 23, 2019: https://warontherocks.com/2018/05/what-did-russian-trolls-want-during-the-2016-election-a-closer-look-at-the-internet-research-agencys-active-measures/

Jervis, Robert, "Hypotheses on Misperception," *World Politics*, Vol. 20, No. 3, April 1968, pp. 454–479.

Ji Deqiang, "Global Communications for China's Anti-Corruption Campaign: Problems and Solutions—Based on Real Research of Chinese Students Studying Abroad" ["中国反腐的国际传播：困境与出路 一一基于对在华外国留学生的实证研究"], *International Communications*, December 2016.

Jia Min, "Creator's Plight: The Good and Bad of Shaping Obama's Image" ["创新者的窘境:奥巴马形象塑造中的得与失"], *International Communications*, April 2014.

Jiang, Steven, "Beijing Has a New Propaganda Weapon: Voice of China," CNN Business, March 21, 2018. As of April 29, 2019: https://money.cnn.com/2018/03/21/media/voice-of-china-propaganda-broadcaster/index.html

Jiang Yunai, "Shaping National Leaders' Image Through Foreign Communication via New Media—2015 Twitter Reporting by Xinhua, *People's Daily* and CCTV as Examples" ["新媒体对外传播中的国家领导人形象塑造——以2015年新华社、《人民日报》、央视的推特报道为例"], *International Communications*, April 2016.

Jiang Yunai and Luo Huanxin, "A Study on the Influence of Video Coverage on Internationally Well-Known Social Media Platforms: A Case Study of RT's English Language YouTube Account" ["国际知名媒体社交平台视频报道影响力研究——以RT的YouTube英文主账号为例"], *International Communications*, September 2017.

John, Leslie K., Oliver Emrich, Sunil Gupta, and Michael I. Norton, "Does 'Liking' Lead to Loving: The Impact of Joining a Brand's Social Network on Marketing Outcomes," *Journal of Marketing Research,* Vol. 54, No. 1, 2017a.

John, Leslie K., Daniel Mochon, Oliver Emrich, and Janet Schwartz, "What's the Value of a Like?" *Harvard Business Review*, March–April, 2017b.

Joske, Alex, "Beijing Is Silencing Chinese-Australians," *New York Times*, February 6, 2018.

Jowett, Garth, and Victoria O'Donnell, *Propaganda and Persuasion*, Beverly Hills, Calif.: Sage Publications, 1986.

Juhász, Attila, Lóránt Győri, Péter Krekó, and András Dezső, "'I Am Eurasian': The Kremlin Connections of the Hungarian Far-Right," Political Capital and Social Development Institute, March 2015.

Kaiman, Jonathan "Free Tibet Exposes Fake Twitter Accounts by China Propagandists," *The Guardian*, July 22, 2014.

Kalugin, Oleg, *Vechernyaya Moskva*, November 3, 1990, as referenced in Robert W. Pringle, "Andropov's Counterintelligence State," *International Journal of Intelligence and Counterintelligence*, Vol. 13, No. 2, 2000, p. 199.

———, *Spymaster: My Thirty-Two Years in Intelligence and Espionage Against the West*, New York: Basic Books, 2009.

Kaminska, Monica, John D. Gallacher, Bence Kollanyi, Taha Yasseri, and Philip N. Howard, "Social Media and News Sources During the 2017 UK General Election," Data Memo 2017.6, Oxford, UK: Project on Computational Propaganda, Oxford Internet Institute, University of Oxford, June 5, 2017.

Kania, Elsa, "The PLA's Latest Strategic Thinking on the 'Three Warfares,'" *Jamestown Foundation China Brief*, Vol. 16, No. 13, August 22, 2016.

Karpinski, Wojciech, "Agents and Exiles," *Survey*, Vol. 27, Autumn–Winter, 1983.

Kasapoglu, Can, "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control," NATO Research Division, Research Paper No. 121, November 2015.

Kavanaugh, Jennifer, and Michael 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 April 19, 2019: https://www.rand.org/pubs/research_reports/RR2314.html

Keck, Zachary, "Justin Bieber Visits Japan's Yasukuni War Shrine," *The Diplomat*, April 24, 2014.

Kelly, Lidia, "Poland Plans Trump-Era Defense Spending Splurge, Critics Say 'Unrealistic,'" Reuters, June 16, 2017. As of May 10, 2019: https://www.reuters.com/article/us-nato-poland-defence/poland-plans-trump-era-defense-spending-splurge-critics-say-unrealistic-idUSKBN1970Y6

Kenez, Peter, *The Birth of the Propaganda State: Soviet Methods of Mass Mobilization, 1917–1929*, Cambridge, UK: Cambridge University Press, 1985.

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, 2017, pp. 484–501.

Kinstler, Linda, "How to Survive a Russian Hack: Lessons from Eastern Europe and the Baltics," *The Atlantic*, February 2, 2017.

Kirk, Michael, interview of Gleb Pavlovsky, former adviser to Vladimir Putin, "The Putin Files," *Frontline*, PBS, July 13, 2017a.

———, interview of Andrei Soldatov, "The Putin Files," *Frontline*, PBS, July 25, 2017b.

Kirkpatrick, David D., "Facebook Sees Little Evidence of Russian Meddling in 'Brexit' Vote," *New York Times*, December 13, 2017.

Kivirähk, Juhan, "Public Opinion and National Defence," Tallinn: Estonian Ministry of Defense, Spring 2018.

Kleemola, Katie, Masashi Crete-Nishihata, and John Scott-Railton, "Targeted Attacks Against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114," Citizen Lab, June 15, 2015. As of May 5, 2019: https://citizenlab.ca/2015/06/targeted-attacks-against-tibetan-and-hong-kong-groups-exploiting-cve-2014-4114

Koh Gui Qing and John Shiffman, "Beijing's Covert Radio Network Airs China-Friendly News Across Washington, and the World," Reuters, November 2, 2015. As of April 29, 2019: https://www.reuters.com/investigates/special-report/china-radio/

Kollanyi, Bence, Phillip N. Howard, and Samuel C. Woolley, "Bots and Automation over Twitter During the U.S. Election," Comprop Data Memo 2016.4, Computational Propaganda Research Project, University of Oxford, Oxford, UK, November 17, 2016.

Kotlyar, Evgenia, "U Nas Byla Cel' . . . Vyzvat Besporjadki': Interv'ju s Jeks-Sotrudnikom 'Fabriki Trollej' v Sankt-Peterburge," *Dozhd*, October 14, 2017. As of April 24, 2019:
https://tvrain.ru/teleshow/bremja_novostej/fabrika-447628/

Kou Liyan, "Strategic Communications in the 'Micro-Struggle'—The Impact and Response of Trump Entering the White House on China's Strategic Communications" ["在"微斗争"中开展战略传播——特朗普入主白宫对中国战略传播的影响及应对"], *International Communications*, February 2017.

Kovalev, Alexey, and Matthew Bodner, "The Secrets of Russia's Propaganda War, Revealed," *Moscow Times*, March 1, 2017. As of April 17, 2019:
https://themoscowtimes.com/articles/
welcome-to-russian-psychological-warfare-operations-101-57301

Kragh, Martin, and Sebastian Asberg, "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies,* Vol. 40, No. 6, pp. 782–784, 2017.

Kramer, Michael, "Rescuing Boris," *Time*, July 15, 1996, pp. 29–37.

Kuhn, Robert Lawrence, "Xi Jinping's China Dream," *New York Times*, June 4, 2013.

Kux, Dennis, "Soviet Active Measures and Disinformation: Overview and Assessment," *Parameters*, Vol. 15, No. 4, 1985.

Kynge, James, Lucy Hornby, and Jamil Anderlini, "Inside China's Secret 'Magic Weapon' for Worldwide Influence," *Financial Times*, October 26, 2017. As of April 29, 2019:
https://www.ft.com/content/fb2b3934-b004-11e7-beba-5521c713abf4

Labin, Suzanne, "The Technique of Soviet Propaganda," presented to the Subcommittee to Investigate the Administration of the Internal Security Act and other Internal Security Laws, 86th U.S. Congress, 2nd Session, 1965.

LaGrone, Sam, "China's First Domestic Aircraft Carrier Almost Certainly Under Construction," *USNI*, September 30, 2015.

Lake, Eli, "Putin's Latest Dirty Trick: Leaking Private Phone Calls," *Daily Beast,* March 26, 2014. As of April 24, 2019:
https://www.thedailybeast.com/putins-latest-dirty-trick-leaking-private-phone-calls

Lakoff, George, *Don't Think of an Elephant: Know Your Values and Frame the Debate*, White River Junction, Vt.: Chelsea Green Publishing, 2014.

Landler, Mark, "Trump Accuses China of Interfering in Midterm Elections," *New York Times*, September 26, 2018. As of April 26, 2019:
https://www.nytimes.com/2018/09/26/world/asia/trump-china-election.html

Langfitt, Frank, "How China's Censors Influence Hollywood," NPR, May 18, 2015. As of April 29, 2019:
https://www.npr.org/sections/parallels/2015/05/18/407619652/how-chinas-censors-influence-hollywood

LaPiere, Richard T., "Attitudes vs. Actions," *Social Forces*, Vol. 13, No. 2, 1934, pp. 230–237.

Lecher, Colin, "Here Are the Russia-Linked Facebook Ads Released by Congress," *The Verge*, November 1, 2017.

Lee, Georgina, "Here's What We Know About the Alleged Russian Involvement in Brexit," 4News, November 16, 2017. As of May 8, 2019:
https://www.channel4.com/news/factcheck/heres-what-we-know-about-alleged-russian-involvement-in-brexit

Lee, Yimou, and Faith Hung, "How China's Shadowy Agency Is Working to Absorb Taiwan," Reuters, November 26, 2014. As of April 29, 2019:
https://www.reuters.com/article/us-taiwan-china-special-report/special-report-how-chinas-shadowy-agency-is-working-to-absorb-taiwan-idUSKCN0JB01T20141127

Li, Pei, and Adam Jourdan, "Mercedes-Benz Apologizes to Chinese for Quoting Dalai Lama," Reuters, February 6, 2018. As of May 5, 2019:
https://www.reuters.com/article/us-mercedes-benz-china-gaffe/mercedes-benz-apologizes-to-chinese-for-quoting-dalai-lama-idUSKBN1FQ1FJ

Li Qiaoming, "Analysis of Modern Warfare Development Based on Russia's Two Conflicts," *PLA Daily*, August 16, 2016.

Li Yiqing, "两家俄官媒推特账号广告功能遭关闭，曾被美指责"干预大选""], *The Paper*, October 27, 2017. As of April 29, 2019:
http://www.thepaper.cn/newsDetail_forward_1839554

Lian Xiaotong, "Analysis of Leaders' Public Diplomacy Strategy from a Cross-Cultural Perspective—Xi Jinping's 2012 Visit to the United States as Example" ["跨文化视野下领导人公共外交策略分析——以2012年习近平访美为例"], *International Communications*, September 2013.

Lieberthal, Kenneth, *Governing China: From Revolution Through Reform*, New York: W.W. Norton & Co., 1995.

Liff, Adam, "China and the U.S. Alliance System," *China Quarterly*, April 2017.

Lin, Herbert, and Jackie Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation," in *Oxford Handbook of Cybersecurity*, August 14, 2017. As of April 19, 2019:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680

Linthicum, Kate, "Meet the Chinese American Immigrants Who Are Supporting Donald Trump," *Los Angeles Times*, May 27, 2016. As of May 6, 2019:
http://www.latimes.com/politics/la-na-pol-asian-voters-20160527-snap-story.html

Liu Chen, "Audience Strategy for Foreign Communications on the Image of China's Economy" ["中国经济形象对外传播的受众策略"], *International Communications*, November 2011.

Liu Jun, "Wang Chen, Guard of China's Image: A Review of His Statements and Actions in the Past Year Shows That the Question-and-Answer Papers Handed in by This Ministerial-Level Official, Who Used to Be a Journalist, Are Outstanding," *Guoji Xianqu Daobao*, March 12, 2010.

Liu Yang, "Thoughts on Change of U.S. Administration and Adjustments to China's International Communications Strategy" ["对美国政府更迭与中国对外传播策略调整的思考"], *International Communications*, February 2017.

Liu Yi, "Public vs. Secret: Military News Releases," *Military Correspondent*, August 2009.

Liu Yunsan, "Review and Outlook—This Article Is Abridged from the Speech Made by Comrade Liu Yunshan at the Meeting for Leading Comrades in Central Propaganda and Cultural Units on 25 December, 2008" *Seeking Truth*, January 2009.

Liu Zhen, "How One Chinese American Became Politically Aware . . . and Joined the Ranks of Trump Supporters," *South China Morning Post*, November 2, 2016. As of May 6, 2019:
http://www.scmp.com/news/china/diplomacy-defence/article/2042268/how-one-chinese-american-became-politically-aware-and

Lord, Charles G., Lee Ross, and Mark R. Lepper, "Biased Assimilation and Attitude Polarization: The Effects of Prior Theories on Subsequently Considered Evidence," *Journal of Personality and Social Psychology*, Vol. 37, No. 11, 1979, pp. 2098–2109. As of April 17, 2019:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.372.1743&rep=rep1&type=pdf

Lu Wenxing, "Innovative Developments in Military Broadcasts to Taiwan in the New Communication Age," *Military Correspondent*, December 2010.

Lu Xin, "Three Highlights from 2011's New Media Propaganda" ["2011年新媒体外宣的三个亮点"], *People's Daily Online*, December 29, 2011. As of April 30, 2019:
http://media.people.com.cn/GB/22114/41180/237490/16754147.html

Lucas, Louise, "Questions over Pace of Growth As WeChat Nears 1bn Users," *Financial Times*, August 30, 2017. As of May 6, 2019:
https://www.ft.com/content/b557d6c8-8891-11e7-8bb1-5ba57d47eff7

Lynch, Daniel C., *After the Propaganda State: Media, Politics, and 'Thought Work' in Reformed China*, Stanford, Calif.: Stanford University Press, 1999.

Ma Chao and Sun Hao, "The Characteristics of Russian Public Opinion Propagation: Taking 'Russia Today' TV Station as an Example" ["俄罗斯对外舆论传播的特点:以'今日俄罗斯'电视台为列"], *Military Correspondent*, June 2018. As of April 28, 2019:
http://www.81.cn/jsjz/2018-06/14/content_8061994.htm

Ma, Damien, "Beijing's 'Culture War' Isn't About the U.S.—It's About China's Future," *The Atlantic*, January 5, 2012. As of April 28, 2019:
https://www.theatlantic.com/international/archive/2012/01/beijings-culture-war-isnt-about-the-us-its-about-chinas-future/250900/

Ma Han, "Research and Opinion on Current Problems in Building China's International Voice" ["当前中国国际话语权构建问题研究谫论"], *Journal of Yunnan Provincial Committee School of CCP*, December 2016.

Ma Jianguang, Zhang Xiubo and Zhang Naiqian, "Russia's New Front for Defending Internet Media" ["俄罗斯布防网络媒体新阵地"], *China Military Online*, April 13, 2016. As of April 28, 2019:
http://www.81.cn/jwgd/2016-04/13/content_7004902.htm

Ma, Wayne, "Marriott Employee Roy Jones Hit 'Like.' Then China Got Mad," *Wall Street Journal*, March 3, 2018. As of May 5, 2019:
https://www.wsj.com/articles/marriott-employee-roy-jones-hit-like-then-china-got-mad-1520094910

Ma Yi, "Strengthening Agenda-Setting for Military News Coverage Targeting Taiwan," *Military Correspondent*, September 2010.

"Macron et Le Pen au Second Tour D'une Présidentielle hors Norme," *Sud-Ouest*, April 23, 2017. As of May 8, 2019:
http://www.sudouest.fr/2017/04/23/macron-et-le-pen-au-second-tour-d-une-presidentielle-hors-norme-3389901-6121.php

"Macron Leaks: The Anatomy of a Hack," BBC News, May 9, 2017. As of May 8, 2019:
http://www.bbc.com/news/blogs-trending-39845105

Maio, Gregory R., and Geoffrey Haddock, *The Psychology of Attitudes and Attitude Change*, London: SAGE Publications, 2009.

"Majority of Young People in Central and Eastern Europe Strongly Backs the EU," Bertelsmann Stiftung, March 21, 2017. As of May 10, 2019:
https://www.bertelsmann-stiftung.de/en/topics/aktuelle-meldungen/2017/maerz/majority-of-young-people-in-central-and-eastern-europe-strongly-backs-the-eu/

Maley, Paul, "From Beijing to Parramatta: How China Muscled Up to Council," *The Australian*, November 11, 2017.

Manchanda, P., Y. Xie, and N. Youn, "The Role of Targeted Communication and Contagion in Product Adoption," *Marketing Science*, Vol. 27, 2008, pp. 961–976.

"Market Share Held by the Leading Social Networks in the United Kingdom (UK) as of July 2017," Statista, 2017.

Markoff, John, "Vast Spy System Loots Computers in 103 Countries," *New York Times*, March 28, 2009. As of May 5, 2019: http://www.nytimes.com/2009/03/29/technology/29spy.html

Marriott Corporation, tweet, Twitter, January 10, 2018. As of May 6, 2019: https://twitter.com/marriottrewards/status/951344031405084673?lang=en

Marwick, Alice, and Rebecca Lewis, "Media Manipulation and Disinformation Online," Data and Society Research Institute, undated. As of April 24, 2019: http://www.chinhnghia.com/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf

Mastro, Oriana Skylar, "Why Chinese Assertiveness Is Here to Stay," *Washington Quarterly*, Vol. 37, No. 4, Winter 2015, pp. 151–170.

Mate, Aron, "RT Was Forced to Register as a Foreign Agent," *The Nation*, November 16, 2017.

Mattis, Peter, "Contrasting China's and Russia's Influence Operations," *War on the Rocks*, January 16, 2018. As of April 29, 2019: https://warontherocks.com/2018/01/contrasting-chinas-russias-influence-operations/

McKinsey and Company, "Targeted Online Marketing Programs Boost Customer Conversion Rates," webpage, undated. As of November 7, 2017: https://www.mckinsey.com/business-functions/marketing-and-sales/how-we-help-clients/clm-online-retailer

Meng Jing and Celia Chen, "China Fines Tencent, Baidu, Weibo over Banned Contents in On-Going Crackdown," *South China Morning Post*, September 26, 2017.

Menn, Joseph, "Exclusive: Russia Used Facebook to Try to Spy on Macron Campaign—Sources," Reuters, July 27, 2017. As of May 9, 2019: https://www.reuters.com/article/us-cyber-france-facebook-spies-exclusive/exclusive-russia-used-facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBN1AC0EI

Meserole, Chris, and Alina Polakova, "Disinformation Wars," *Foreign Policy*, May 25, 2018.

Metaxas, Panagiotis T., and Eni Mustafaraj, "Social Media and the Elections," *Science*, Vol. 338, No. 6106, October 2012. As of May 8, 2019: http://dx.doi.org/10.1126/science.1230456

"Military Expenditure by Country As Percentage of Gross Domestic Product," Stockholm International Peace Research Institute, 2017. As of May 10, 2019: https://www.sipri.org/sites/default/files/Milex-share-of-GDP.pdf

Ministry of Defense of the Russian Federation, "Russian Federation Armed Forces' Information Space Activities Concept, 2011," January 2012. As of July 10, 2019: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

Ministry of Foreign Affairs of the Republic of Latvia, "16+1 Summit Has Concluded," press release, February 22, 2017. As of May 10, 2019: http://www.mfa.gov.lv/en/policy/multilateral-relations/cooperation-between-central-and-eastern-european-countries-and-china

Ministry of Foreign Affairs of the Russian Federation, "National Security Concept of the Russian Federation," January 10, 2000.

———, "Doctrine of Information Security of the Russian Federation," December 5, 2016. As of April 18, 2018: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

Monaco, Nicholas J., "Computational Propaganda in Taiwan: Where Digital Democracy Meets Automated Autocracy," Computational Propaganda Research Project, Oxford University, Oxford, UK, June 2017. As of April 30, 2019: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Taiwan-2.pdf

Monaghan, Andrew, *The New Politics of Russia,* Manchester, UK: Manchester University Press, 2016.

Morozov, Evgeny, "Is Russia Google's Next Weak Spot?" *Foreign Policy*, March 26, 2010.

Mozur, Paul, "Facebook Briefly Suspends Account of Outspoken Chinese Billionaire," *New York Times*, April 21, 2017a.

———, "China Spreads Propaganda to U.S. on Facebook, a Platform It Bans at Home," *New York Times*, November 8, 2017b.

———, "China Presses Its Internet Censorship Efforts Across the Globe," *New York Times*, March 2, 2018. As of May 5, 2019: https://mobile.nytimes.com/2018/03/02/technology/china-technology-censorship-borders-expansion.html

Munro, Geoffrey D., and Peter H. Ditto, "Biased Assimilation, Attitude Polarization, and Affect in Reactions to Stereotype-Relevant Scientific Information," *Personality and Social Psychology Bulletin*, Vol. 23, No. 6, 1997, pp. 636–653.

Mutz, Diana C., Richard A. Brody, and Paul M. Sniderman, eds., *Political Persuasion and Attitude Change*, Ann Arbor, Mich.: University of Michigan Press, 1996.

"Nacgvardija Obstreljala Semenovku Fosfornymi Bombami," Zvezda, June 6, 2014. As of April 24, 2019: https://tvzvezda.ru/news/vstrane_i_mire/content/201406120351-12ni.htm

Nakamura, David, and Ellen Nakashima, "Without Offering Evidence, Trump Accuses China of Interfering in U.S. Midterm Elections," *Washington Post*, September 26, 2018. As of April 26, 2019: https://www.washingtonpost.com/politics/without-evidence-trump-accuses-china-of-interfering-in-us-midterm-elections/2018/09/26/c0069910-c19d-11e8-b338-a3289f6cb742_story.html?noredirect=on&utm_term=.cc9eacb0578b

Narayanan, Vidya, Philip N. Howard, Bence Kollanyi, and Mona Elswah, "Russian Involvement and Junk News During Brexit," Oxford, UK: Oxford Program on Computational Propaganda, Oxford University, December 19, 2017. As of May 8, 2019: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/12/Russia-and-Brexit-v27.pdf

Nathan, Andrew J., and Andrew Scobell, *China's Search for Security*, New York: Columbia University Press, 2012.

National Endowment for Democracy, "Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News,'" October 17, 2017.

"National Security Strategy," *Republic of Lithuania*, January 17, 2017. As of May 10, 2019: http://kam.lt/download/56659/national%20security%20strategy%202017-01-17.pdf

National Security Strategy of the United States of America, Washington, D.C.: The White House, December 2017.

"National Security Unit: Anti–Pension Reform Protests Had Intervention from Chinese Forces" ["國安單位：反年改陳抗 有中國勢力介入"], *Liberty Times*, July 18, 2017.

NATO—*See* North Atlantic Treaty Organization.

"NATO's Enhanced Forward Presence Factsheet," NATO Public Diplomacy Division, May 2017. As of May 7, 2019: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_05/1705-factsheet-efp.pdf

"Negotiating the News: Informal State Censorship of Ukrainian Television," *Human Rights Watch*, Vol. 3, No. 2, March 2003, pp. 13–24. As of April 23, 2019: https://www.hrw.org/reports/2003/ukraine0303/Ukraine0303.pdf

Nelson, Elizabeth, Robert Orttung, and Anthony Livshen, "Measuring RT's Impact on YouTube," *Russian Analytical Digest*, December 2016.

Nelson, Thomas E., and Zoe M. Oxley, "Issue Framing Effects and Belief Importance and Opinion," *Journal of Politics*, Vol. 61, No. 4, 1999, pp. 1040–1067.

Nelson, Thomas E., Rosalee A. Clawson, and Zoe M. Oxley, "Media Framing of a Civil Liberties Conflict and Its Effect on Tolerance," *American Political Science Review,* Vol. 91, No. 3, 1997, pp. 567–583.

Neudert, Lisa-Maria, Bence Kollanyi, and Philip N. Howard, "Junk News and Bots During the German Parliamentary Election: What Are German Voters Sharing over Twitter?" Data Memo 2017.7, Oxford, UK: Project on Computational Propaganda, Oxford Internet Institute, University of Oxford, September 19, 2017.

Newman, Eryn J., Mevagh Sanson, Emily K. Miller, Adele Quigley-McBride, Jeffrey L. Foster, Daniel M. Bernstein, and Maryanne Garry, "People with Easier to Pronounce Names Promote Truthiness of Claims," *PLoS One*, Vol. 9, No. 2, 2014. As of April 18, 2019:
http://www.oalib.com/paper/3060435#.XLkg4i2ZOX0

Newport, Frank, "Americans' Confidence in Institutions Edges Up," press release, Gallup, June 26, 2017. As of May 7, 2019:
http://news.gallup.com/poll/212840/americans-confidence-institutions-edges.aspx

Ng, Teddy, "Marriott Sacks Employee Who 'Liked' Twitter Post from Tibet Independence Group," *South China Morning Post*, January 13, 2018. As of May 5, 2019:
http://www.scmp.com/news/china/society/article/2128124/marriott-sacks-employee-who-liked-twitter-post-tibet-independence

Nimmo, Ben, "Election Watch: Beyond Russian Impact," Atlantic Council Digital Forensic Research Lab, February 27, 2018.

North Atlantic Treaty Organization STRATCOM Center of Excellence, *Internet Trolling As a Tool of Hybrid Warfare: The Case of Latvia*, undated.

"Number of Social Network Users in France from 2014 to 2018 (in Millions)," Statista, 2017. As of May 8, 2019:
https://www.statista.com/statistics/260717/number-of-social-network-users-in-france/

"Number of Twitter Users in the United Kingdom (UK) from 2012 to 2018 (in Million Users)," Statista, 2017. As of May 8, 2019:
https://www.statista.com/statistics/271350/twitter-users-in-the-united-kingdom-uk/

Nyhan, Brendan, and Jason Reifler, "Misinformation and Fact Checking: Research Findings from Social Science," *New America Foundation*, February 2012. As of April 18, 2019:
http://www.dartmouth.edu/~nyhan/Misinformation_and_Fact-checking.pdf

———, "The Roles of Information Deficits and Identity Threat in the Prevalence of Misperceptions," Dartmouth College, February 24, 2017. As of April 18, 2019:
https://www.dartmouth.edu/~nyhan/opening-political-mind.pdf

Office for National Statistics, "Internet Access—Households and Individuals: 2017," August 3, 2017. As of May 8, 2019: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2017#email-remains-the-most-common-internet-activity

———, "Social Media Usage in the United Kingdom," Statista Dossier, August 2017b.

Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community assessment, January 6, 2017.

Olesen, Alexa, "Where Did Chinese State Media Get All Those Facebook Followers?" *Foreign Policy*, July 7, 2015. As of May 6, 2019: http://foreignpolicy.com/2015/07/07/china-facebook-peoples-daily-media-soft-power/

Olsson, Jojje, "Beware of Chinese Social Media," *Taiwan Sentinel*, September 23, 2017.

Oskamp, Stuart, and P. Wesley Schultz, *Attitudes and Opinions*, London: Lawrence Erlbaum Associates, 2005.

Osnos, Evan, "China's Culture Wars," *New Yorker*, January 5, 2012. As of April 28, 2019: https://www.newyorker.com/news/evan-osnos/chinas-culture-wars

Overseas Information Programs of the United States, "Hearings Before a Subcommittee of the Committee on Foreign Relations of the United States," 82nd Congress, November 20–21, 1953.

Palmer, James, "What China Didn't Learn from the Collapse of the Soviet Union," *Foreign Policy*, December 24, 2016. As of April 28, 2019: http://foreignpolicy.com/2016/12/24/what-china-didnt-learn-from-the-collapse-of-the-soviet-union/

Pan, Jason, "Military Men Probed over Wang Ties," *Taipei Times*, January 4, 2018. As of May 6, 2019: http://www.taipeitimes.com/News/front/archives/2018/01/04/2003685148

Pandey, Anil Azad, "How the Chinese Communist Party Is Using Social Media to Win Friends and Influence People," *OZY*, October 25, 2017.

Pannier, Alice, "Between Autonomy and Cooperation: The Role of Allies in France's New Defense Strategy," *War on the Rocks*, November 2, 2017. As of May 9, 2019: https://warontherocks.com/2017/11/between-autonomy-and-cooperation-the-role-of-allies-in-frances-new-defense-strategy/

Parker, Emily, "Can WeChat Thrive in the United States?" *MIT Technology Review*, August 11, 2017. As of May 6, 2019:
https://www.technologyreview.com/s/608578/can-wechat-thrive-in-the-united-states

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 April 23, 2019:
https://www.rand.org/pubs/perspectives/PE198.html

Peel, Michael, "EU States Poised to Agree Joint Defence Pact," *Financial Times*, November 7, 2017. As of May 9, 2019:
https://www.ft.com/content/29f6fe76-c2eb-11e7-a1d2-6786f39ef675

Peisakhin, Leonid, and Arturas Rozenas, "When Does Russian Propaganda Work—and When Does It Backfire? Here's What We Found." *Washington Post*, April 3, 2018. As of May 10, 2019:
https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/03/when-does-russian-propaganda-work-and-when-does-it-backfire-heres-what-we-found/?utm_term=.b05b1faf362b&wpisrc=nl_cage&wpmm=1

Pellerin, Cheryl, "Poland, a Valued NATO Member, Leads by Example, Mattis Says," press release, U.S. Department of Defense, September 22, 2017. As of May 10, 2019:
https://www.defense.gov/News/Article/Article/1321306/poland-a-valued-nato-member-leads-by-example-mattis-says/

People's Liberation Army Air Force, Weibo microblog status, December 12, 2017. As of April 29, 2019:
https://m.weibo.cn/status/4184081916589933

"Percentage of U.S. Population with a Social Media Profile from 2008 to 2017," Statista, 2019. As of May 8, 2019:
https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/

Persily, Nathaniel, "Can Democracy Survive the Internet?" *Journal of Democracy*, Vol. 28, No. 2, April 2017,

Pew Research Center, "Global Indicators Database," database, undated. As of October 12, 2018:
http://www.pewglobal.org/database/indicator/27/country/231/

———, "Partisanship and Political Animosity in 2016," June 22, 2016a. As of May 7, 2019:
http://www.people-press.org/2016/06/22/partisanship-and-political-animosity-in-2016/

———, "Many Americans Believe Fake News Is Sowing Confusion," December 15, 2016b.

Phillips, Tom, "Chinese Student Abused for Praising 'Fresh Air of Free Speech' in US," *The Guardian*, May 23, 2017. As of May 5, 2019: https://www.theguardian.com/world/2017/may/23/china-yang-shuping-free-speech-university-of-maryland-us-student

Pisnia, Natalka, "Why Has RT Registered As a Foreign Agent in the US?" BBC News, November 15, 2017.

PLAAF—*See* People's Liberation Army Air Force.

"Poland, NATO Launch Defensive Exercises amid Security Concerns," CBS News, September 21, 2017. As of May 10, 2019: https://www.cbsnews.com/news/poland-nato-launch-defensive-drills-security-concerns/

"Polish President Signs Defence Spending Boost into Law," Radio Poland, October 23, 2017. As of May 10, 2019: http://thenews.pl/1/9/Artykul/331690,Polish-president-signs-defence-spending-boost-into-law

Polyakova, Alina, "Russia Can't Decide If Ukrainian Jews Are Victims or Villains," *New Republic*, April 28, 2014. As of April 18, 2019: https://newrepublic.com/article/117556/putins-russia-using-ukrainian-jews-propaganda-tools

Pomerantsev, Peter, "Russia and the Menace of Unreality," *The Atlantic*, September 9, 2014.

Pomerantsev, Peter, and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, New York: The Interpreter, Institute of Modern Russia, 2014.

Popken, Ben, "Russian Trolls Went on Attack During Key Election Moments," NBC News, February 13, 2018. As of April 26, 2019: https://www.nbcnews.com/tech/social-media/russian-trolls-went-attack-during-key-election-moments-n827176

Poushter, Jacob, and Dorothy Manevich, "Globally, People Point to ISIS and Climate Change as Leading Security Threats," Pew Research Center, August 1, 2017.

"President Macron's Initiative for Europe: A Sovereign, United, Democratic Europe," French Ministry for Europe and Foreign Affairs, September 26, 2017. As of May 9, 2019: https://www.diplomatie.gouv.fr/en/french-foreign-policy/european-union/events/article/president-macron-s-initiative-for-europe-a-sovereign-united-democratic-europe

"President Signs Portman-Murphy Counter-Propaganda Bill into Law," Office of Senator Rob Portman, December 23, 2016. As of April 28, 2019: https://www.portman.senate.gov/public/index.cfm/2016/12/president-signs-portman-murphy-counter-propaganda-bill-into-law

"President Xi Urges New Media Outlet to 'Tell China Stories Well,'" Xinhua, December 31, 2016.

Pringle, Robert W., "Andropov's Counterintelligence State," *International Journal of Intelligence and Counterintelligence*, Vol. 13, No. 2, 2000, p. 199.

"Products and Services," webpage, Sputnik, undated. As of February 5, 2018: https://sputniknews.com/docs/products/index.html

"Protesters Demand Russian Soldier's Trial in Armenia, Clash with Police," RT, January 15, 2015. As of April 23, 2019: https://www.rt.com/news/223103-armenia-clash-russia-soldier/

Qin Yongzhang, "Utilizing Overseas Chinese Students' Role for Foreign Propaganda Related to Tibet" ["发挥海外中国留学生群体在涉藏外宣工作中的作用"], *International Communications*, May 2016.

Radin, Andrew, and Clint Reach, *Russian Views of the International Order*, Santa Monica, Calif.: RAND Corporation, RR-1826-OSD, 2017. As of April 18, 2019: https://www.rand.org/pubs/research_reports/RR1826.html

RBC, "Rassledovanie RBK: Kak 'Fabrika Trollej' Porabotala Na Vyborah v SShA," Vol. 11, No. 35, October 17, 2017. As of April 24, 2019: https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1

Regan, Tom, "Facebook Helped Blunt Russian Meddling in French Elections," *Engadget*, July 27, 2017. As of May 9, 2019: https://www.engadget.com/2017/07/27/facebook-helped-blunt-russian-meddling-in-french-elections/

"Reince Priebus Breaks Down Trump's Trip to the G-20 Summit," Fox News, July 9, 2017. As of May 6, 2019: http://www.foxnews.com/transcript/2017/07/09/reince-priebus-breaks-down-trumps-trip-to-g-20-summit.html

"Residents' Poll on State Defence Issues," Ministry of Defence of the Republic of Latvia, 2016.

Robertson, Matthew, "UK Firm Can't Figure Out Who Hired Them to Promote Chinese Propaganda Video," *Epoch Times*, October 19, 2015. As of April 30, 2019: https://www.theepochtimes.com/uk-firm-cant-figure-out-who-hired-them-to-promote-chinese-propaganda-video_1880606.html

Rogin, Josh, "China's Foreign Influence Operations Are Causing Alarm in Washington," *Washington Post*, December 10, 2017. As of April 19, 2019: https://www.washingtonpost.com/opinions/global-opinions/chinas-foreign-influencers-are-causing-alarm-in-washington/2017/12/10/98227264-dc58-11e7-b859-fb0995360725_story.html?utm_term=.de1e5488cde7

———, "How China Forces American Companies to Do Its Political Bidding," *Washington Post*, January 21, 2018. As of May 6, 2019: https://www.washingtonpost.com/opinions/global-opinions/how-china-forces-american-companies-to-do-its-political-bidding/2018/01/21/52a1d5a0-fd63-11e7-8f66-2df0b94bb98a_story.html

Rohac, Dalibor, "Cranks, Trolls and Useful Idiots," *Foreign Policy*, March 12, 2015.

Rosenberger, Laura, "Shredding the Putin Playbook," *Democracy Journal*, No. 47, Winter 2018. As of May 7, 2019: https://democracyjournal.org/magazine/47/shredding-the-putin-playbook/

Ross, Lee D., Mark R. Lepper, Fritz Strack, and Julia Steinmetz, "Social Explanation and Social Expectation: Effects of Real and Hypothetical Explanations on Subjective Likelihood," *Journal of Personality and Social Psychology*, Vol. 35, No. 11, 1977, pp. 817–829.

Ross, Robert S., and Jo Inge Bekkevold, eds., *China in the Era of Xi Jinping*, Washington, D.C.: Georgetown University Press, 2016.

RT, *About RT*, webpage, undated(a). As of February 5, 2018: https://www.rt.com/about-us/

———, homepage, undated(b). As of March 7, 2018: https://www.rt.com/

———, "RT Watched by 70mn Viewers Weekly, Half of Them Daily—Ipsos Survey," March 10, 2016. As of May 21, 2019: https://www.rt.com/news/335123-rt-viewership-ipsos-study/

———, "#StopMorganLie: Twitterati Disappointed in Freeman After His 'War with Russia' Video," September 20, 2017.

"RT's Propaganda Is Far Less Influential Than Westerners Fear," *The Economist*, January 19, 2017.

Ruan, Lotus, Jeffrey Knockel, Jason Q. Ng, and Masashi Crete-Nishihata, "One App, Two Systems: How WeChat Uses One Censorship Policy in China and Another Internationally," Citizen Lab, November 30, 2016. As of May 6, 2019: https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/

Ruffini, Patrick, "Why Russia's Facebook Ad Campaign Wasn't a Success," *Washington Post*, November 5, 2017.

Russian Federation, "National Security Strategy of the Russian Federation to 2020," Publication No. 537, May 12, 2009.

———, "Military Doctrine of the Russian Federation," December 26, 2014.

"Russian Propaganda Broadcast into Canadian Homes," CBC News, *The Weekly*, January 21, 2018. As of April 24, 2019:
http://www.cbc.ca/news/the-weekly/
the-weekly-russian-propaganda-broadcast-into-canadian-homes-1.4498536

"Russian Twitter Trolls Meddled in the Brexit Vote. Did They Swing It?" *The Economist*, November 23, 2017. As of May 8, 2019:
https://www.economist.com/news/britain/21731669-evidence-so-far-suggests-only-small-campaign-new-findings-are-emerging-all

"Russia's Top Lies About Ukraine. Part 1," blog post, *StopFake*, July 10, 2014a. As of April 24, 2019:
https://www.stopfake.org/en/russia-s-top-lies-about-ukraine-part-1/

"Russia's Top Lies About Ukraine. Part 2," blog post, *StopFake*, July 10, 2014b. As of April 24, 2019:
https://www.stopfake.org/en/russia-s-top-lies-about-ukraine-part-2/

Rutenberg, Jim, "RT, Sputnik and Russia's New Theory of War," *New York Times*, September 13, 2017.

"S.3274–Countering Foreign Propaganda and Disinformation Act," U.S. Senate, 2016. As of April 28, 2019:
https://www.congress.gov/bill/114th-congress/senate-bill/3274

Sanovich, Sergey, *Computational Propaganda in Russia: The Origins of Digital Misinformation*, Working Paper No. 2017.3, Computational Propaganda Research Project, University of Oxford, Oxford, UK, 2017. As of April 24, 2019:
http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Russia.pdf

Satell, Greg, "3 Ways to Use Social Network Analysis for Marketing," blog post, *DigitalTonto*, October 5, 2011. As of October 24, 2017:
http://www.digitaltonto.
com/2011/3-ways-to-use-social-network-analysis-for-marketing/

Sayfetdinov, Kh. I., "Information Operations on the Battlefield," *Military Thought,* Vol. 3, 2014.

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

Scholer, Gabriele, "Russia—A Threat to European Security? A View from Germany," Bertelsmann Stiftung, October 1, 2016. As of May 10, 2019:
http://www.bfna.org/research/
russia-a-threat-to-european-security-a-view-from-germany/

Schultheis, Emily, "What Went Right with the French Campaign Polls?" *The Atlantic*, May 13, 2017. As of May 9, 2019: https://www.theatlantic.com/international/archive/2017/05/what-went-right-with-the-french-election-polls/526326/

"Secretary General Marks Deployment of NATO Battlegroups During Visit to Latvia," press release, NATO, June 19, 2017. As of May 10, 2019: https://www.nato.int/cps/en/natohq/news_144993.htm

"Secured Borders Ad_Cultural _Metadata 1," U.S. House of Representatives Permanent Select Committee on Intelligence, 2017. As of April 19, 2019: https://democrats-intelligence.house.gov/uploadedfiles/secured_borders_cultural_metadata_1.pdf

Seddon, Max, "Documents Show How Russia's Troll Army Hit America," BuzzFeed News, June 2, 2014a. As of April 24, 2019: https://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america?utm_term=.vcnbmwvY5o#.hh2b3EKayD

———, "Russian TV Airs Clearly Fake Image to Claim Ukraine Shot Down MH17," BuzzFeed News, November 15, 2014b. As of April 24, 2019: https://www.buzzfeed.com/maxseddon/russian-tv-airs-clearly-fake-image-to-claim-ukraine-shot-dow?utm_term=.rvNp9DABRE#.myO7zJpEaG

Semichastny, V., and Lubomir Strougal, "Record of a Conversation About the Results of Cooperation and Further Coordination of Intelligence and Counterintelligence Activities Between the MVD of the Czechoslovak Socialist Republic and the KGB Under the USSR Council of Ministers," transcript, Wilson Center Digital Archive, June 12, 1962. As of April 19, 2019: http://digitalarchive.wilsoncenter.org/document/175926

Sethuraman, Raj, Gerard J. Tellis, and Richard A. Briesch, "How Well Does Advertising Work? Generalizations from Meta-Analysis of Brand Advertising Elasticities," *Journal of Marketing Research*, Vol. 48, No. 3, June 2011.

Shaik, Shabnam, "Improvements in Protecting the Integrity of Activity on Facebook," Facebook, April 12, 2017. As of May 9, 2019: https://www.facebook.com/notes/facebook-security/improvements-in-protecting-the-integrity-of-activity-on-facebook/10154323366590766/

Shambaugh, David, *China's Communist Party: Atrophy and Adaptation*, Washington, D.C.: Woodrow Wilson Center Press, 2009.

———, *China Goes Global: The Partial Power*, Oxford, UK: Oxford University Press, 2013.

———, "China's Soft-Power Push," *Foreign Affairs*, July 2015. As of May 6, 2019: https://www.foreignaffairs.com/articles/china/2015-06-16/china-s-soft-power-push

Shane, Scott, "The Fake Americans Russia Created to Influence the Election," *New York Times*, September 7, 2017a.

———, "These Are the Ads Russia Bought on Facebook in 2016," *New York Times*, November 1, 2017b.

"Share of Individuals in France Participating in Social Networks From 2011 to 2016," Statista, 2017.

Shekhovtsov, Anton, "Pro-Russian Network Behind the Anti-Ukrainian Defamation Campaign," blog post, *Anton Skekhovtsov's Blog*, February 3, 2014.

Sheng Peilin and Li Xue, "On 'Media Decapitation,'" *Journal of the PLA Nanjing Institute of Politics*, May 2006, pp. 114–117.

Shi Anbing and Liu Ying, "Three Steps to Advance the Construction of International Communications Power" ["三步走"推进国际传播力建设"], *People's Daily Online*, May 19, 2014. As of April 29, 2019:
http://opinion.people.com.cn/n/2014/0519/c1003-25034295.html

Shi-Kupfer, Kristin, "Governance Through Information Control," *China Monitor*, No. 26, Mercator Institute for China Studies, January 19, 2016.

Shi Lei and Xiao Tao, "Chen Quanguo, Lobsang Gyaincain Meet Media Delegation 'Beijing Internet Media Red Land—Tibet'; Wu Yingjie Present at Meeting," *Tibet Daily*, August 20, 2014.

Shirk, Susan, China: Fragile Superpower, Oxford, UK: Oxford University Press, 2007.

Shishkin, Phillip, and James Marson, "Ukraine Accuses Kremlin Agents of Coordinating Separatist Unrest," *Wall Street Journal*, April 20, 2014.

Shuster, Simon, "Inside Putin's On-Air Machine," *TIME*, March 5, 2015

Sides, John, and Jack Citrin, "How Large the Huddled Masses? The Causes and Consequences of Public Misperceptions About Immigrant Populations," presented at 2007 Annual Meeting of the Midwest Political Science Association, Chicago, Ill., 2007.

Silver, Nate, "It Wasn't Clinton's Election to Lose," 538.com, January 23, 2017. As of May 8, 2019:
http://fivethirtyeight.com/features/it-wasnt-clintons-election-to-lose/

Silverstein, Jason, "North Korea and China Also Interfered in U.S. Election, Reince Priebus Says," *New York Daily News*, July 9, 2017. As of May 6, 2019:
http://www.nydailynews.com/news/politics/
north-korea-china-interfered-u-s-election-priebus-article-1.3312905

Sinovets, Polina, and Bettina Renz, "Russia's 2014 Military Doctrine and Beyond, Threat Perceptions, Capabilities and Ambitions," Research Paper No. 117, Research Division, NATO Defense College, July 2015.

Skorobutov, Dmitry, "Ispoved' Propagandista. Chast' I. Kak Delajut Novosti na Gosudarstvennom TV," *The Insider*, June 9, 2017. As of April 24, 2019:
https://theins.ru/confession/59757/2

Skurnik, Ian, Carolyn Yoon, Denise C. Park, and Norbert Schwarz, "How Warnings About False Claims Become Recommendations," *Journal of Consumer Research*, Vol. 31, 2005, pp. 713–724.

Smith, Aaron, and Monica Anderson, "Social Media Use in 2018," Pew Research Center, March 1, 2018. As of May 8, 2019: http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/

Smith, Alexander, "British PM Theresa May Says Russia Seeks to 'Weaponize' Information," NBC News, November 14, 2017.

Smyth, Jamie, "China's $10bn Propaganda Push Spreads Down Under," *Financial Times*, June 9, 2016. As of May 6, 2019: https://www.ft.com/content/324d82c4-2d60-11e6-a18d-a96ab29e3c95

"Social Media Usage in the United Kingdom," Statista Dossier, August 2017.

"Social Network Usage in France," Statista Dossier, 2017.

Soldatov, Andrei, and Irina Borogan, *The Red Web*, New York: Public Affairs, 2015.

Song Shunan, "Gather the Abroad Students to Strengthen the Dream of National Revival—A Report of the Speech of General Secretary Xi Jinping Learning the 100th Anniversary" ["凝聚留学人员力量共筑民族复兴梦想 - 欧美同学会学习习近平总书记在百年庆典上的讲话纪实"], *China United Front*, February 2014.

Song Suxia, "Small WeChat and Big Family: Hebi City Builds WeChat Platform for United Front Work" [" '小' 微信 '大' 家庭——鹤壁市委统战部建立统一战线微信平台"], *China United Front*, May 2013.

"Sorbonne Speech of Emmanuel Macron—Full Text/English Version," blog post, *Ouest France*, September 26, 2017. As of May 8, 2019: http://international.blogs.ouest-france.fr/archive/2017/09/29/macron-sorbonne-verbatim-europe-18583.html

Sørensen, Camilla T. N., "The Significance of Xi Jinping's 'China Dream' for Chinese Foreign Policy: From 'Tao Guang Yang Hui' to 'Fen Fa You Wei,'" *Journal of Chinese International Relations*, Vol. 3, No. 1, 2015, pp. 53–73

"Soviet Use of Declassified Documents," memorandum from A. Denis Clift to Secretary of State Henry Kissinger, National Security Council Files, President Gerald R. Ford Library, October 8, 1975.

Spencer, David, "Is the Incense Ban Furor More Than Just Simple Fake News?" *Taiwan News*, July 27, 2017.

Sputnik, *About Us*, webpage, undated. As of February 5, 2018: https://sputniknews.com/docs/about/index.html

Stelzenmüller, Constanze, "The Impact of Russian Interference on Germany's 2017 Elections," testimony before the U.S. Senate Select Committee on Intelligence, June 28, 2017.

Stember, Nick, "The Road to Rejuvenation: The Animated Xi Jinping," in Gloria Davies, Jeremy Goldkorn, and Luigi Tomba, eds., *China Story Yearbook 2015: Pollution*, Canberra: ANU Press, 2016. As of April 30 2019: http://press-files.anu.edu.au/downloads/press/n2095/pdf/introduction_forum_stember.pdf

Stevenson, Alexandra, "Facebook Blocks Chinese Billionaire Who Tells Tales of Corruption," *New York Times*, October 1, 2017. As of April 29, 2019: https://www.nytimes.com/2017/10/01/business/facebook-china-guo-wengui.html

Stokes, Bruce, *NATO's Image Improves on Both Sides of Atlantic*, Pew Research Center, May 23, 2017. As of May 7, 2019: http://assets.pewresearch.org/wp-content/uploads/sites/2/2017/05/26170755/Pew-Research-Center-NATO-Report-FINAL-May-23-2017.pdf

Stokes, Mark, and Russell Hsiao, "The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics," Project 2049 Institute, October 14, 2013.

Stone, Jessica, "Chinese-Americans Voters Mobilize Ahead of US Election," CGTV, November 1, 2016. As of May 6, 2019: https://america.cgtn.com/2016/11/01/chinese-americans-voters-mobilize-ahead-of-us-election

Storrs, Carina, "How Effective Are Misinformation Campaigns to Manipulate Public Opinion?" *Scientific American*, September 29, 2017.

Stretch, Colin, General Counsel, Facebook, "Hearing Before the United States Senate Select Committee on Intelligence," testimony, November 1, 2017. As of April 25, 2019: https://www.intelligence.senate.gov/sites/default/files/documents/os-cstretch-110117.pdf

Strzelecki, Marek, and Ewa Krukowska, "EU Sanctions Risk for Poland Rises on Democratic Backsliding," Bloomberg, December 20, 2017. As of May 10, 2019: https://www.bloomberg.com/news/articles/2017-12-20/eu-proposes-polish-sanctions-option-over-democratic-backsliding

"Student Heckled by Chinese Netizens After Praising US Fresh Air and Free Speech," *Study International*, May 24, 2017. As of May 5, 2019: https://www.studyinternational.com/news/student-heckled-chinese-netizens-praising-us-fresh-air-free-speech/

"Successfully Do Foreign Propaganda Work for the 90th Anniversary of the Party's Founding: Fully Show Our Party's Positive Image" ["做好建党90周年对外宣传工作 充分展示我党良好形象"], *International Communications*, January 2011.

Suls, Rob, "Share of Democrats Calling Russia 'Greatest Danger' to U.S. Is at Its Highest Since End of Cold War," Pew Research Center, April 20, 2017. As of May 7, 2019:
http://www.pewresearch.org/fact-tank/2017/04/20/share-of-democrats-calling-russia-greatest-danger-to-u-s-at-its-highest-since-end-of-cold-war/

Sun Ming, "International Public Opinion on This Year's 'Two Congresses'" ["今年"两会"的国际舆论关切"], *International Communications*, March 2013.

Sun Tzu, *Art of War*, military treatise, circa fifth century BCE.

Swaine, Michael D., "China's Assertive Behavior, Part One: On 'Core Interests,'" *China Leadership Monitor*, No. 34, September 2010.

Swift, Art, "Americans' Trust in Mass Media Sinks to New Low," press release, Gallup, September 14, 2016. As of May 7, 2019:
http://www.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx

———, "Democrats' Confidence in Mass Media Rises Sharply from 2016," press release, Gallup, September 21, 2017. As of May 7, 2019:
http://news.gallup.com/poll/219824/democrats-confidence-mass-media-rises-sharply-2016.aspx

Taber, Charles S., and Milton Lodge, "Motivated Skepticism in the Evaluation of Political Beliefs," *American Journal of Political Science*, Vol. 50, No. 3, 2006, pp. 755–769.

"Table for Chinese Foreign Propaganda Pages for News on Facebook" ["Facebook中国外宣专页列表之新闻类"], Medium, September 17, 2017. As of May 6, 2019:
https://medium.com/@fanghua/facebook%E4%B8%AD%E5%9B%BD%E5%A4%96%E5%AE%A3%E4%B8%93%E9%A1%B5%E5%88%97%E8%A1%A8%E4%B9%8B%E6%96%B0%E9%97%BB%E7%B1%BB-a75032a98213

"Table of Chinese Foreign Propaganda Accounts for News on Twitter" ["Twitter中国外宣帐号列表之新闻类"], Medium, November 12, 2017. As of May 6, 2019:
https://medium.com/@fanghua/twitter%E4%B8%AD%E5%9B%BD%E5%A4%96%E5%AE%A3%E5%B8%90%E5%8F%B7%E5%88%97%E8%A1%A8%E4%B9%8B%E6%96%B0%E9%97%BB%E7%B1%BB-9c1f10eb4231

"Table of Chinese Foreign Propaganda Accounts on Instagram" ["Instagram中国外宣帐号列表"], Medium, December 19, 2017. As of May 6, 2019:
https://medium.com/@fanghua/instagram%E4%B8%AD%E5%9B%BD%E5%A4%96%E5%AE%A3%E5%B8%90%E5%8F%B7%E5%88%97%E8%A1%A8-8245c69e6891

Tahroor, Ishaan, "China's 'Long Arm' of Influence Stretches Ever Further," *Washington Post*, December 14, 2017.

"Taiwan Cuts 18 Pct Interest in Civil Service Pension Reform Bill," Reuters, June 27, 2017.

"Taiwan's Taoists Protest Against Curbs on Incense and Firecrackers," BBC News, July 23, 2017.

"Taking on Taiwan's Ruinous and Partisan Pension System," *The Economist*, May 18, 2017.

Tan, Chenhao, Vlad Niculae, Cristian Danescu-Niculescu-Mizil, and Lillian Lee, "Winning Arguments: Interaction Dynamics and Persuasion Strategies in Good-Faith Online Discussions," International World Wide Web Conference Committee, presented at WWW2016, Montreal, Canada, April 11–15, 2016. As of April 16, 2019:
https://arxiv.org/pdf/1602.01103v1.pdf

Tan Feng, "Why China Became the 'Sacrificial Lamb' of U.S. Elections" ["中国为何成为美国大选的'替罪羊'"], *International Communications*, September 2016.

Tang Dashan, "Tibet Should Build a Major External Propaganda Structure," *Tibet Daily*, September 14, 2013.

Tatlow, Didi Kirsten, "China Reaches into the Heart of Europe," *New York Times*, January 25, 2018. As of April 28, 2019:
https://www.nytimes.com/2018/01/25/opinion/china-germany-tech-manufacturing.html

"Telling the Untold," webpage, Sputnik, undated. As of April 24, 2019:
https://sputniknews.com/files/newswires_sputnik.pdf

"Temnik—the Kremlin's Route to Media Control," *EU vs Disinfo*, March 29, 2017. As of April 24, 2019:
https://euvsdisinfo.eu/temnik-the-kremlins-route-to-media-control/

"The Vote to Leave the EU," *British Social Attitudes*, Vol. 34, National Centre for Social Research, undated. As of May 8, 2019:
http://www.bsa.natcen.ac.uk/media/39149/bsa34_brexit_final.pdf

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

Thorson, Emily, "Belief Echoes: The Persistent Effects of Corrected Misinformation," *Political Communication*, Vol. 33, No. 3, 2016, pp. 460–480.

"Tracking Ghostnet: Investigating a Cyber Espionage Network," Citizen Lab, March 28, 2009. As of May 5, 2019:
https://citizenlab.ca/2009/03/tracking-ghostnet-investigating-a-cyber-espionage-network/

Tran, Pierre, "France Adds $2B to Defense Budget, Moving Closer to NATO Spending Target," *Defense News*, September 27, 2017. As of May 9, 2019:
https://www.defensenews.com/global/europe/2017/09/27/france-adds-2b-to-2018-defense-budget/

Tsoi, Grace, "Why Katy Perry and Gigi Hadid Were Missing from Shanghai's Victoria's Secret," BBC News, November 20, 2017.

Turak, Natasha, "Estonia Has No Doubts on Trump's Commitment to NATO, Says Prime Minister Juri Ratas," CNBC, January 26, 2018. As of May 7, 2019: https://www.cnbc.com/2018/01/26/estonia-has-no-doubts-on-trumps-nato-commitment-prime-minister.html

"Twenty-Five EU States Sign PESCO Defense Pact," *Deutsche Welle*, December 11, 2017. As of May 9, 2019: http://www.dw.com/en/twenty-five-eu-states-sign-pesco-defense-pact/a-41741828

"UK and France Commit to New Defence Cooperation," press release, United Kingdom Ministry of Defence, January 18, 2018. As of May 8, 2019: https://www.gov.uk/government/news/uk-and-france-commit-to-new-defence-cooperation

"Ukraine Bans Russian TV Channels for Airing War 'Propaganda,'" Reuters, August 19, 2014.

U.S. Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent U.S. Elections," unclassified assessment, January 6, 2017. As of May 7, 2019: https://www.dni.gov/files/documents/ICA_2017_01.pdf

U.S. District Court for the District of Columbia, "United States of America v. Internet Research Agency LLC, [et. al]," filed February 16, 2018.

U.S. DNI—See U.S. Director of National Intelligence.

U.S. House of Representatives Permanent Select Committee on Intelligence, "HSPCI Minority Open Hearing Exhibits," webpage, undated. As of April 19, 2019: https://intelligence.house.gov/hpsci-11-1/hpsci-minority-open-hearing-exhibits.htm

U.S. House of Representatives Permanent Select Committee on Intelligence, *Soviet Active Measures*, Washington, D.C.: Government Printing Office, 1982.

U.S. House of Representatives Permanent Select Committee on Intelligence, *Report on Russian Active Measures*, March 22, 2018.

U.S. House of Representatives Permanent Select Committee on Intelligence, Subcommittee on Oversight, *Soviet Covert Action (The Forgery Offensive)*, Washington, D.C.: U.S. Government Printing Office, 1980.

U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, Washington, D.C., November 2010. As of April 19, 2019: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

———, *Information Operations*, Joint Publication 3-13, Washington, D.C., November 27, 2012, incorporating Change 1, November 20, 2014.

U.S. Senate, Committee on the Judiciary, "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions," subcommittee hearing video, Washington, D.C., October 31, 2017. As of November 22, 2017: https://www.judiciary.senate.gov/meetings/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions

U.S. Senate, Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, Minority Staff Report, January 10, 2018. As of May 8, 2019: https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

Valášek, Tomáš, "Trump's Relationship with NATO, One Year into His Presidency," Carnegie Europe, December 28, 2017. As of May 7, 2019: http://carnegieeurope.eu/2017/12/28/trump-s-relationship-with-nato-one-year-into-his-presidency-pub-75153

Vice, Margaret, "Publics Worldwide Unfavorable Toward Putin, Russia," Pew Research Center, August 16, 2017.

"Victoria 'F*ck the EU' Nuland Leaves Her Post at the US State Department," Sputnik, January 27, 2017.

Waddell, Kaveh, "Kremlin-Sponsored News Does Really Well on Google," *The Atlantic*, January 25, 2017.

Wagner, John, and Karoun Demirjian, "Trump Blames Congress for 'All-Time' Low Relationship with Russia; Lawmakers Push Back," *Washington Post*, August 3, 2017. As of May 7, 2019: https://www.washingtonpost.com/news/post-politics/wp/2017/08/03/trump-blames-congress-for-all-time-low-relationship-with-russia/?utm_term=.37fcbf03f08b

Wakabayashi, Daisuke, and Nicholas Confessore, "Russia's Favored Outlet Is an Online News Giant. YouTube Helped," *New York Times*, October 23, 2017.

Walker, Christopher, "A New Era of Competition," Konrad Adenauer Stiftung *International Reports*, No. 2, 2017. As of December 10, 2017: http://www.kas.de/wf/en/33.49464/

Waltzman, Rand, "The Weaponization of the Information Environment," Defense Technology Program brief, American Foreign Policy Council, September 2015.

———, "The Weaponization of Information: The Need for Cognitive Security," testimony before the Committee on Armed Services, Subcommittee on Cybersecurity, U.S. Senate, April 27, 2017, Santa Monica, Calif.: RAND Corporation, CT-473, 2017. As of April 19, 2019: https://www.rand.org/pubs/testimonies/CT473.html

Wakabayashi, Daisuke, and Nicholas Confessore, "Russia's Favored Outlet Is an Online News Giant. YouTube Helped." *New York Times*, October 23, 2017.

Wan, William, "In China, Soviet Union's Failure Drives Decisions on Reform," *Washington Post*, March 23, 2013. As of April 28, 2019: https://www.washingtonpost.com/world/asia_pacific/in-china-soviet-unions-failure-drives-decisions-on-reform/2013/03/23/9c090012-92ef-11e2-ba5b-550c7abf6384_story.html

Wang, Amy B., "Bowing to Pressure from China, Mercedes-Benz Apologizes for Quoting the Dalai Lama in Ad," *Washington Post*, February 6, 2018. As of May 5, 2019: https://www.washingtonpost.com/news/worldviews/wp/2018/02/06/bowing-to-pressure-from-china-mercedes-benz-apologizes-for-quoting-the-dalai-lama-in-ad

Wang, Amy X., "China's Government Has a Bizarre Official Rap Song, Featuring President Xi Jinping," *Quartz*, December 31, 2015.

Wang, Andi, "Meet Some of the Chinese Americans Voting for Trump," PBS, August 20, 2016. As of May 6, 2019: https://www.pbs.org/newshour/politics/chinese-americans-diverge-political-views-converge-addressing-low-voter-turnout

Wang Bin and Chen Yu, "Political Figures' Campaign Concept as Shown Through Social Media—Taking Hilary and Trump's Instagram Accounts as Example" ["政治人物在社交媒体上的竞选理念呈现—以希拉里和特朗普的Instagram账号为例"], *International Communications*, September 2016, pp. 62–65.

Wang Chen and Zhou Ting, "Three Problems for Building and Communicating National Leader's Public Image" ["国家领导人公共形象的构建与传播三问"], *International Communications*, June 2015.

Wang, Esther, "Conservative Chinese Americans Are Mobilizing, Politically and Digitally," *Pacific Standard Magazine*, October 11, 2017. As of May 6, 2019: https://psmag.com/social-justice/conservative-chinese-americans-are-mobilizing-politically-and-digitally

Wang Jichang, "Main Experience of Russia's Military Operations in Syria," *China Military Science*, March 2016, pp. 119–126.

Wang Pan, "Casting a New 'Window to China'—Explorations and Thoughts on Shenzhen's Foreign Propaganda Work in the New Era" ["铸造新的"中国窗口"—新时期深圳特区外宣工作探索与思考"], *International Communications*, February 2012.

Wang, Yaqiu, "The Business of Censorship: Documents Show How Weibo Filters Sensitive News in China," blog post, Committee to Protect Journalists, March 3, 2016. As of April 29, 2019: https://cpj.org/blog/2016/03/the-business-of-censorship-documents-show-how-weib.php

Wardle, Claire, "Fake News: It's Complicated," *First Draft*, February 16, 2017.

Watson, Kathryn, "How Did WikiLeaks Become Associated with Russia?" CBS News, November 15, 2017.

Way, Lucan Ahmad, and Adam Casey, "Is Russia a Threat to Western Democracy? Russian Intervention in Foreign Elections, 1991–2017," draft memo prepared for conference on Global Populisms as a Threat to Democracy? Stanford University, November 3–4, 2017. As of May 28, 2019:
https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/is_russia_a_threat_to_western_democracy_russian_intervention_in_foreign_elections_1991-2017_.pdf

———, "Russia Has Been Meddling in Foreign Elections for Decades. Has It Made a Difference?" *Washington Post*, January 8, 2018.

Weaver, Kimberlee, "Inferring the Popularity of an Opinion from Its Familiarity: A Repetitive Voice Can Sound Like a Chorus," *Journal of Personality and Social Psychology*, Vol. 92, No. 5, 2007, pp. 821–833.

Webster, C. M., and P. D. Morrison, "Network Analysis in Marketing," *Australian Marketing Journal*, Vol. 12, pp. 8–18, 2004.

Werkhäuser, Nina, "German Military Spending Gets Political," *Deutsche Welle*, August 8, 2017. As of May 10, 2019:
http://www.dw.com/en/german-military-spending-gets-political/a-40016299

Whitson, Jennifer A., and Adam D. Galinsky, "Lacking Control Increases Illusory Pattern Perception," *Science*, Vol. 322, 2008.

Wikipedia, "Sputnik (news agency)," article, 2018. As of February 5, 2018:
https://en.wikipedia.org/wiki/Sputnik_(news_agency)

Wilson, Andrew, *Virtual Politics: Faking Democracy in the Post-Soviet World*, New Haven, Conn.: Yale University Press, 2005.

Wong, Chun Han, "The Foreigner Advising Beijing on Propaganda," blog post, *Wall Street Journal*, May 13, 2016. As of April 30, 2019:
https://blogs.wsj.com/chinarealtime/2016/05/13/the-foreigner-advising-beijing-on-propaganda/

Wong, Edward, "Chinese Warship May Be Nearly Ready," *New York Times*, April 7, 2011.

———, "China's President Lashes out at Western Culture," *New York Times*, January 3, 2012. As of April 28, 2019:
http://www.nytimes.com/2012/01/04/world/asia/chinas-president-pushes-back-against-western-culture.html

Woolley, Samuel C., and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," in Samuel Woolley and Philip N. Howard, eds., Working Paper 2017.11, Oxford, UK: Project on Computational Propaganda, 2017. As of August 19, 2019:
http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf

Wu Feng and Li Yaofei, "The Latest Status and Operation Model of Overseas Anti-China Media and Countermeasures" ["境外反华媒体的最新态势，及应对策略"], *Journal of Intelligence*, March 2017, pp. 36–42.

Wu Rui, "Be on Guard Against Other Kinds of Soft Warfare," *Military Correspondent*, November 2013, pp. 53–54.

Wu Xu, "Trump's 'Twitter Diplomacy': China's International Communications Facing New Challenges" ["特朗普的"推特外交":中国对外传播面临的新挑战"], *International Communications*, February 2017.

Wu, Zaiping, "The Social Challenges and Responses to New Media" ["新媒体的社会挑战与应对"], *Journal of the Party School of the Central Committee of the C.P.C.*, October 2012.

Wyler, Grace, "What Do Chinese-Americans Think of Trump's Tough China Talk? We Asked Them," *Los Angeles Daily News*, January 4, 2017. As of May 6, 2019:
https://www.dailynews.com/2017/01/04/what-do-chinese-americans-think-of-trumps-tough-china-talk-we-asked-them/

"Xi Calls for Persistently Pursuing Chinese Dream of National Rejuvenation," *China Daily*, September 26, 2017.

Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," speech to the 19th National Congress of the Communist Party of China, via Xinhua, October 18, 2017. As of April 28, 2019:
http://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm

Xia, C., S. Guha, and S. Muthukrishnan, "Targeting Algorithms for Online Social Advertising Markets," IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), San Francisco, Calif., August 2016.

Xiang Debao, "Rules, Characteristics and Guidance Strategy for Public Debate over Tibet in International Social Media and the Public Opinion Struggle" ["国际自媒体涉藏舆情及舆论斗争的规律、特征及引导策略"], *Journal of Intelligence*, Vol. 35, No. 5, 2016, pp. 20–26.

Xiang Debao and Zhang Renwen, "Characteristics of Public Opinions About China on International Social Media in 2012" ["2012国际自媒体涉华舆情特征"], *Journal of Intelligence*, Vol. 32, No. 8, 2013, pp. 31–34.

Xiao Fei and Caichan Minbao, "Analysis of Online Public Opinion Dangers and Online Public Opinion Guidance Countermeasures for Overseas Border Conflicts" ["涉外边境冲突的网络舆情风险与舆论引导对策探析"], *International Communications*, August 2016.

Xiao Lili, "Challenges and Public Opinion Responses for China's National Image in Africa" ["中国国家形象在非洲面临的挑战及舆论应对"], *International Communications*, August 2011.

Xiong Yuhua, "To Seek Advantages and Avoid Disadvantages and Make Good Use of the 'Double-Edged Sword' of Internet—Cadres, Staff Members, and Workers of Our Region's Propaganda and Cultural System Conscientiously Study the Spirit of the Sixth Plenary Session of the 17th CPC Central Committee," *Tibet Daily*, October 24, 2011.

"Xi's Secret Economic Weapon: Overseas Chinese," *Nikkei Asian Review*, April 3, 2017.

Xu Lei, "What Can We Learn from Russia Today?" ["我们向"今日俄罗斯"学什么? "], *People's Daily Overseas Edition*, September 19, 2014. As of April 29, 2019: http://paper.people.com.cn/rmrbhwb/html/2014-09/19/content_1479579.htm

Xu, Beina, and Eleanor Albert, "Media Censorship in China," Council on Foreign Relations, February 17, 2017 As of April 29, 2019: https://www.cfr.org/backgrounder/media-censorship-china

Xu Hua, "How Did Putin Create the Image of a Leader" ["普京如何塑造领袖形象"], *International Communications*, March 2015.

Xu Shaomin, "Insights into the Impact of the Proliferation of Fake News in the United States and Europe on China's Public Diplomacy" ["欧美假新闻泛滥对我国开展公共外交的启"], *Public Diplomacy*, Vol. 2, 2017.

Xu Xiujun, "Foreign Communication of Chinese Global Governance Ideas Under Counter-Globalization Trend" ["逆全球化思潮下中国全球治理观的对外传播"], *International Communications*, March 2017.

Xuecun, Murong, "The New Face of Chinese Propaganda," *New York Times*, December 20, 2013.

Yan Liang, "Global Changes and Foreign Communication Responses After Trump's Taking Office" ["特朗普上任后的世界变局与对外传播应对"], *International Communications*, February 2017.

Yan Xuetong, "From 'Keeping a Low Profile' to 'Striving for Achievement,'" *Chinese Journal of International Politics*, Vol. 7, No. 2, 2014, pp. 153–184.

Yang Yunsheng, "Research on Foreign Propaganda for the China Dream" ["中国梦海外宣讲研究"], *New Orient*, June 2016.

Yao Yao, "The West's View of China, or the World's View of China? New Thinking on Building China's Global Image" ["西方的中国观,还是世界的中国观?——中国建构国际形象的新思路"], *International Communications*, July 2014.

Ye Xiaoli and Gu Haoyu, "The Analysis for Influence Factors of Chinese-American Political Participation: Take the Protesting Action to the Insulting Chinese for an Example" ["当代美国华人政治参与影响因素分析: 以抗议ABC辱华行动为例"], *Overseas Chinese Journal of Bagui*, June 2015, pp. 13–20.

———, "The Factors on Election Campaign of Modern Chinese-American: Based on the Analyses of Sustainability" ["当代美国华人竞选影响因素: 基于可持续性的分析"], *Overseas Chinese Journal of Bagui*, September 2017, pp. 31–38.

Yi Changjun, "Research on New Overseas Chinese Associations and the Construction of 'Soft Power'" ["海外新华侨华人社团与国家 '软实力' 建设研究"], *Journal of Huaqiao University*, May 2016.

Ying Yu Lin, "China's Hybrid Warfare and Taiwan," *The Diplomat*, January 13, 2018.

Young, C. W. Bill, "Soviet Active Measures in the United States—An Updated Report by the FBI," U.S. Congressional Record, December 9, 1987.

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.

Yu Xiaoqing, "The Growth of China's Outreach Flagship Media: 20 Years of Transformation of an English Anchorwoman" ["中国外宣旗舰媒体成长记：一位英文女主播的20年蜕变"], *The Paper*, April 1, 2017. As of May 6, 2019: http://www.thepaper.cn/newsDetail_forward_1652275

Yuhas, Alan, "Russian Propaganda over Crimea and the Ukraine: How Does It Work?" *The Guardian*, March 17, 2014.

Zhai Huixia, Xie Lianghong, and Yu Yunquan, "New Perspective on Western Research on 'China Model' Since Global Financial Crisis" ["国际金融危机以来西方对 '中国模式' 研究的新视角"], *International Communications*, January 2012.

Zhang Leilei, "Actively Use Overseas Social Media for Military Foreign Propaganda" ["积极利用海外社交媒体参与军事外宣"], *Military Correspondent*, August 2016, pp. 59–60.

Zhao Qinghai, "New Western Reflections on Globalization" ["西方对全球化的新反思"], *International Communications*, January 2008.

Zhao Liangying and Xu Xiaolin, "Actively Build China's National Strategic Communication System" ["积极构建中国国家战略传播体系"], *Media Outpost*, September 2016.

Zhao Mingwu, "Messaging One Belt One Road Strategy: Problems and Responses" ["'一带一路'的政策传播:问题与应对"], *International Communications*, April 2016.

Zhong Zhigang, "New Explorations on Military Propaganda Toward Taiwan Under the Goal of Building a Strong Military," *Military Correspondent*, November 2013.

Zhou Xiang and Han Weizheng, "Using Image Social Media to Improve China's International Communication Power" [利用图像社交媒体提升中国国际传播力研究"], *Academic Journal of Zhongzhou*, March 2017.

Zhou Xinyu and Feng Bo, "Foreign Communication of Chinese Values Under the Waves of Populism in the West" ["西方民粹主义浪潮下的中国价值观对外传播"], *International Communications*, February 2017.

Zhou Yang, "Examination of Social Media Actions in U.S. Strikes on ISIS" ["美军打击ISIS的社交媒体行动探索"], *Military Correspondent*, July 2017.

Zhu Ningning, "An Analysis of Russia's Unfolding of Media Warfare Tactics amid the Turbulent Political Situation in Ukraine," *Military Correspondent*, May 2014.

Zhu Yuping, "Factors and Inspiration for Public Opinion Warfare Under Informationized Conditions," *Military Art Journal*, October 2003, pp. 29–30.

Zu, Stephanie, "揭秘特朗普最大华裔助选团 组织集资全靠微信," Sohu, November 6, 2016. As of May 6, 2019: http://news.sohu.com/20161106/n472416900.shtml

The role of information warfare in global strategic competition has become much more apparent in recent years. Today's practitioners of what this report's authors term *hostile social manipulation* employ targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, distribution of rumors and conspiracy theories, and other tools and approaches to cause damage to the target state. These emerging tools and techniques represent a potentially significant threat to U.S. and allied national interests. This report represents an effort to better define and understand the challenge by focusing on the activities of the two leading authors of such techniques—Russia and China. The authors conduct a detailed assessment of available evidence of Russian and Chinese social manipulation efforts, the doctrines and strategies behind such efforts, and evidence of their potential effectiveness. RAND analysts reviewed English-, Russian-, and Chinese-language sources; examined national security strategies and policies and military doctrines; surveyed existing public-source evidence of Russian and Chinese activities; and assessed multiple categories of evidence of effectiveness of Russian activities in Europe, including public opinion data, evidence on the trends in support for political parties and movements sympathetic to Russia, and data from national defense policies. The authors find a growing commitment to tools of social manipulation by leading U.S. competitors. The findings in this report are sufficient to suggest that the U.S. government should take several immediate steps, including developing a more formal and concrete framework for understanding the issue and funding additional research to understand the scope of the challenge.

NATIONAL DEFENSE RESEARCH INSTITUTE

www.rand.org

$45.00

ISBN-10 1-9774-0260-7
ISBN-13 978-1-9774-0260-8

RR-2713-OSD