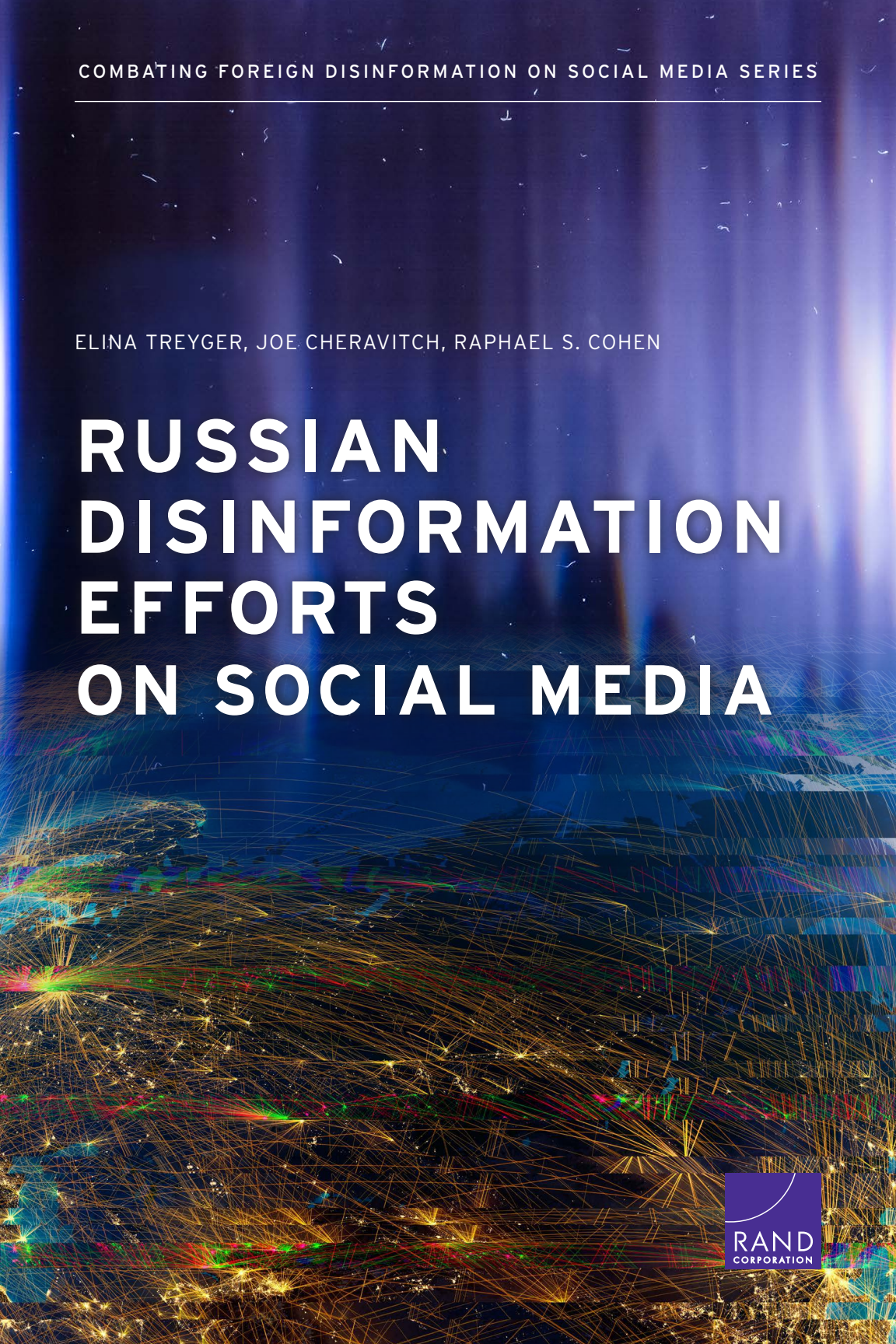
COMBATING FOREIGN DISINFORMATION ON SOCIAL MEDIA SERIES

ELINA TREYGER, JOE CHERAVITCH, RAPHAEL S. COHEN

# RUSSIAN DISINFORMATION EFFORTS ON SOCIAL MEDIA



RAND CORPORATION

For more information on this publication, visit **www.rand.org/t/RR4373z2**.

### About RAND

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

### Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.


Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0968-3

*Cover: golubovy/Adobe Stock; Anton Balazh/Adobe Stock.*

### Limited Print and Electronic Distribution Rights

# Preface

How are countries using social media—particularly, disinformation campaigns—to influence the competitive space? How have governments, the private sector, and civil society responded to this threat? What more can be done? And what do these developments mean for future U.S. Air Force and the joint force training and operations?[1] In this report, we attempt to answer these questions as part of a broader study of disinformation campaigns on social media and the implications of those campaigns for great-power competition and conflict. The other volumes in this series are:

- Raphael S. Cohen, Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwille, Elina Treyger, and Nathan Vest, *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*, Santa Monica, Calif.: RAND Corporation, RR-4373/1-AF, 2021
- Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, *Chinese Disinformation Efforts on Social Media*, Santa Monica, Calif.: RAND Corporation, RR-4373/3-AF, 2021
- Raphael S. Cohen, Alyssa Demus, Michael Schwille, Nathan Vest, *U.S. Efforts to Combat Foreign Disinformation on Social Media*, Santa Monica, Calif.: RAND Corporation, 2021, Not available to the general public.

[1] This report was completed before the creation of the U.S. Space Force and therefore uses the name "U.S. Air Force" to refer to both air and space capabilities.

The research reported here was commissioned by the Air Force Special Operations Command and conducted within the Strategy and Doctrine Program of RAND Project AIR FORCE as part of the fiscal year 2019 project "Bringing Psychological Operations and Military Information Support Operations into the Joint Force: Counterinformation Campaigns in the Social Media Age," which was designed to assist the Air Force in evaluating the threat of foreign influence campaigns on social media and assessing possible Air Force, joint force, and U.S. government countermeasures.

This report should be of value to the national security community and interested members of the public, especially those with an interest in how global trends will affect the conduct of warfare. This research was completed in September 2019, before the February 2022 Russian invasion of Ukraine. It has not been subsequently revised.

RAND is committed to ethical and respectful treatment of RAND research participants and complies with all applicable laws and regulations, including the *Federal Policy for the Protection of Human Subjects*, also known as the "Common Rule." The research described in this report was screened and, if necessary, reviewed by RAND's Human Subjects Protection Committee, which serves as RAND's institutional review board (IRB) charged with ensuring the ethical treatment of individuals who are participants in RAND projects through observation, intervention, interaction, or use of data about them. RAND's Federalwide Assurance (FWA) for the Protection of Human Subjects (FWA00003425, effective until June 22, 2023) serves as our assurance of compliance with federal regulations.

The views of any unnamed sources are solely their own and do not represent the official policy or position of any department or agency of the U.S. government.

### RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alterna-

tives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Strategy and Doctrine; Force Modernization and Employment; Resource Management; and Workforce, Development, and Health. The research reported here was prepared under contract FA7014-16-D-1000.

Additional information about PAF is available on our website: www.rand.org/paf

This report documents work originally shared with the DAF in October 2019. The draft report, issued on November 13, 2019, was reviewed by formal peer reviewers and DAF subject-matter experts.

# Contents

# Figures and Tables

## Figures



## Tables

# Summary

## Issue

Russia is waging wide-reaching information warfare with the Western world. A significant part of its ongoing efforts takes place on social media, which Russia has employed to spread disinformation and to interfere with the internal politics of other countries, targeting varied audiences, including the U.S. military. The impact of Russia's social media activities on specific outcomes (such as votes or policy decisions) is uncertain to date, but Russian information warfare threatens to undermine the integrity of democratic processes, erode the belief in factual truths, and cause concrete harm with well-timed or sophisticated disinformation. We sought to help the U.S. Air Force (USAF) and the joint force more effectively respond to this threat.[1]

## Approach

We sought to better understand Russia's disinformation on social media and generate recommendations to better meet and counter this evolving threat. We relied on an analysis of Russian military literature, investigative efforts, official reports, academic and policy literature, media reporting, and expert interviews. We also conducted a case study in Ukraine, interviewing a variety of key experts in the Ukrai-

[1] This report was completed before the creation of the U.S. Space Force and therefore uses the name "U.S. Air Force" to refer to both air and space capabilities.

nian government and in the nongovernmental sector who are involved in confronting Russian information warfare.

## Conclusions

We conclude that:

- Russia views social media as a double-edged sword, at once harboring anxieties about social media's potential to undermine Russia's security and recognizing its advantages as a low-cost and potentially highly effective weapon of asymmetric warfare.
- Russia's use of social media outside the former Soviet Union picked up most markedly in 2014, suggesting that this behavior is, in part, a response to the West's response to the Ukraine conflict.
- The Russian disinformation machine has been neither well organized nor especially well resourced (contrary to some implications in popular media), and the impact of Russian efforts on the West has been uncertain.
- However, even with relatively modest investments, Russian social media activity has been wide reaching, spreading disinformation and propaganda to sizable audiences across multiple platforms.
- Russia appears to view its own activity as successful, so the threat posed by this activity is likely to persist—and, potentially, to grow.
- Western countermeasures have raised awareness of Russian activities, but their impact on Russia's efforts has been uncertain, and Russia appears undeterred.
- Moreover, Russia's social media–based information warfare is evolving. Russia is likely to continue pursuing some of the same goals and targets but is developing more-sophisticated tactics and techniques aimed at circumventing Western countermeasures.

## Recommendations

The Air Force and/or the joint forces should consider the following:

- USAF should be mindful of Russia's perceptions when deploying assets related to military information support operations or psychological operations in areas that Russia perceives to be of strategic importance or interest.
- The joint force should adopt appropriate monitoring processes to improve detection of Russian information efforts of greatest concern to the U.S. Department of Defense (e.g., those targeting members of U.S. military and associates, U.S. and North Atlantic Treaty Organization operations).
- The joint force should take measures to reduce overattribution of disinformation on social media to Russia.
- USAF and the joint force should train troops and their family members to expect and recognize disinformation and other information manipulation by Russian actors.
- USAF and the joint force should develop policy regarding social media platforms and devices and should train and educate troops about vulnerabilities related to sharing personal data online.
- USAF and the joint force should train and educate top officials about salient risks stemming from hacking and leaking information.
- USAF and the joint force should foster institutional capacity for disseminating counternarratives and debunking disinformation on matters pertaining to USAF and the U.S. Department of Defense.
- USAF and the joint force should maintain clear, consistent public messaging pertaining to ongoing U.S. and allied activity and matters of public controversy implicating the U.S. and allied militaries.
- USAF and the joint force should work through nongovernmental organizations to debunk disinformation.

# Acknowledgments

Many people contributed to the completion of this report. We are grateful to the people who arranged and participated in interviews in Ukraine and the United States. We greatly appreciate the participation of Alyssa Demus with fieldwork in Ukraine, and we thank Andrew Radin for advice and assistance with the fieldwork. We are especially grateful to the reviewers of this study, Donald Jensen, Dara Massicot, and Chris Paul. Any and all errors in this report are the sole responsibility of the authors.

## Abbreviations

| | |
|---|---|
| AFSOC | Air Force Special Operations Command |
| APT | Advanced Persistent Threat |
| CYBERCOM | U.S. Cyber Command |
| DDoS | distributed denial of service |
| DFRLab | Digital Forensics Lab |
| DNC | Democratic National Committee |
| DoD | U.S. Department of Defense |
| EU | European Union |
| FSB | Federal Security Service (Russian Federation) |
| GRU | Russian Military Intelligence |
| GOU | Main Operational Directorate |
| IRA | Internet Research Agency |
| IT | information technology |
| ISIL | Islamic State of Iraq and the Levant |
| MH-17 | Malaysia Airlines Flight 17 |
| MISO | military information support operations |
| NATO | North Atlantic Treaty Organization |
| NGO | nongovernmental organization |
| ODNI | Office of the Director of National Intelligence |
| OK | Odnoklassniki |
| PSYOPS | psychological operations |

| | |
|---|---|
| StratCom CoE | Strategic Communications Centre of Excellence |
| SVR | Foreign Intelligence Service (Russian Federation) |
| UK | United Kingdom |
| USAF | U.S. Air Force |
| USAGM | U.S. Agency for Global Media |
| VK | VKontakte |

CHAPTER ONE

# Introduction

Russia is waging a wide-reaching and relentless information warfare—or, to use the Russian term, *information confrontation*—with the Western world. In 2017, the U.S. intelligence community publicly announced that Russia interfered in the 2016 U.S. election. Although Russian influence efforts predate 2016, Russia's activities directed at the U.S. presidential election "represented a significant escalation in directness, level of activity, and scope of effort compared to previous operations aimed at U.S. elections."[1] A core part of the election-meddling effort employed social media. Individuals working within the Internet Research Agency (IRA)[2] and as part of Russia's military intelligence have been exposed, sanctioned, and/or indicted.[3] Nonetheless, Russia's social media activity has flourished in the United States and across the Western world.[4] Russia has employed social media to spread disinformation and propaganda and

[1] Office of the Director of National Intelligence (ODNI), *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, January 6, 2017, p. 6.

[2] The IRA is a now-infamous *troll farm*—a team of trolls, or bloggers and social media operators that disseminate messaging favorable to a sponsoring organization, typically for a fee. These groups are also referred to as *troll factories*.

[3] For an overview of indictments, see Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Vol. I, Washington, D.C.: U.S. Department of Justice, March 2019, pp. 174–180.

[4] For evidence of continued growth in Russia's information warfare on social media, see Philip Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François, *The IRA, Social Media and Political Polarization in the United States, 2012–2018*, University of Oxford: Computational Research Project, December 2018.

to interfere with the internal politics of other countries, targeting varied audiences—including the U.S. military.

Although the impact of Russia's social media activities on specific outcomes—such as votes, policy decisions, or public opinion—is largely unknown, their very notoriety represents a kind of success for Russia.[5] By creating doubts about the outcome of any election, Russia's efforts threaten to undermine the trust that people have in the legitimacy of their democratic institutions. Similarly, sowing doubts about the validity of any given piece of news threatens to undermine the belief in the professional media and the possibility of factual truth itself. More-discrete adverse consequences are readily imaginable: For example, hijacked military social media accounts can be used to spread false and alarming information; voting can be affected by persuasive disinformation about a candidate spread on the eve of an election with little time to debunk; leaking manipulated communications can drive a wedge between the United States and its allies or partners. In sum, Russian capabilities to operate on social media, if unimpeded, could grow into a more serious threat.

Thus, in this study, we sought to better understand Russia's disinformation through social media as a way to help the U.S. Air Force (USAF) and the joint force respond more effectively to this threat.[6] In this report, we examine Russian thinking and practice of social media–based information efforts, and we consider the limitations and successes of existing countermeasures. Although the Russian information warfare machinery is modestly resourced and not centrally organized, it can reach sizable audiences through social media.[7] Thus, the U.S. military should improve its awareness of this continuously evolving threat, its ability to respond, and the resilience of its members to dis-

---

[5] As the intelligence community assessed, "Russian intelligence services would have seen their election influence campaign as at least a qualified success because of their perceived ability to impact public discussion" (ODNI, 2017, p. 5).

[6] This report was completed before the creation of the U.S. Space Force and therefore uses the name "U.S. Air Force" to refer to both air and space capabilities.

[7] See our discussion in Chapter Three.

information. At the end of this report, we offers specific recommendations for how to do so.

## Methodology

To conduct this study, we performed several distinct tasks using a combination of research methods. Our process is described here.

### Russian Thinking About Social Media in Information Warfare

To illuminate Russian thinking about this subject, we examined official Russian strategic documents (such as the Information Security Doctrine), public statements by Russia's leaders, and publicly available Russian-language military writings pertaining to information confrontation in general and to the role of social media in particular. Importantly, Russian military and defense experts often abstain in publicly accessible formats from declaring what Russia's approach is or should be. Instead, they discuss the nature of information confrontation in the abstract, or they address their perceptions of the approaches to information warfare adopted by the United States or the West; so, we must infer their views of Russia's approach from this discussion.

### Russian Social Media–Based Information Operations

To describe how Russia uses social media, we examined a wide variety of sources, supplemented with expert interviews. Sources that we examined included research and analysis by governmental bodies involved in responding to Russian information warfare (such as the North Atlantic Treaty Organization [NATO]'s Strategic Communications Centre of Excellence [StratCom CoE]) and nongovernmental organizations (NGOs), such as Bellingcat, Atlantic Council's Digital Forensics Lab (DFRLab), and Ukrainian StopFake. We also relied on a large number of media reports that have covered Russian information efforts over the past several years. Whenever possible, we rely on established, professional media outlets such as the *New York Times* or *Washington Post*. However, we are mindful of the fact that the Russian activities that are investigated and reported by major outlets might not be representative of the

universe of Russian activity in this realm. In an attempt to lessen any systematic skewing that might result from reliance solely on established media sources, we also drew on lesser-known and/or foreign media outlets. In so doing, we assessed the credibility of each source sited, and caveat our claims accordingly. We supplemented printed sources with unstructured interviews conducted on an anonymous basis with subject-matter experts, such as representatives of international organizations, the private sector, and the nonprofit, nongovernmental sector.

### Selected Countermeasures Adopted by the United States and Other Western Countries

To offer an account of intergovernmental responses and select national responses by governments and NGOs, we relied on research and analysis by governmental bodies involved in responding to Russian information warfare, research produced by academics and policy experts, and media reports. To a limited extent, we drew on social science research in attempts to assess potential effects of specific categories of countermeasures.

### Ukraine Case Study

Members of our research team also conducted fieldwork interviews in Kyiv, Ukraine, on an anonymous basis. Ukraine arguably has been at the forefront of Russia's disinformation effort and, because of the 2014–2015 conflict in Eastern Ukraine, also provides insight into how Russia might employ these tactics in an actual military conflict. Interviews were conducted with experts in all major state bodies involved in responding to Russian information operations, representatives of Ukraine's robust network of NGOs engaged in monitoring, debunking, and investigating Russian information warfare and/or cyber activities, representatives of the private sector (including the technology sector), and researchers. In addition, we examined the large body of publicly available research pertaining to Russia's activities in Ukraine issued by government bodies, NGOs, and individual researchers. We also drew on media reports, including Ukrainian-language sources. Again, we assessed the credibility of each source cited and caveat our claims accordingly.

### Analysis of Russia's Anxieties About and Vulnerabilities Stemming from the Rise of Social Media

In the appendix, we examine Russia's anxieties about the threat that social media presents to the regime and its interests. For this task, we drew in part on the same official and military literature employed for our other tasks, supplemented by academic and policy research. To understand the real vulnerabilities that underlie those anxieties (and to identify which of these vulnerabilities present potential opportunities for exploitation) we also drew on academic, think tank, and policy works and on media reporting on Russia under President Vladimir Putin.

In all tasks, we rely substantially on past RAND research in this area.

## Definitions and Scope

Numerous terms—*information operations*, *information war*, *information campaigns*, *psychological warfare*—are used in the military and civilian literature to describe Russia's activities in the informational domain. As Ulrike Franke of the Swedish Defence Research Agency notes, "[t]o the professional, some of [these terms] have precise and well-defined meanings, some of them have become non grata, and some are just vague," and "[t]o the layman, the intricacies of these terms are even less transparent."[8] Our goal is to avoid irritating the professionals or confusing the laymen, so we use the terms *information confrontation* and *information warfare* interchangeably, broadly, and loosely to capture all hostile activities in the informational domain that are (likely) intended to influence perceptions or behavior.[9] The terms loosely correspond to the Russian understanding of information confrontation (информационное противоборство), which covers all "hostile activities using information as a tool, or a target,

[8] Ulrik Franke, *War by Non-Military Means: Understanding Russian Information Warfare*, Kista, Sweden: Swedish Defense Research Agency, March 2015, p. 10.

[9] We specify these activities as "likely" to accommodate the fact that intent can be exceedingly difficult to infer based on observable evidence.

or a domain of operations."[10] The Russian understanding of this term refers both to activities conducted during peacetime and to those conducted during conflicts.[11] We avoid references to *information operations*, which has a narrower and more precise definition in U.S. Department of Defense (DoD) doctrine.[12] We do use a nontechnical term—*information efforts*—to broadly capture activities and efforts that are part of Russia's information warfare, within which disinformation on social media is embedded.

The central focus of this study is on disinformation on social media, which is just one component of Russia's broader information confrontation activities. We define both operative concepts that make up our focus. By *disinformation*, we mean "false, incomplete, or misleading information that is passed, fed, or confirmed to a target individual, group, or country."[13] We define *social media* as any "[w]eb-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with

---

[10] This articulation belongs to Keir Giles, a noted expert on the topic. Keir Giles, *Handbook of Russian Information Warfare*, Rome, Italy: NATO Defense College, November 2016, p. 6. For a similar Russian definition, see S. I. Makarenko, *Information Confrontation and Electronic Warfare in Net-Centric Wars of the Beginning of the XXI Century [Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века*], St. Petersburg, Russia: Knowledge-Intensive Technology [Наукоемкие технологии], 2017, p. 223. For the Russian definition, see Ministry of Defense of the Russian Federation, "Information Warfare [Informatsionnoe protivoborstvo]," *Military-Encyclopedic Dictionary of the Ministry of Defense*, undated.

[11] The distinction between "information confrontation" and "information war" in the Russian understanding is "the subject of detailed debate in official Russian sources" that is "of little practical impact for assessing Russian approaches" (Giles, 2016, p. 6). To avoid wading into unnecessary terminological debates, we avoid the term "information war" unless it appears in an original source.

[12] In Joint Publication 3-13, the Joint Chiefs of Staff defines *information operations* as, "[t]he integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own" (Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, Washington, D.C., November 27, 2012, incorporating change 1, November 20, 2014).

[13] Richard H. Shultz and Roy Godson, *Dezinformatsiya: Active Measures in Soviet Strategy*, Washington, D.C.: Pergamon-Brassey, 1984, p. 41.

whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[14]

We emphasize, however, that the reality of Russia's activities does not neatly map onto these conceptual definitions. Whether specific pieces of information discussed are truly disinformation can be debatable. We do not think that placing rigid boundaries around this term aids understanding; thus, although the focus is disinformation, we might also discuss *propaganda*, or "the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist."[15] Understood in terms of these common definitions, both disinformation and propaganda manipulate information in a manner that appears calculated to mislead (such as through selective omission of facts, framing, appeal to emotions, and the use of logical fallacies).[16]

Furthermore, Russia does not distinguish between cyberwarfare and information warfare, and it views such activities as stealing information through cyberattacks and distributed denial of service (DDoS) as tools of information confrontation.[17] Some of Russia's activities that take place on or through social media are not pure disinformation efforts; rather, they are disinformation efforts functionally linked to a cyberattack of some kind. Thus, although we largely stay away from technical discussion of cyberattacks, we do touch on cyberoperations when these are closely tied to activities that use information to shape perceptions or behavior—for example, hacks that produce information that is subsequently leaked.

---

[14] Danah M. Boyd and Nicole B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, No. 13, 2008, p. 211.

[15] Garth S. Jowett and Victoria O'Donnell, *Propaganda and Persuasion*, Thousand Oaks, Calif.: Sage Publications Inc., 2012, p. 7.

[16] For a more thorough taxonomy of the ways in which information is manipulated by Russian actors, see Miriam Matthews, Alyssa Demus, Elina Treyger, Marek N. Posard, Hilary Reininger, and Christopher Paul, *Understanding and Defending Against Russia's Malign and Subversive Information Efforts in Europe*, Santa Monica, Calif.: RAND Corporation, RR-3160-EUCOM, 2021.

[17] Giles, 2016.

Moreover, Russia's activities often extend to spaces that might not meet the rigorous definition of social media. We discuss activities that take place in online fora or platforms that simply allows users to generate content and interact with other users even if the platform does not meet all three definitional criteria noted. This means that we go beyond well-known platforms, such as Facebook and Twitter, to activities that take place on publishing platforms (such as Medium), video-sharing sites, blogs, encrypted messaging applications, and (occasionally) simple websites on which readers can comment and interact with each other.

We cannot capture the entire domain of relevant activity. Our scope is limited geographically; we tend to focus on Russian activities aimed against the United States and Europe. We are also limited by the opaque nature of Russian efforts, which means that only disinformation and related activity that have been discovered and publicly disclosed or relayed to us in interviews can be included. Moreover, even our synthesis of the publicly known efforts might not be exhaustive in light of the significant amount of attention that many analysts, researchers, and organizations have devoted to Russia's information confrontation efforts.

## Overview of the Report

Overall, this report substantiates the following arguments and conclusions. Moscow views social media as a double-edged sword. On the one hand, the novel technology adds another layer to Russia's preexisting anxieties about the West's hostile intentions and capabilities. At the same time, Russia recognizes the advantages of social media as a low-cost and potentially highly effective weapon of asymmetric warfare. Its use of this weapon outside the former Soviet Union picked up most markedly in 2014, suggesting that Russia resorted to this tool in part as a response to the West's reaction to the Ukraine conflict.

Although popular portrayals of the Russian disinformation machine sometimes imply an organized and well-resourced operation, evidence suggests that it is neither. Even with relatively modest invest-

ments, however, Russian social media activity has been wide-reaching, deploying a great number of social media accounts to spread disinformation and propaganda across multiple platforms, reaching broad and varied international audiences. Whether and how the wide reach of social media activity translates into impact or success are open questions. Still, Russia's efforts have certainly raised alarm among U.S. allies and partners and prompted a variety of responses to confront and deter Russia—to largely uncertain effect. Although evidence is scarce that Russia's efforts have altered specific measurable outcomes (such as votes or political decisions), the amount of attention that Russia's efforts have received is itself a kind of success. The appearance of pervasive foreign disinformation threatens to erode trust in the media, acceptance of vital facts, and the perceived legitimacy of democratic processes.

Moreover, more-discrete adverse consequences of Russian disinformation campaigns, such as those implicating the U.S. armed forces, are entirely plausible. Thus, we recommend that USAF and the joint force improve defensive measures aimed at raising awareness and lowering the susceptibility of military members and their families to Russian disinformation and propaganda campaigns. Russia's own vulnerabilities to social media might present opportunities for offensive action to deter disinformation campaigns, but many of these hypothetical actions carry more risks than benefits. We address these issues in the appendix, but ultimately recommend that the U.S. government and the joint force focus on creating a less fertile ground for Russian disinformation.

The rest of the report proceeds as follows. In Chapter Two, we introduce the Russian conception of information confrontation, and we synthesize Russian thinking about the place of social media within that broader conception. We also examine the ways in which publicly available Russian military literature grappled with this technological advance. In Chapter Three, we focus on the practical and more-detailed aspects of Russia's information operations on social media, looking into the when, who, where, why, and how of relevant activities. In Chapter Four, we present a selective overview of countermeasures against Russia's social media–based information operations

(focusing on the intergovernmental response), and their apparent or perceived consequences. In Chapter Five, we focus on the Ukrainian experience with Russia's social media–based disinformation; in Chapter Six, we synthesize key policy recommendations most relevant to the USAF Special Operations Command and the joint force. An appendix addresses Russia's own anxieties about social media and vulnerabilities that underlie these anxieties; although vulnerabilities could hypothetically be exploited by Western offensive information operations or psychological operations (PSYOPS), we generally identify weighty reason to be cautious in this regard.

CHAPTER TWO

# Russian Approach to Social Media-Based Information Warfare in Theory

Although Russian defense experts focused on information warfare from the 1990s through the early 2000s, they only tenuously grasped how advances in modern communication technologies could play a role in that warfare. A 1999 textbook by Russian Military Intelligence (GRU) on psychological warfare, for instance, frequently notes the use of television in supporting operations, although the internet is mentioned only twice.[1] The same textbook overstates the potential of a mythical "virus666" to affect the "psychological state of owners of personal computers" by using a specialized color scheme and frame rate to induce "hypnosis" or even "near death."[2] Through the 2000s, however, Russian defense experts developed a better understanding of the new technology—and of the internet and social media—through Russia's own experiences alongside those of other countries. The evolution of Russia's understanding and embrace of social media became evident in the course of the Ukraine conflict and thereafter, as Russia thoroughly

[1] Vladimir Gavrilovich Krysko, *The Secrets of Psychological War (Goals, Tasks, Methods, Forms, and Experience) [Секреты психологической войны (цели, задачи, методы, формы, опыт)]*, Minsk, Belarus: Main Intelligence Directorate [Главное разведывательное управление], 1999; Alexey Kovalev and Matthew Bodner, "The Secrets of Russia's Propaganda War, Revealed," *Moscow Times*, March 1, 2017.

[2] Krysko, 1999, p. 9; Gennadiy Zhilin, "Information-Psychological Weapons: Yesterday and Today [Информационно-Психологическое Оружие: Вчера и Сегодня]," *Soldier of the Fatherland [Солдат Отечество]*, No. 57, 2004; Igor Panarin, "'Trojan Horse' of the 21st Century. Informational Arms: Realities and Possibilities ['Троянский конь' XXI века. Информационное оружие: реалии и возможности]," *Red Star [Красная звезда]*, No. 282, August 12, 1995.

incorporated the technology into its information warfare arsenal. In this chapter, we seek to synthesize the development of Russian thinking about the place of social media within the broader information confrontation.

## Russian Approaches to Information Confrontation

Although preoccupation with information warfare—alongside other channels of malign influence or hybrid warfare—appears recent, Russia's approach to information confrontation is rooted in its history, stretching from as early as the 15th century through the Soviet-era institutionalization of propaganda to contemporary forms of information confrontation.[3] Information confrontation, a Russian conception, is loosely analogous to the Western ideas of information operations or information war—but with distinct differences. Unlike the Western concepts, information confrontation is not limited to wartime, and it encompasses of a variety of means, such as digital propaganda, psychological operations, electronic warfare, and technical cyberoperations.[4] Keir Giles, a noted authority on Russian information confrontation, says that Russia's approach "cover[s] a vast range of different activities and processes seeking to steal, plant, interdict, manipulate, distort or destroy information."[5] In Russian terms, information confrontation integrates two aspects—the *information-technical*, which aims to affect "technical systems which receive, collect, process and transmit information," and the *information-psychological*, which aims to affect "the personnel of the armed forces and the population."[6]

---

[3] For example, see Olga Oliker, "Russia's New Military Doctrine: Same as the Old Doctrine, Mostly," *Washington Post*, January 15, 2015.

[4] Giles, 2016, p. 4.

[5] Giles, 2016, p. 4; Tony Selhorst, "Russia's Perception Warfare: The Development of Gerasimov's Doctrine in Estonia and Georgia and Its Application in Ukraine," *Militaire Spectator*, Vol. 185, No. 4, 2016, p. 151.

[6] Giles, 2016, p. 9, quoting an "authoritative Russian textbook."

In Moscow's view, since the 1990s, Russia and the West have become increasingly embroiled in a "civilizational struggle," in which Russia believed it must protect its worldview and culture against the aggressive encroachment of Western liberalism.[7] A Western "information aggression" against Russia was viewed as an intrinsic part of that struggle.[8] As another Russian academic observed, history has demonstrated that victory in information confrontation requires the offensive use of "active information measures" and "psychological operations"—and that a merely defensive approach loses out.[9] By extension then, the perceived Western use of information warfare played a significant role in compelling Russia to develop its own offensive information confrontation arsenal.

Russia's recognition that it could not compete with the West in conventional capabilities raised the importance of information confrontation for Russian military planners and the Kremlin.[10] In Putin's own words, "[o]ur responses [to other countries' development of armed forces] must be based on intellectual superiority, they will be asymmetric, and less expensive."[11] Conventional inferiority would not matter if, as the Russian conception would have it, information warfare was a substitute for force rather than just a "force multiplier" for kinetic oper-

---

[7] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, Santa Monica, Calif.: RAND Corporation, RR-1772-A, 2018, p. 5.

[8] For example, see Sergey Modestov, "The U.S. Is Ready for an Information War with Russia [США готовы к информационной войне с Россией]," *Independent Military Review [Независимое военное обозрение]*, No. 25, July 12, 1997; A. A. Streltsov, "The Main Tasks for Government Policy in Information Warfare [Основные задачи государственной политики в области информационного противоборство]," *Military Thought [Военная мысль]*, No. 5, 2011, pp. 18–25. For a related discussion of Russian military thought, see Franke, 2015.

[9] Andrey Evdokimov, "About Active Information Measures along the Southern Strategic Direction [Об активных информационных мероприятиях на южном стратегическом направлении]," *Defense and Security [Защита и безопасность]*, No. 4, 2010.

[10] Giles, 2016, p. 16.

[11] Vladimir Putin, "'Soldier' Is an Honourable and Respected Rank [Солдат есть звание высокое и почетное]," excerpts from the annual address to the Federal Assembly of the Russian Federation, *Red Star [Красная звезда]*, May 11, 2006.

ations.[12] Thus, Russian military authors pronounced that the "potential of information weapons is so great, that there exist precedents of victory in operations and conflicts solely due to their use, without traditional means of armed struggle."[13] Consequently, by 2010, Russia's military doctrine articulated a growing role for information confrontation, featuring its use to "achieve political goals without force."[14]

The ways in which Russia wages information confrontation at the time of this writing was shaped by several key developments. It was significantly influenced by the 2008 Georgian War, when "a resilient Georgia overtook Russia in the larger information war, forcing Russia to rethink how it conducts information-based operations."[15] According to various Russian military observers, Georgia portrayed Russia as an aggressor, successfully influencing global opinion through mass media, while Russian public affairs specialists failed to develop a compelling counternarrative.[16] Between that war and Russia's annexation of Crimea, Russia's understanding and means of waging information warfare evolved, combining military operations, state-controlled media, official rhetoric, and unofficial covert activity, such as the

---

[12] Mark Galeotti, "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?" *Small Wars & Insurgencies*, Vol. 27, No. 2, March 21, 2016, p. 291.

[13] V. M. Burenok, A. A. Ivlevl, and V. Yu. Korchak, *Development of Military Technologies of the XXI Century: Problems, Planning, Actualization [Развитие военных технологий XXI века: проблемы планирование, реализация]*, Tver, Russia: OOO "Kupol" 2009, cited in Makarenko, 2017, p. 224; also see S. G. Chekinov and S. A. Bogdanov, "Forecasting the Nature and Content of Wars of the Future: Problems and Assessments [Прогнозирование характера и содержания войн будущего: проблемы и суждения]," *Military Thought [Военная мысль]*, No. 15, 2015, pp. 44–45.

[14] Administration of the Russian President [Администрация Президента России], "Military Doctrine of the Russian Federation [Военная доктрина Российской Федерации]," webpage, February 5, 2010.

[15] Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters*, Vol. 47, No. 2, 2017, p. 51.

[16] Mikhail Novikov and Vyacheslav Ovchinnikov, "Information Confrontation in Contemporary Geopolitics [Информационное Противоборство в Современной Геополитике]," *Defense and Security [Защита и безопасность]*, No. 2, 2011; Dmitriy Makarov, "Information Wars. A Word, Placed Under the Gun [Информационные Войны. Слово, Поставленное под Ружье]," *Flag of the Motherland [Флаг Родины]*, No. 115, 2009.

IRA and other troll farms. In contrast to Georgia, Russia activated these multiple actors and weapons in Ukraine to shape public opinion there, in Russia, and internationally—while retaining Soviet-era theoretical approaches, such as the notion of *reflexive control*, or inducing the adversary to act in the interests of Russia on their own volition.[17] Since the Ukraine crisis, Russia's information warfare has expanded to a global scale, generally seeking to bolster Russia's regime stability and international standing—usually through undermining the West.[18]

## Russian Approaches to Social Media

By the onset of the Ukraine crisis in 2014, Russian experts had integrated social media platforms into its information confrontation arsenal. Russian military thinkers and experts viewed the rise of social media as a threat to Russia's security, but they also embraced it as a low-cost and potentially highly effective offensive weapon—which can help Russia redress the imbalance in military capabilities between itself and the United States and its allies.

### Social Media as a Threat

Moscow has long believed that the United States and the West dominate traditional print and television media and that they manipulated media conglomerates during Operations Just Cause and Desert Storm and NATO activity elsewhere.[19] Such "modern realities," in the words

---

[17] Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Russia Report I, Washington, D.C.: Institute for the Study of War, September 2015; Oliker, 2015; for a discussion of the exploitation of preexisting divisions and vulnerabilities by the Soviet Red Army, see Krysko, 1999.

[18] Katherine Costello, *Russia's Use of Media and Information Operations in Turkey*, Santa Monica, Calif.: RAND Corporation, PE-278-A, 2018; Scott Jasper, "Russia's Ultimate Weapon Might Be Cyber," *The National Interest*, January 28, 2018; Eduard Kovacs, "Russian Cyberspies Shift Focus from NATO Countries to Asia," *Security Week*, February 20, 2018.

[19] Krysko, 1999; D. Semenov "The Role of Disinformation in Information Confrontation of the Parties in the Syrian Conflict [Роль Дезинформации в информационном противостоянии сторон в сирийском конфликте]," *Foreign Military Review [Зарубежное военное обозреное]*, No. 12, December 2014.

of former Soviet diplomat Georgy Shakhnazarov, demanded that Russia raise the level of its "technological" and "propaganda" support.[20] Part of this new reality—at least to Putin and his close circle of advisers—was that the rise of the internet was bound to hand the West a tremendous advantage over Russia. The internet, as Putin pronounced publicly, was a "CIA project," and Russia had to be protected from it.[21] Similarly, any emerging information technology was also generally seen to aid Russia's adversaries in undermining Moscow. Military officers and experts closely monitored actual foreign capabilities related to waging information-psychological operations, such as the use of the airborne Commando-Solo broadcasting platform and the 193rd Air Wing in Yugoslavia (which was able to supplant Serbian state-sponsored television with U.S. broadcasting that supported psychological operations) during NATO's intervention in the Balkans.[22] Some military literature, however, grossly exaggerated the nature of technological innovations developed by the West and their impacts on future conflict.[23]

Perhaps unsurprisingly given this context, Russia also saw the spread of social media as threatening. A series of political developments further fueled these perceptions. First among these were the

---

[20] Elena Mikhaleva, "Georgiy Shakhnazarov: Russia and Her Army Should Be Ready for Computer, Information, and Ecological Wars . . . [Георгий Шахназаров: 'Россия и ее армия должны быть готовы к компьютерным, информационным, экологическим войнам . . .]," *At the Fighting Post [На боевом посту]*, No. 29, April 9, 1997.

[21] Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, New York: PublicAffairs, 2015, p. 238. For an account of the Kremlin's attempts to change the rules of global internet governance to give authoritarian countries more control over the internet, also see Soldatov and Borogan, 2015, pp. 235–238. The EC-130 Commando-Solo is a modified transport aircraft that can broadcast messages on radio and television. As such, it is a key delivery platform for military information efforts. Vladimir Akhmadullin, "The Word, Equal to the Bomb [Слово, приравненное кбомбе]," *Independent Military Review [Независимое военное обозрение]*, No. 25, July 2, 1999.

[22] Zhilin, 2004.

[23] For example, see Nikolai Borskiy, "Main Directions for Ensuring Information Security in the Activities of Troops (Forces) [Основные направления обеспечения информационной безопасности в деятельности войск (сил)]," *Orienteer [Ориентир]*, No. 11, November 2001; and V. Belous, "Weapons of the 21st Century [Оружия XXI века]," *International Life [Международная Жизнь]*, No. 2, 2009.

so-called color revolutions in former Soviet states in the early 2000s. As leading Russia scholars Timothy Colton and Samuel Charap explain, "Moscow came around to the interpretation that the uprisings next door were a tool of Western, and pointedly of American, policy . . . deployed . . . in order to remove sitting governments that pursued policies counter to U.S. interests."[24] The Russians believed that the United States engineered these uprisings in no small part through communications technology—the internet in particular. Many Russian military authors pointed to the West's capacity to influence and organize mass movements through the internet during the color revolutions in Ukraine and Georgia.[25]

After about 2011, social media became a more prominent part of the conversation among Russian military officers and experts. For instance, one Russian officer claimed that such programs as the supposed U.S. effort to distribute cheap computers to youth in Afghanistan, Iraq, and Libya in 2005 demonstrated the growing importance of electronic networks (to the United States) to manipulate a given target audience.[26] The Snowden revelations and the unwinding case of the "Stuxnet" virus exacerbated Russian fears of rapid advances in U.S. capabilities.[27] In 2014, for example, several general staff officers claimed that the hardware exploitation revealed by Snowden's leaks

---

[24] Samuel Charap and Timothy J. Colton, *Everyone Loses: The Ukraine Crisis and the Ruinous Contest for Post-Soviet Eurasia*, Milton Park, United Kingdom: Routledge, 2018.

[25] For example, see V. Kuzmin, "U.S. Role in Implementing 'Color Revolutions' in Foreign Countries [Роль США в осуществлении «цветных революций» в зарубежных странах]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 9, September 2008; and Vladimir Timofeev, "On Informshablon [Про информшаблону]," *Red Star [Красная звезда]*, No. 6, January 19, 2005.

[26] A. Serov, "About the Role of Disinformation in Modern Conflicts and Wars [О роли дезинформации в современных конфликтах и войнах]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 8, 2011.

[27] N. P. Romashkina, and A. B. Koldobskiy, "New Methods of Confrontation in the XXI Century [Новые Методы Противоборства XXI Века]," *Digest of the Academy of Military Sciences [Вестник Академии Военных Наук]*, No. 1, 2015. Perhaps no developments were more influential in promoting these fears than the Stuxnet virus, the establishment of CYBERCOM, and the leaked information provided by former National Security Agency contractor Edward Snowden.

carried direct implications for psychological warfare and might be deployed to sway "the behavioral and emotional attitudes of groups or individuals on any issues in the way wanted by the adversary."[28]

No events, however, shaped the Russian view of social media as a dire threat to national security more than the Arab Spring revolts and the protests in Moscow in 2011–2012.[29] The Moscow protests, triggered by the perceptions of fraud in the 2011 parliamentary elections, represented the greatest challenge to the Russian regime since Putin ascended to the presidency. Russian protesters even borrowed from the social media repertoire of protesters in the United States in their mobilization efforts.[30] Like Putin himself, Russian military authors often attribute these events to premeditated and well-orchestrated PSYOPS organized by Western special services, especially U.S. intelligence and the U.S. military's PSYOPS units.[31]

Russia saw the same forces operating behind the Arab Spring. In 2013, Chief of the General Staff Valery Gerasimov delivered a now well-known speech that emphasized the significance of using "technologies for influencing state structures and the population with the help

---

[28] I. N. Dylevskii, V. O. Zapivakhin, S. A. Komov, S. V. Korotkov, and A. N. Petrunin, "An International Nonproliferation Regime for Information Weapons: Utopia or Reality? [Международный режим нераспространения информационного оружия: утопия или реальность?]," *Military Thought [Военная мысль]*, No. 10, October 2014.

[29] Vladimir Nesmeyanov, "This Quiet, Deadly War [Эта тихая смертельная война]," *Flag of the Motherland [Флаг Родины]*, No. 10, March 10, 2017, p. 7; Konstantin Sivkov, "The 'Wisdom' of Yanukovich [«Мудрость Януковича»]," *Military-Industrial Courier [Военно-промышленный курьер]*, No. 26, July 23, 2014, p. 2. For more on the use of social media during the Moscow protests, see Alissa de Carbonnel, "Insight: Social Media Makes Anti-Putin Protests 'Snowball,'" Reuters, December 7, 2011.

[30] For example, see the use of #Occupy (Miriam Elder, "Russian Protests: Thousands March in Support of Occupy Abay Camp," *The Guardian*, May 13, 2012b).

[31] A. Kudryashov, "Use Abroad of Internet Networks in the Interests of Conducting Information Wars [Исползование за Рубежом Сети Интернет в Интересах Ведения Информационных Войн]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 4, 2011; Vasiliy Mikryukov, " Victory in War Should Be Achieved Even Before the First Shot [Победа в войне должна быть достигнута еще до первого выстрела]," *Independent Military Review [Независимое военное обозрение]*, January 15, 2016; Vladimir Nesmeyanov, "Can We Defend the Great Victory? [Сумеем ли Защитить Великую Победу?]," *Flag of the Motherland [Флаг Родины]*, No. 60, 2013.

of information networks" in North Africa: The Arab Spring, according to him, demonstrated how quickly "perfectly thriving states" could fall victim to "foreign intervention" and "descend into the depths of chaos, humanitarian catastrophe, and civil war."[32] This speech gave rise to the term *Gerasimov doctrine*, coined by Russia expert Mark Galeotti and subsequently misappropriated by others to describe Russia's "'new way of war,' 'an expanded theory of modern warfare,' or even 'a vision of total warfare.'"[33] As Galeotti and others subsequently explained, Gerasimov was not offering an articulation of Russia's doctrine; he was describing the threat from the West—against which Russia must learn to defend.[34] One Russian officer, A. Bobrov, explained that social media was a key tool for such foreign intervention: "[O]pposition forces, *with the support of interested parties*, quickly created autonomous mobile networks, distributed computers and communications to the public free of charge, thereby contributing to filling the information vacuum."[35] This kind of targeting of specific, highly active audiences led to "unprecedented success" in engineering a revolution through digital means, according to another Russian author.[36] Although social media facilitated uprisings supported by external actors, Russians observed that the same technology could render regime forces powerless to disrupt the organization of opposition through social media: The "Arab secret services were not able to prevent people sending inflammatory messages," according to Bobrov, "because they didn't have access to the social network manage-

---

[32] Valeriy Gerasimov, "The Value of Science Is in Prediction [Ценность науки в предвидении]," *Military-Industrial Courier [Военно-промышленный курьер]*, No. 8, February 26, 2013.

[33] Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" *Foreign Policy*, March 5, 2018.

[34] Galeotti, 2018.

[35] A. Bobrov, "Information War: From Leaflets to Twitter [Информационная война: от листовки до Твиттера]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 1, January 2013 (emphasis added).

[36] S. Orlov, "The Role of Social Networks in the Organization of Protest Populations in the Course of the 'Arab Spring' [Роль социальных сетей в организации протестных выступленный населения в ходе «Абарсной весны»]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 12, December 2014.

ment servers located in the territory and *under the control of the U.S. special services*."[37]

Reflecting on these experiences since the early 2000s, Gerasimov in 2016 explicitly pointed to the internet as a weapon of hybrid warfare:

> "Color revolutions" are employed as the main means [of hybrid warfare], which should . . . lead to a nonviolent change of government in the adversary's country. Any "color revolution"—it's regime change, organized externally. At its core are found information technologies that contemplate manipulation of the protest potential of the population, together with other non-military means. An important part of this will be a mass, targeted influence on the consciousness of the citizens—the objects of aggression by means of the global internet network.[38]

The Russian military's perception of social media as a national security vulnerability continued to evolve against the backdrop of rising tensions with the West.[39] Russian military literature at times identifies specific actors behind the social media threat. Most commonly and unsurprisingly, the social media threat is identified as being presented by the United States, particularly the military—including the 4th Military Information Support Group, 193rd Special Aviation Wing—and U.S. intelligence services.[40] Other NATO countries also attract significant attention: A 2019 article, for instance, lays out the threat to Russia posed by the United Kingdom (UK)'s 77th Brigade, which allegedly uses social media and computer network attacks to undermine Russia's international and domestic standing, referencing

---

[37] Bobrov, 2013 (emphasis added).

[38] Valeriy Gerasimov, "According to the Experience of Syria [По опыту Сирии]," *Military Industrial Courier [Военно-промышленный курьер]*, No. 9, March 9, 2016.

[39] The appendix provides a brief account of Moscow's responsive measures to control internet access.

[40] "Information Wars [Информационные войны]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 5, 2015, p. 100; Boris Podoprigora, "Third World [War]—Informational? [ретья мировая—информационная?]," *Navy Newspaper [Морская газета]*, No. 39–40, 2011.

"expert" opinions that the unit was not bound by any "moral norms" or "humanitarian restrictions" in executing its operations.[41] The article ended on an alarmist note concerning the threat posed by social media to the Russian state and asserted that social media threats could be "even more destructive than tank breakthroughs of bygone days."[42]

### Social Media as an Offensive Weapon

At least according to Russian military writings, Russia vaguely perceived the offensive implications of emerging communications technology in the 1990s but began to embrace the offensive potential of social media only in the early 2000s.[43] For example, a GRU psychological operations officer was impressed with NATO's use of the Commando-Solo platform.[44] The same officer noted that NATO's online efforts involved "more than 300,000 websites," including sites that were—according to the officer—fake ones promoting NATO propaganda.[45] Russian authors also praised Yugoslav hackers' attacks on U.S. military networks as a deft way to leverage an asymmetric capability against a conventionally superior adversary, leading the authors to conclude that the "transformation of information confrontation" could thwart U.S. geopolitical ambitions.[46] Russia's own counterterrorism efforts

---

[41] Aleksandr Novik, "Weapons of the Future, British Style [Оружие будещего по-британски]," *Baltic Guard [Страж Балтики]*, No. 2, January 18, 2019, p. 7.

[42] Novik, 2019, p. 7.

[43] For example, a GRU textbook published in 1999 (Krysko, 1999) provided intricate methods of exploiting ethnic, religious, and political differences to sow societal discord in a target country but only fleetingly discussed the importance of the internet as it related to information confrontation.

[44] Akhmadullin, 1999; Vladimir Akhmadullin, "Informational Suppression of Ghaddafi's Colonel and His Army [Информационное подавление полковника Каддафи и его армии]," *Asia Center [Центр Азия]*, September 3, 2011. Some Russian defense analysts were less impressed with the same asset in other contexts, such as Afghanistan; for example, see Igor Kapustin, "Gypsies in Pentagon's Employ [Цыгане на службе Пентагона]," *Red Star [Красная Звезда]*, September 20, 2006.

[45] Akhmadullin, 1999.

[46] Sergey Modestov and Sergey Sokut, "Bytes in Place of Bullets [Байты вместо пуль]," *Independent Military Review [Независимое военное обозрение]*, No. 13, April 9, 1999.

in Dagestan yielded the observable impact of "constant psychological operations" that used "international computer networks" and the internet, according to a former Russian general and military theorist.[47]

A Russian colonel in 2008, setting forth lessons from that year's war with Georgia, noted South Ossetia's success in organizing mass influence efforts through social media to counter Georgian messaging.[48] The use of online forums and blogs to illustrate Georgian atrocities against locals, according to the author, were far more effective than the claims in "Anglo-Saxon" media about reported South Ossetian brutalities against Georgians.[49] In this view, the new "mass information armies" were more effective than the "mediated" dialogue of state leaders with the peoples of the world.[50]

Somewhat in contrast to the internet and traditional media, both of which Russia views as Western-dominated, at least some defense experts and analysts in Russia have expressed a view of social media as decentralized and a potential chink in U.S. armor.[51] For example, one Russian officer reported that the Taliban using social media to influence audiences outside Afghanistan was an effective insurgent counter-propaganda effort in Afghanistan against NATO efforts.[52]

---

[47] V. F. Kulakov, "Moral-Psychological Support of the Counter-Terrorist Operation in the Republic of Dagestan [Морально-психологическое обеспечение контртеррористической операции в Республики Дагестан]," *Military Thought [Военная мысль]*, No. 1, January 1, 2000. Likewise, Russians noted effective Chechen use of "global computer networks" to proliferate messages in favor of their cause (Yuriy Vladimirov, "The Chechen War (The Psychological Aspect) [Чеченская воина (психологический аспект)]," *On the Fighting Post [На боевом посту]*, No. 75, September 29, 2000).

[48] P. Kolesov, "Georgia's Information War Against South Ossetia and Abkhazia [Информационная воина Грузии против Южной Осетии и Абхазии]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 10, October 2008.

[49] Kolesov, 2008.

[50] Kolesov, 2008.

[51] As Soldatov and Borogan explain, "Russian officials in charge of information security often spoke bitterly of US domination of the internet, believing all the tools and mechanisms for technical control were in US hands" (Soldatov and Borogan, 2015, p. 229).

[52] D. Davydov, "Information-Psychological War in Afghanistan [Информационно-психологическая война в Афганистане]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 8, August 2012.

Oleg Ivannikov, a suspected GRU officer implicated in the destruction of civilian Malaysia Airlines Flight 17 (MH-17) over Ukraine in 2014, argued that because the United States leveraged network communications technology to rearrange the "world order" along Russia's periphery, Russia must use nontraditional media in influencing target audiences.[53]

Since 2014, Russian military authors have become more explicit about the potential uses of social media and the perceived need to reciprocate. A defense analyst at a prominent Russian military journal warned of U.S. "information troops" spreading propaganda on social media platforms and claimed that the Russian army was now "learning to wield these weapons."[54] Another analyst observed an advantage in leveraging communications technology to achieve asymmetric military ends against superior counterparts.[55] Russian political scientists observed that the "national media system" was being replaced by an international one, which increasingly relied on "internet resources" and "social networks"—and they noted that control over these resources could allow for "a quick change of power" within countries.[56] By 2016, a group of general staff officers focused on cyberwarfare and diplomacy argued that negotiations with the United States were only possible after

---

[53] Oleg Vladimirovich Ivannikov, *The Complex Character of Information Warfare in the Caucasus: A Social-Philosophical Perspective [Комплексный характер информационной войны на Кавказе: Социально-философские аспекты]*, Rostov-on-Don, Russia: Southern Federal University [Южный Федеральный Университет], July 3, 2008. Ivannikov reportedly served as South Ossetia's de facto defense minister between 2004 and 2008, a period that seemed to garner at least some praise from other Russian military figures in terms of information confrontation ("MH17—Russian GRU Commander 'Orion' Identified as Oleg Ivannikov," Bellingcat, May 25, 2018).

[54] Vladimir Mukhin, "Bet on an Informational Spetsnaz [Ставка на информационный спецназ]," *Independent Military Review [Независимое военное обозрение]*, No. 14, April 17, 2015, p. 1.

[55] P. Antonovich, "Key Aspects of the Information War [Ключевые аспекты информационной войны]," *Army Digest, January [Армейский сборник]*, No. 1, 2014.

[56] Vasily Belozerov and Daria Kopylova, "Mass Media: Information Confrontation [СМИ: Информационное Противоборство]," *Orienteer [Ориентир]*, No. 5, May 2014.

Russia demonstrated an equal "information potential."[57] At least some Russian writings imply that Russia needed to move into social media space before the West could dominate this media. A former deputy director in the GRU, for example, claimed in 2016 that the West was deploying the potential of the internet, including blogs and such platforms as Twitter and Facebook, because—according to the author—biased and "specially fabricated" information, disseminated through these venues, could force adversaries to make poor decisions, destabilize countries, and even "eliminate regimes."[58]

The Russian military's embrace of using social media offensively is partly rooted in the perceived advantage of leveraging a relatively low-cost capability to undermine a conventionally predominant opponent while insulating state-sponsored actors from direct attribution. Even prior to the rise of social media, some military writings that examined U.S. doctrine identified the value of "information confrontation tools" (such as "manipulating information") that are "relatively low cost" and present an adversary with significant attribution challenges.[59] In 2015, Andrey Kartapalov, a senior Russian military officer, noted that the effects of online psychological operations could affect a particular audience before its members realized any attempt to influence them had occurred, adding that such propaganda could even obviate armed

---

[57] I. N. Dylevskii, V. O. Zapivakhin, S. A. Komov, S. V. Korotkov, and A. A. Krivchenko, "On the Dialectic of Deterrence and Prevention of Military Conflicts in the Information Age [О диалектике сдерживания и предотвращения военных конфликтов в информационную эру]," *Military Thought [Военная мысль]*, No. 7, 2016.

[58] Vyzcheslav Viktorovich Kondrashov, "Information Confrontation in the Cybernetic Space [Информационное противоборство в кибернетическом пространстве]," *Scientific-Research Center of Problems of National Security [Научно-исслеовательский центр проблем национальной безопасности]*, August 22, 2016. For Kondrashov's biography, see Municipal Information Library System of Volzhinskiy [Муниципальная Информационная Библиотечная Система г. Волский], "Kondrashov, Vyacheslav Viktorovich [Кондрашов Вячеслав Викторович]," webpage, February 21, 2018.

[59] S. Grinyaev, "Views of U.S. Military Experts on the Conduct of Information Confrontation [Взгляды военных экспертов США на ведение информационного противоборства]," *Foreign Military Observer [Зарубежное военное обозрение]*, No. 8, August 1, 2001.

conflict.[60] Generally, military authors have identified the following features as recommending social media as an information weapon:

- the low cost of social media operations in terms of both funds and personnel
- the wide potential reach of online information operations, especially considering the growing penetration of the internet
- the ability to react in real time and in places without physical presence
- the deniability of social media operations, given the difficulty in distinguishing ordinary activity from state-sponsored acts of information warfare
- the perception that psychological effects of online and social media are superior to those provided by traditional media because of the potential for packaging multimedia content in ways that achieve "additional emotional and psychological influence."[61]

## Conclusion

The evolution of Russian military thought on social media, both as a threat and a weapon, is intertwined with broader Russian concerns about the implications of advances in communications technology for

[60] A. V. Kartapolov, " Lessons of Military Conflicts and Prospects for the Development of Means and Methods of Conducting Them. Direct and Indirect Actions in Contemporary International Conflicts [Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах]," *Bulletin of the Academy of Military Science [Вестник Академии Военных Наук]*, No. 2, 2015. The author, Kartapalov, has since been elevated to a prominent position within Russia's information confrontation apparatus (see Chapter Three).

[61] Kartapolov, 2015; Makarenko, p. 432; A. Polskikh, "General Military Problems. On the Application of the Global Computing Network Internet in the Interest of Information Confrontation [Общипе военные проблемы. О применении глобальной компьютерной сети интернет в интересах информационного противоборства]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 7, July 31, 2005.

national security and domestic stability.[62] The Russian military's own experiences in Chechnya, Georgia, and Ukraine—along with what was observed during the Arab Spring—shaped Russian strategic thinking about the uses of social media in modern information confrontation. Furthermore, a consistent fixation on the possibility that NATO and the United States might use social media forums against Russia to spark popular unrest have birthed a virtual imperative for Russia to develop its own countermeasures and incorporate social media into its information confrontation arsenal.

---

[62] For a comprehensive account of the Kremlin's decisionmaking on the internet and national security, see Soldatov and Borogan, 2015.

CHAPTER THREE

# Russian Social Media–Based Information Warfare in Practice

Popular portrayals of the Russian disinformation machine at times imply an organized and well-resourced operation, capable of affecting behaviors and events around the world. Evidence paints a more nuanced picture: Despite its strengths, there are also distinct limitations to the power of Russia's information confrontation machine. Russia has a wider variety of official and unofficial actors to wage its information warfare than do Western countries. However, publicly available evidence indicates that these actors are not all seamlessly coordinated or particularly well funded. Although Russia has used a multitude of social media accounts to spread disinformation and propaganda on a great variety of subjects across multiple platforms and has reached broad and varied international audiences, this outreach does not equate to impact. The fullest display of Russian information warfare—with, almost certainly, the greatest impact—took place in Ukraine, where Russia integrated information and kinetic operations, using disinformation and propaganda both as strategic tools to shape political outcomes and as operational tools to undermine military morale. The impact of Russia's information operations in Western countries is less obvious and more difficult to assess. In this chapter, we examine the practical and more-detailed aspects of Russia's information operations on social media by addressing the details of Russia's information warfare, offering a sense of the scale of the activities, and providing observations on their impact.

## Russia's First Social Media–Based Activities

Russia's earliest online information operations were domestic ones: During the Chechen conflict in the late 1990s, both Russian state and pro-Russian nonstate actors attacked Chechen online media and other websites. Although best described as hacking, the actions appear to have been intended to provoke informational-psychological effects.[1] Subsequently, Russians also developed their social media toolkit domestically: Since about 2011, for example, such techniques as hijacking Twitter and Facebook conversations to flood out meaningful coordination of opposition activity began to be detected.[2] A year after his reelection, Putin had reportedly tasked Igor Sergun, then head of the GRU, to begin "repurposing cyberweapons previously used for psychological operations in war zones for use in electioneering"—after which Russian intelligence agencies began funding troll farms to expand psychological warfare in cyberspace.[3]

Russia's earliest online information operations abroad likely occurred some time between 2005 and 2008, stemming from tensions with Estonia and the Georgian War.[4] These efforts, which, involved DDoS attacks against targeted websites, were conducted by a mix of state actors and so-called patriotic hackers.[5] Farther from Russia's borders, the English-language operations by the IRA began sometime in

---

[1] "FSB Does Not See Violations of the Law in the Actions of the Tomsk Hackers Against the Site 'Caucus-Center' [ФСБ не видит нарушения закона в действиях томских хакеров против сайта «Кавказ-центр»]," Newsru.com, February 4, 2002; Daniil Turovsky, "Our Time to Serve Russia Has Arrived [0 Пришло наше время послужить России]," *Meduza*, August 7, 2018.

[2] Missimo Calabresi, "Inside Russia's Social Media War on America," *Time*, Vol. 189, No. 20, May 18, 2017; Miriam Elder, "Russians Fight Twitter and Facebook Battles over Putin Election," *The Guardian*, December 9, 2011.

[3] Calabresi, 2017.

[4] Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money: A Special Report Presented by the Interpreter, a Project of the Institute of Modern Russia*, New York: Institute of Modern Russia, 2014; Craig Timberg, "Russian Propaganda Effort Helped Spread 'Fake News' During Election, Experts Say," *Washington Post*, November 24, 2016.

[5] Pomerantsev and Weiss, 2014; Timberg, 2016.

2013, but at a "low level," according to the Oxford University's Computational Propaganda Research Project, one of two firms given access to IRA accounts by Facebook, Twitter, and Instagram.[6]

The most-expansive and most-aggressive uses of social media outside the former Soviet space occurred after the 2014 crisis in Ukraine. The Computational Propaganda Research Project, in seeking to track English-language activity, indicates that tweets "increased somewhat in early 2014, before ramping up dramatically at the end of 2014 into 2015." At the same time, postings expanded from Twitter to YouTube, Instagram, and Facebook.[7] In one of its earliest visible campaigns, the IRA stirred panic in a Louisiana town by spreading, via Twitter, claims of an alleged explosion at the Columbia Chemicals plant.[8] Russian state-sponsored operations on social media also appear to have begun in 2014, as a GRU campaign sought to discredit Ukraine's new government after the ouster of Viktor Yanukovych through the Maidan Revolution. According to documents obtained by the *Washington Post*, GRU operatives relied on a Facebook primer containing basic instructions on how to use the platform.[9]

## Who Conducts Social Media–Based Activities and Coordinates Campaigns

Russia's social media–based information warfare machinery involves three type of actors (Table 3.1). *State actors*—i.e., actors who are formally part of the Russian state—consist of civilian and military officials working in government agencies, such as the Ministry of Foreign Affairs and the intelligence services. *State-affiliated actors*—i.e., actors who routinely act on direction from the state but are not formally part of the state—

---

6 Howard et al., 2018, p. 9.

7 Howard et al., 2018, p. 9.

8 Rohan Smith, "Columbia Chemical Hoax Tracked to 'Troll Farm' Dubbed the Internet Research Agency," News.com, June 4, 2015.

9 Ellen Nakashima, "Inside a Russian Disinformation Campaign in Ukraine in 2014," *Washington Post*, December 25, 2017b.

**Table 3.1**
**Actors in Russia's Social Media Information Warfare**

| | Acting Overtly | Acting Covertly |
|---|---|---|
| State actors | • Civilian government officials (e.g., Ministry of Foreign Affairs social media accounts)<br>• Military public affairs | • GRU (e.g., APT28, DCLeaks, Russian compatriot organizations)<br>• Foreign Intelligence Service (SVR)<br>• Federal Security Service (FSB) |
| State-affiliated actors | • State-controlled media, domestic and foreign (e.g., RT, Sputnik)<br>• State-owned corporations (e.g., Gazprom)<br>• Other state-controlled or affiliated institutions | • IRA<br>• Some state-affiliated actors acting covertly (e.g., Facebook groups covertly created by Sputnik)<br>• Freelancers (e.g., patriotic bloggers or hackers, oligarchs) |
| State-unaffiliated actors | • Other freelancers: patriotic bloggers and hackers; activists and radical groups, businessmen, criminals | |

consist of state-controlled media, state-owned corporations, and other directed parties. The media outlets include, most notably, RT (formerly *Russia Today*, a media outlet that operates eight television channels with digital platforms in six languages and a video news agency[10]) and Sputnik (a news organization that operates newswires, websites, social networks, mobile apps, radio broadcasts and multimedia press centers in multiple languages);[11] both outlets are "deeply integrated with social media."[12] The state-affiliated corporations include Gazprom and other state-con-

[10] RT, "About RT," webpage, undated.

[11] Sputnik, "About Us," webpage, undated.

[12] VGTRK is the All-Russia State Television and Radio Broadcasting Company, which operates Russia's state television and radio channels. RT (formerly Russia Today) and Sputnik are

> both deeply integrated with social media. . . . RT . . . calls itself 'essentially an internet media company'. RT claims that its presence on YouTube is even higher than on TV, although this statistic might be overestimated because of RT's wish to present itself as one of the leading channels globally, as leaked documents reveal (Anna Reynolds, ed., *Social Media as a Tool of Hybrid Warfare*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, May 2016, p. 25).

trolled institutions.[13] This also includes various groups and individuals, who appear to be freelancing, but might also be acting on direction from state officials.[14] Finally, *state-unaffiliated actors*—i.e., actors who do not routinely act on direction from state officials but might coordinate actions with state or state-affiliated actors on an ad hoc basis—are a variety of freelancers, such as bloggers, hackers, activists, and businessmen.[15] Entities that successfully obscure their connection to the Russian state would be considered unaffiliated, unless or until evidence emerges linking them to the state.[16]

---

[13] For example, the Russian Institute for Strategic Studies (RISI) is a state-founded think tank, led by retired foreign intelligence officials. According to some U.S. officials, RISI created the framework for interference with the U.S. presidential election. "Putin-Linked Think Tank Drew up Plan to Sway 2016 US Election—Documents," Reuters, April 19, 2017.

[14] Daniil Turovsky, "Our Time to Serve Russia Has Arrived [Пришло наше время послужить России]," Meduza, August 7, 2018a. Other freelancers are oligarchs—such as Konstantin Malofeev, a Russian businessman with ties to the Kremlin who was implicated in a scheme to fund anti-Ukrainian rallies and protests in Poland (Aleksey Dzikavitskiy and Yaroslav Shimov, "Knights of the 'Russian World' [Рыцари «русского мира»]," Radio Svoboda [Радио Свобода], March 2, 2017).

[15] For example, the Siberian Network Brigade, a group of students at Tomsk University that supported Russia during and after the Second Chechen War, provides a clear example of activists who operated without direct guidance from the Russian state, at least at the outset. Turovsky, 2018a. The pro-Russian blog Stalkerzone.org is also "not directly funded by the Kremlin," but is "run by Oleg Tsarov, a pro-Russian separatist in eastern Ukraine" (Bret Schafer, *View from the Digital Trenches—Lessons from Year One of Hamilton 68*, Washington, D.C.: The German Marshall Fund of the United States, November 19, 2018, p. 9). Another example is South Front, a military affairs website registered in Moscow in April 2015, that has consistently published articles that reinforce Kremlin messaging; at least one expert (in the U.S. State Department) claimed that it was linked to the state (Ben Schreckinger, "How Russia Targets the U.S. Military," *Politico Magazine*, June 12, 2017). For a detailed account of how Russian criminals supported Kremlin efforts in both technical and psychological cyberoperations, see Daniil Turovsky, *Invasion: A Short History of Russian Hackers [Вторжение: Краткая История Русских Хакеров]*, Moscow: Inviduum Publishing [Индивидуум паблишинг], 2019.

[16] For example, Baltnews, news websites formed in 2014, presented themselves as independent media organizations—or unaffiliated actors—in the Baltic states. In 2018, investigative journalism uncovered evidence that tied these sites to Russian state-owned news agency Rossiya Segodnya (meaning they were state-affiliated actors). See Holger Roonemaa and Inga Springe, "This Is How Russian Propaganda Actually Works in the 21st Century," *BuzzFeed News*, August 31, 2018.

Some of these actors operate overtly—that is, their identities are not obscured. For example, the military openly runs the Zvezda (Star) broadcasting service, the Defense Ministry operates a YouTube channel and associated social media accounts, and RT and Sputnik report openly. All of these actors also operate covertly, without such transparency: For example, the GRU acts through a variety of proxies such as Advanced Persistent Threat (APT) 28, DCLeaks, and Russian compatriot organizations; IRA trolls and state-affiliated media both impersonate authentic social media accounts or pages.[17] For outside observers, the distinctions among these three groups might be blurry because an actor might be secretly taking directions from the Russian state or spreading pro-Russian and Russian-origin content on his own initiative. Moreover, the large universe of individuals who disseminate Kremlin-friendly views can complicate the question of who qualifies as a state-unaffiliated actor. In this report, we treat individuals who disseminate such content in order to advance Moscow's interests or curry favor with the state as parts of Russia's information warrior ranks; we exclude those who do so entirely for their own reasons, often unwittingly. An accurate assessment of threat requires a good-faith effort to determine precisely the status of any given individual, even if we are ultimately unable to assess the side of the line on which he or she falls.[18] Sweeping in all voices that spread Russian messaging would inflate the scale of the threat; excluding them would understate it.

---

[17] ODNI, 2017, p. ii. Russian organizations aimed at Russian expatriates abroad, such as InfoRos and the Institute of the Russian Diaspora, claim to be public diplomacy organizations but have been linked to the GRU (Anton Troianovski and Ellen Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West," *Washington Post*, December 28, 2018). In an example of state-affiliated media acting covertly, Facebook recently took down 364 pages operating in the FSU (as well as Central and Eastern Europe), that were covertly set up by Sputnik (Adam Satariano, "Facebook Identifies Russia-Linked Misinformation Campaign," *New York Times,* January 17, 2019; Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior from Russia," Facebook Newsroom, January 17, 2019).

[18] For an explanation of why the distinction is important in the context of Twitter, see Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, RR-2237-OSD, 2018, p. 67.

Many of Russia's information efforts are waged by a variety of these state and nonstate actors, often on an ad hoc basis. Mark Galeotti, for example, observes that "the majority of ventures come from the initiative of individuals within and without the government apparatus, guided by their sense of the Kremlin's desires rather than any detailed master plan."[19] Similarly, Constanze Stelzenmüller, a German expert on Russia's influence efforts in Europe, describes the execution of information operations as being "more often than not loosely organized, and delegated to a broad variety of actors," some of whom "are tied closely into a chain of command, others are linked much more tenuously to government authorities."[20]

This ad hoc approach is largely intentional (Figure 3.1). A loose constellation of actors allows Putin to point to potential Russian "patriots" who "fight against those who say bad things about Russia," while denying any direct Kremlin involvement.[21] Informal arrangements with such patriots appear rooted in the Chechen conflict and likely continue to shape both offensive cyberoperations and online information activity (at least in FSB's operations).[22] The difficulty in distinguishing state-unaffiliated actors from state or state-affiliated actors—or from genuinely independent voices—increases the challenge of credibly countering Russia's denials.[23]

---

[19] Mark Galeotti, *Controlling Chaos: How Russia Manages its Political War in Europe*, London, United Kingdom: European Council on Foreign Relations, September 2017.

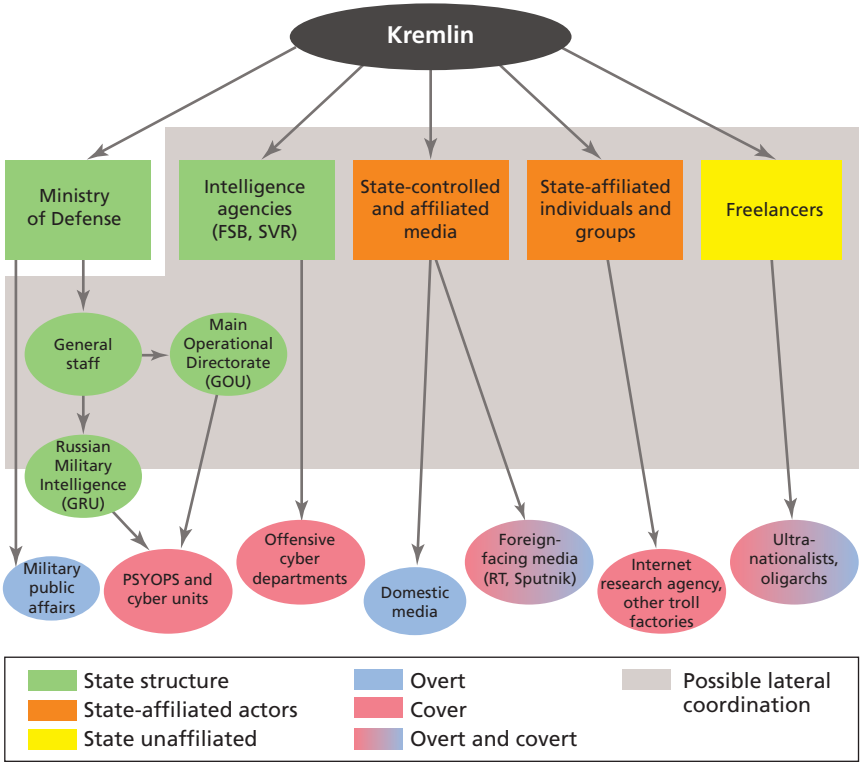
[20] See Constanze Stelzenmüller, "The Impact of Russian Interference on Germany's 2017 Elections," testimony presented before the U.S. Senate Select Committee on Intelligence, June 28, 2017; and Naja Bentzen, *Foreign Influence Operations in the EU*, Brussels, Belgium: European Parliamentary Research Service, July 2018, p. 5.

[21] Euan McKirdy, "Putin: 'Patriotic Russian Hackers May Have Targeted U.S. Election," CNN, June 2, 2017.

[22] Andrew E. Kramer, "How Russia Recruited Elite Hackers for Its Cyberwar," *New York Times*, December 29, 2016.

[23] Stelzenmüller, 2017; Mark Galeotti, "The 'Trump Dossier,' or How Russia Helped America Break Itself," *Tablet Magazine*, June 13, 2017b.

**Figure 3.1**
**Russia's Information Warfare Machinery**




## Operation and Coordination Within the Russian State

Even within the Russian state, an opaque shell of operational security surrounds Russia's command-and-control scheme as it relates to conducting cyber and digital influence operations. Wide discrepancies in levels of awareness and contribution likely distinguish planners from the network of operators within Russia's information confrontation machine.[24]

[24] This is especially true for the information-technical component of these efforts, which falls on the shoulders of a wide array of partners. For a snapshot of Russia's efforts to corral public and private enterprises to conduct cyberoperations, see Kramer, 2016; Turovsky, 2018a.

Publicly available evidence suggests that the Ministry of Defense (the GRU in particular) emerged after the 2008 Georgian War as a key state actor in the domain of digital psychological warfare.[25] Russia's military has historically been a key actor in offensive psychological operations: Shortly before World War II, the Red Army established a "special propaganda" directorate and was tasked with highly sensitive missions under the general rubric of "political work."[26] In 1991, these special propaganda units were reassigned to the GRU under the auspices of the Center for Foreign Military Information and Communication.[27] It is believed, for instance, that the GRU's 72nd Special Service Center (or Unit 54777) was responsible for activity in Ukraine after 2014 and is likely responsible for digital influence operations aimed at the United States and for offensive information-psychological operations.[28] The GRU's likely cyberfocused units (e.g., Units 26165 and 74455) also participate in social media influence operations.[29] For example, an investigation conducted by the University of Toronto's Citizen Lab in 2017 revealed an information campaign aimed at more than 200 targets from 39 countries that involved sophisticated hack-and-leak techniques; Citizen Lab attributed this campaign to CyberBerkut, an ostensibly pro-Russian hacktivist group that the UK National Cyber Security Centre later linked to the GRU.[30]

---

[25] Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations*, Washington, D.C., 2017, p. 74.

[26] "Special Front [Особый фронт]," *Arguments of Time [Аргументы времени]*, October 1, 2018.

[27] Nikolay Pushkarev, "The Activities of Military Intelligence During the Fall of the Soviet Union [Деятельность военной разведки в период Распада СССР]," *GRU: Inventions and Reality [ГРУ: вымысли и реальность]* Moscow: Eksmo [Эксмо], 2004; "Special Front . . ." 2018.

[28] Troianovski and Nakashima, 2018.

[29] U.S. Department of Justice, Office of Public Affairs, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," press release, October 4, 2018.

[30] National Cyber Security Centre, "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed," October 3, 2018; Adam Hulcoop, John Scott-Railton,

In 2009, Russia's military stood up the Zvezda broadcasting service, which runs programs on television, radio, and a website and which is mostly funded by state subsidies and contracts with the defense ministry,[31] although audiences for any of Zvezda's platforms are small compared with more-popular Russian media outlets.[32] The Defense Ministry's official YouTube channel and associated social media accounts enjoy more success. As of mid-2019, that YouTube channel has 137,000 subscribers and 154 million views, which is reportedly more popular than the DoD official YouTube channel.[33] Zvezda's website attracts between 360,000 and 380,000 visitors a day; China's equivalent (China Military Online) brings in 60,000–80,000—although Zvezda appears to go after a broader audience than China Military Online.[34]

In 2013, Defense Minister Sergey Shoygu reportedly inaugurated a "big hunt" for programmers to join Russia's military, having earlier ordered the Main Operational Directorate (GOU) of the General Staff to develop a cybercommand "as soon as possible."[35] Deputy Prime Minister Dmitriy Rogozin simultaneously announced plans to create a cyberforce.[36] The force would have both technical and psychological warfare mandates, and would involve everything from network

---

Peter Tanchak, Matt Brooks, and Ron Deibert, "Tainted Leaks: Disinformation and Phishing with a Russian Nexus," The Citizen Lab, University of Toronto, May 25, 2017.

[31] Pavel Luzin, "How Successful Is Russia's Military Propaganda Media?" *Moscow Times*, July 10, 2019.

[32] Zvezda consistently fails to make the top 100 most-popular television channels. Luzin, 2019.

[33] The latter was reported to have 87,000 subscribers and slightly more than 17 million views as of summer of 2019. Luzin, 2019.

[34] Luzin, 2019.

[35] "Cyber-Forces Will Appear in the Army Before the End of the Year [Кибервойска появятся в армии до конца года]," *Moscow 24 [Москва 24]*, July 5, 2013; "Russia Is Creating a Cyber-Force [Россия создает кибервойска]," *Military Review [Военное обозрение]*, August 8, 2013.

[36] "Cyber-Forces Will Appear . . .", 2013; "Russia Is Creating . . .", 2013.

security to information operations.[37] Probably between 2014 and 2017, Russia's military established such a force, called the Information Operations Troops (Войска Информационных Операций).[38] How that force fits into the existing military structure remains unclear.[39]

The information operations troops participated in a large-scale wargame in 2016, where Gerasimov explained that the General Staff's GOU would function as the coordinating body for information confrontation.[40] Gerasimov similarly revealed that subordinate "information confrontation centers" (центры информационного противоборства) established in each of Russia's four main military districts, supplemented by information operations troops, electronic warfare units, and information security specialists, would wage information confrontation in Russia's military, which had the same importance as military units focused on planning kinetic attacks against potential adversaries.[41] According to Estonian and Ukrainian sources,

---

[37] "In the Armed Forces They Are Creating a Force of Information Operations [в Вооруженных силах создают войска информационных операций]," *Independent Military Review [Независимое военное обозрение]*, May 16, 2014; "The Russian Ministry of Defense Is Working on the Option of Creating Humanitarian Scientific Companies [Минобороны России прорабатывает вариант создания гуманитарных научных рот]," TASS, July 10, 2013.

[38] "Minister of Defense of the Russian Federation Created Troops for Information Operations [В Минобороны РФ создали войска информационных операций]," Interfax [Интерфакс], February 22, 2017; "Source in Ministry of Defense: The Armed Forces of the Russian Federation are Creation Troops for Information Operations [Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций]," TASS, May 12, 2014.

[39] Maria Latsinskaya, Aleksandr Braterskiy, and Ignat Kalinin, "Russia Introduced a Force to the Internet [Россия ввела войска в интернет]," Gazeta.ru, February 22, 2017; Daniil Turovsky, "The GRU—What's to It? Whom Do They Recruit as Spies? And Why Are They So Often Revealed? [ГРУ— это вообще что? Кого берут в шпионы? И почему их так часто раскрывают?]," *Meduza*, October 15, 2018.

[40] This was revealed in a large-scale military exercise in 2016. "Information Confrontation Was Worked Out at 'Caucasus 2016' [Информационное противоборство отработали на «Кавказе-2016»]," *Izvestiya [Известия]*, September 14, 2016; Defense Intelligence Agency, 2017, p. 38.

[41] "At the Exercises of 'Caucasus-2016' They Worked Out 'Information Confrontation' for the First Time [На учениях «Кавказ-2016» впервые отработали «информационное

Russia's military established an information confrontation center near Ukraine a year prior to Gerasimov's announcement and then expanded the model to other military districts in 2016 with the ultimate purpose of discrediting political leadership in a targeted state, sowing distrust of its military's leaders, and demoralizing its public and rank-and-file military service members.[42]

Command-and-control efforts beyond the military are more ambiguous. At the operational level, nonmilitary intelligence agencies—i.e., the FSB and the SVR—likely play a more limited role in social media–related information warfare. As Russian security expert Galeotti explains, these agencies "have overlapping responsibilities (even the FSB is increasingly involved in foreign operations)"—and they "compete fiercely and ruthlessly to outshine the others" in Putin's eyes.[43] Considering the attention accorded to information operations, it is unlikely that these agencies simply cede the ground to the GRU.[44] At the same time, there is reason to believe that at least the FSB tends to concentrate more on computer espionage and exploiting strategic targets than digital influence operations.[45]

The FSB does participate in some influence operations abroad.[46] Domestically, the FSB has responded to the perceived threat of social

---

противоборство»]," *RIA Novosti [РИА Новости]*, September 14, 2016.

[42] Department of External Intelligence of Estonia [Департамент внешней разведки Эстонии], *Estonia in International Security Environment 2018 [Эстония в Международной Среде Безопастности 2018]*, Tallinn, Estonia, 2018, p. 29; "Putin's Propagandists Filmed a New Fake in the Donbas: Details From Intelligence [Пропагандисты Путина отсняли на Донбассе новый фейк: подробности от разведки]," Online.ua, July 29, 2016.

[43] Mark Galeotti, "Russian Intelligence Is at (Political) War," *NATO Review Magazine*, May 12, 2017a.

[44] Galeotti, 2017a.

[45] A comparison of an intrusion set associated with Russia's FSB through the activity of FancyBear, attributed to the GRU, reinforces this notion. See Catalin Cimpanu, "Russia's Elite Hacking Unit Has Been Silent, but Busy," *Zero Day*, October 5, 2018; and Cyber Operations Tracker, "Turla," webpage, undated.

[46] Among the more notorious foreign activities by the FSB are the poisoning of ex-spy Litvinenko and ties with alleged Russian spy Maria Butina. See Moscow Project, "Russia's Three Intelligence Agencies, Explained," October 12, 2018.

media in instigating opposition since the 2011 protests, and because Moscow often treats its former Soviet neighborhood as an extension of Russia, the FSB might have something of a role in social media influence operations, particularly in its near abroad. Our interviews suggested that there was FSB social media activity in Ukraine and Belarus—although it is unclear whether that activity is driven by intelligence or information warfare goals, and the evidence for FSB involvement is not clear cut.[47] Insofar as the collection of *kompromat* (blackmail material) is a classic FSB function, the FSB is well resourced to orchestrate leaks via social media or otherwise repurpose the material for disinformation or intimidation.[48] Which parts of the FSB might be running social media operations is opaque, as is the activity itself. For instance, correspondence between a Russian programmer who developed social media–monitoring software and the FSB in 2011 showed that the FSB's Center for Information Security is probably the organization's leading office on social media issues.[49] But in mid-2019, when independent hackers obtained 7.5 terabytes of information related to FSB projects that included social media–scraping and securing Russia's internet from the larger global network, these projects were connected to the FSB's Center 16, a branch known to conduct signals intelligence and accused of sending malware to Ukrainian intelligence officers in 2015.[50]

Likewise, the SVR likely participates in influence operations abroad—including digital ones, although probably to a limited extent.

---

[47] Interview with Ukrainian NGO officials, Kyiv, Ukraine, March 5, 2019; interview with Ukrainian government official, Kyiv, Ukraine, March 5, 2019; interview with Ukrainian information technology research firm officials, Kyiv, Ukraine, March 7, 2019; interview with Ukrainian internet experts, Kyiv, Ukraine, March 7, 2019.

[48] Moscow Project, 2018.

[49] Soldatov and Borogan, 2015, p. 127. The Center for Information Security is alternatively known as Center 18, as evidenced by the arrest of the former head of the department, Sergey Mikhailov, in late 2016. See Alya Ponomaryova, "Humpty-Dumpty Under the 'Cover' of the FSB [Шалтай-Болтай под «крышей» ФСБ]," Radio Svoboda [Радио Свобода], January 26, 2017.

[50] Zak Doffman, "Russia's Secret Intelligence Agency Hacked: 'Largest Data Breach in Its History,'" *Forbes*, July 20, 2019.

Revelations from a defector showed a limited online influence effort run out of the SVR's United Nations office in New York as early as the mid-1990s.[51] The SVR inherited the KGB's old Section A, First Chief Directorate, which was responsible for disinformation during the Cold War.[52] One of the actors responsible for the 2015 Democratic National Committee (DNC) hack—Cozy Bear, or APT29—is largely attributed to the SVR.[53] Although the evidence is murky, the SVR also is alleged to have circulated a false intelligence report related to the murder of former DNC staffer Seth Rich in 2016, according to a former assistant U.S. attorney who led the murder investigation.[54]

Finally, the U.S. intelligence community concluded that President Putin personally authorized the effort to interfere in the 2016 U.S. presidential elections.[55] This suggests that senior Kremlin leadership are at least occasionally involved in information confrontation campaigns. Certain figures close to Putin probably have significant roles in coordinating activity between state and state-affiliated actors. Vladislav Surkov, for instance, is an alumnus of the GRU and a personal adviser to Putin; thus, he is probably a well-positioned interlocutor for coordinating these operations at a senior level.[56] Ultimately, however, the extent to which the Kremlin becomes involved in lower-profile actions remains unclear.

---

[51] Pete Earley, *Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War*, New York: Berkley, 2006, p. 194.

[52] Yevhen Fedchenko, "Kremlin Propaganda: Soviet Active Measures by Other Means," Stopfake.org, March 21, 2016.

[53] Moscow Project, 2018; Ellen Nakashima, "U.S. Identifies Russian Government Hackers Who Accessed DNC Computers," *Washington Post*, November 3, 2017a. Also see Huib Modderkolk, "Dutch Agencies Provide Crucial Intel About Russia's Interference in US-Elections," *de Volksrant*, January 25, 2018.

[54] Michael Isikoff, "Exclusive: The True Origins of the Seth Rich Conspiracy Theory," Yahoo News, July 9, 2019; Philip Bump, "Don't Blame the Seth Rich Conspiracy on Russians. Blame Americans," *Washington Post*, July 9, 2019.

[55] ODNI, 2017.

[56] "What's Known About Vladislav Surkov [Чем известен Владислав Сурков]," *Kommersant [Коммерсантъ]*, May 24, 2019; "Surkov Declared Putinism the Ideology of the Future [Сурков объявил путинизм идеологией будущего]," Lenta.ru, February 11, 2019.

### Operation and Coordination of State-Affiliated Actors

Two sets of known state-affiliated actors play significant roles in information warfare generally and in social media in particular. The first set consists of state-sponsored media organizations—specifically, RT and Sputnik, both of which have been described as Russia's propaganda and disinformation machines.[57] These organizations employ social media to disseminate a wide variety of pro-Russian, anti-Western, divisive, and false and misleading content, which often enjoys greater popularity than it would if distributed by traditional media channels. In 2017, the U.S. intelligence community cited RT's estimates that its videos received more than 800 million views on YouTube between roughly 2005 and 2012, which reflects the highest levels among major international news outlets, such as BBC or CNN—although RT's apolitical "clickbait" content appears to be a major driver of RT's online viewership.[58] As of early 2019, RT further expanded its footprint on Facebook with three new video channels targeting millennials in the United States.[59] The channels' producer, Maffick Media, was reportedly beholden to a video news agency that is a subsidiary of RT; although online only for a couple of months, these channels gained 30 million video views.[60]

RT, Sputnik, and affiliated actors often act overtly, posting on social media under their true organizational identities. As *New York Times* columnist Jim Rutenburg points out, "[t]his makes RT and Sputnik harder for the West to combat than shadowy hackers. You can tighten your internet security protocols to protect against data breaches, run counterhacking operations to take out infiltrators, sanction countries with proven links to such activities. But RT and Sputnik

---

[57] Jeremy Diamond, "Intel Report: Putin Directly Ordered Effort to Influence Election," CNN, January 6, 2017; Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, August 28, 2016.

[58] ODNI, 2017; Robert Orttung, Elizabeth Nelson, and Anthony Livshen, "How Russia Today Is Using YouTube," *Washington Post*, March 23, 2015.

[59] Donie O'Sullivan, Drew Griffin, Curt Devine, and Atika Shubert, "Russia Is Backing a Viral Video Company Aimed at American Millennials," CNN Business, February 18, 2019.

[60] O'Sullivan et al., 2019.

operate on the stated terms of Western liberal democracy; they count themselves as news organizations, protected by the First Amendment and the libertarian ethos of the internet."[61] However, RT and Sputnik have also acted covertly. For example, Facebook recently took down 364 pages that were covertly set up by Sputnik and had been operating in the former Soviet Union (and in Central and Eastern Europe) over the past few years.[62]

The second set of state-affiliated actors that played a significant role is troll farms. These originated in Russia within the first decade of the century, and were used to undermine commercial and political rivals, much like the roughly contemporaneous evolution of DDoS cyberattacks in Russia.[63] The best known of these entities is the IRA, allegedly started some time after 2012 by a Putin crony, Yevgeniy Prigozhin—reportedly without instructions from the Kremlin.[64] Although Russian corporate records indicate that the IRA has been technically defunct since late 2016, the organization appears to operate under a new name. As Glavset, it has been active since 2015; as of 2017, it was run by the former head of the IRA, Mikhail Bystrov.[65] Another group that was active on social media is the now-disbanded pro-Kremlin youth organization Nashi.[66] In 2012, hacked emails revealed a payment scheme arranged by Nashi's leadership—principally its original leader, Vasily Yakemenko, and its spokesperson, Kristina Potupchik—that rewarded bloggers and activists for posting pro-Kremlin material online, such as campaigns to denigrate

---

61 Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *New York Times*, September 13, 2017.

62 Satariano, 2019; Gleicher, 2019.

63 Soldatov and Borogan, 2015; Turovsky, 2019.

64 Mikhail Mettsel, "An Accomplice to the Founder of Russia's 'Troll Factory' Says the Organization Was Created Without Kremlin Instructions," *Meduza*, November 8, 2018.

65 Issie Lapowsky, "Facebook May Have More Russian Troll Farms to Worry About," *Wired*, September 8, 2017.

66 Daisy Sindelar, "The Kremlin's Troll Army: Moscow Is Financing Legions of Pro-Russia Internet Commenters. But How Much Do They Matter?" *The Atlantic*, August 12, 2014.

Russia's leading oppositionist, Alexey Navalny, and other human rights activists, journalists, bloggers, film directors, and literary figures.[67]

Command and coordination of these actors is difficult to discern. Editors receive verbal guidance from the Kremlin as to what themes to cover (in the form of a verbal *temnik*—"theme book" or "list"), but it is unclear how much Kremlin direction there is for any specific social media operation.[68] Operators of media channels likely anticipate what messaging would be favorably received by the Kremlin and what content to avoid without explicit direction. The Kremlin also staffs RT with people aligned with Russian officials' worldview and pays close attention to the network's broadcasts.[69] Margarita Simonyan, the head of the network, reportedly enjoys a close relationship with Presidential Administration Deputy Chief of Staff Aleksey Gromov—who was also sanctioned by the European Union (EU) in 2014 for "instructing Russian media outlets to take a line favorable with the separatists in Ukraine and the annexation of Crimea."[70] According to Simonyan, RT fulfills tasks given by the state because that is the source of the network's funding.[71] According to another senior Russian media official, RT's stories are developed exclusively in the outlet's Moscow office.[72]

---

[67] Miriam Elder, "Emails Give Insight into Kremlin Youth Group's Priorities, Means and Concerns," *The Guardian*, February 7, 2012a.

[68] "Temnik—the Kremlin's Route to Media Control," *EU vs. Disinfo*, March 29, 2017; Dmitriy Skorobutov, "Confession of a Propagandist. Part I. How to Make News on Government TV [Исповедь пропагандиста. Часть I. Как делают новости на государственном ТВ]," *The Insider*, June 9, 2017. Also see Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*, New York: PublicAffairs, 2015. Additionally, as ODNI, 2017, recounts,

> According to Simonyan, Gromov oversees political coverage on TV, and he has periodic meetings with media managers where he shares classified information and discusses their coverage plans. Some opposition journalists, including Andrey Loshak, claim that he also ordered media attacks on opposition figures.

[69] ODNI, 2017.

[70] ODNI, 2017, p. 9; "EU Releases New Sanctions List," Radio Free Europe/Radio Liberty, July 30, 2014.

[71] ODNI, 2017.

[72] ODNI, 2017.

Although the U.S. intelligence community was highly confident that Putin personally ordered the effort to undermine the 2016 presidential elections, the link between Putin and the operations of Prigozhin's IRA remains obscure.[73] A former IRA blogger who exposed some of the agency's operations in 2015 observed, "[i]t is laughable when Putin says that we do not know about trolls or trolls do not exist . . . because when anyone looks through the Kremlin-controlled newspapers or state television, they can see that the propaganda in that media is the exact same stuff that the trolls are posting."[74] The link between the IRA's operations and Prigozhin is more clearly established: A U.S. Department of Justice indictment in 2018 specified that Mikhail Bystrov, the IRA's highest-ranking manager in 2016, communicated frequently with Prigozhin about the state of Project Lakhta, the effort to undermine the 2016 U.S. presidential election.[75]

### Operation and Coordination of Unaffiliated Actors

Russians have frequently and independently supported their government through digital means, including such groups as the Siberian Network Brigade (a group of Russian university students who began launching DDoS attacks against pro-Chechen websites during the Second Chechen War), the Nashi youth movement, and other organizations that lend their support or amplify state messaging only on specific issues that resonate with that group. Although the Kremlin cannot maintain contact with all these groups, they nonetheless play an important—if ad hoc—role in Russian information efforts.

Ukrainian security experts, for example, believed that Russia's intelligence services as of early 2019 had started "outsourcing" much of their digital propaganda efforts to "younger creative people."[76] Simi-

---

[73] "Yle Kioski Traces the Origins of Russian Social Media Propaganda—Never-Before Seen Material from the Troll Factory," *Kioski*, February 20, 2015.

[74] Jolie Myers, "Meet The Activist Who Uncovered The Russian Troll Factory Named in the Mueller Probe," NPR, March 15, 2018.

[75] *United States v. Internet Research Agency*, indictment, case 1:18-cr-00032-DLF, D.D.C., February 16, 2018, p. 8.

[76] Interview with Ukrainian security experts, Kyiv, Ukraine, February 6, 2019.

larly, since mid-2018, Russian agents reportedly tried to recruit popular Belarusian bloggers and the owners of popular social media groups to expand Russian messaging in Belarus.[77] In at least one instance, a would-be buyer of independent blog services self-identified as a representative of Russia's Sputnik news agency.[78] In some ways, these tactics resemble efforts by Russian intelligence and security services to recruit or coerce freelance hackers into working for their cyberoperations.[79]

There are numerous examples of independent actors (or those with unknown affiliation to the state) on social media doing Moscow's bidding. Analysts assess that the '#SyriaHoax' hashtag used on Twitter (disseminating a claim by a website supporting Syrian President Bashar al-Assad that videos of a 2017 chemical attack on civilians were fake) was originally part of a state-backed influence campaign. Subsequently, however, it was picked up by a variety of actors—doubtless, some disseminated the message for their own purposes, but others were likely serving Moscow's interest without explicit directives.[80] Similarly, a candid cell phone conversation between Victoria Nuland, the former U.S. assistant secretary of State for Europe, and Geoffrey Pyatt, the U.S. ambassador to Ukraine, was infamously leaked and posted anonymously on YouTube—and originally reposted by a popular pro-Kremlin troll account (Lev Mishkin—a reference to the main character in Fyodor Dostoevsky's *The Idiot*).[81] The senior diplomats' conversation contained frank discussion about Ukraine's fiscal and political situation in 2014 and disparaged the EU; Mishkin's reposting caused it to go viral.[82] Regardless of who

---

[77] International Strategic Action Network for Security, *Coercion to "Integration": Russia's Creeping Assault on the Sovereignty of Belarus*, Warsaw, Poland, February 2019, p. 44.

[78] International Strategic Action Network for Security, 2019, p. 46.

[79] Turovsky, 2019.

[80] Brian Ross, Megan Christie, and James Gordon Meek, "Behind #SyriaHoax and the Russian Propaganda Onslaught," ABC News, April 13, 2017.

[81] Fyodor Dostoevsky, *The Idiot: A Novel in Four Parts [Идиот: Роман в четырех частях]*, Moscow: Sciences Publishing House [Издательный дом «НАУКА»], reprint 1988.

[82] Anne Gearan, "In Recording of U.S. Diplomat, Blunt Talk on Ukraine," *Washington Post*, February 6, 2014; Soldatov and Borogan, 2015, p. 286.

was responsible for recording the conversation, such actors as Mishkin are often neither part of the Russian state nor in need of explicit direction from the Kremlin.[83]

### Possible Lateral Coordination

There might be a level of lateral coordination among the key sets of actors (state, state-affiliated, and unaffiliated) below the level of the Kremlin.[84] The IRA rebroadcasting Sputnik and RT material on social media fails to indicate any specific cooperation at a higher level, but there are other—albeit circumstantial—indications that such cooperation exists sometimes. New Knowledge, a cybersecurity research firm given access to some of the IRA social media accounts used to interfere in the U.S. elections, suggests that the IRA was tasked with boosting the reputation of Wikileaks and Julian Assange days prior to the document-dumps facilitated by the GRU's hackers, given the timing of IRA posts.[85] DFRLab offers an example of Russian diplomatic missions following an IRA account and amplifying the disinformation.[86] DFRLab also picked up on a piece of evidence that some coordination might occur in advance: For example, an IRA troll account disseminated content honoring Russian diplomats—claiming that this was "with the support of foreign representations of the Russian Foreign Ministry."[87] Accounts held by the Foreign Ministry, Consulate General in Geneva, and Embassy in South Africa appeared to confirm this

[83] Although this incident is commonly attributed to the Russian security services, there is some disagreement about who is responsible for the eavesdropping on the call. See Soldatov and Borogan, 2015, pp. 285–287.

[84] Galeotti, 2017c.

[85] Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson, *The Tactics & Tropes of the Internet Research Agency*, New Knowledge, December 17, 2018, p. 67.

[86] DFRLab, "Russia's Full Spectrum Propaganda: A Case Study in How Russia's Propaganda Machine Works," *Medium*, January 23, 2018a.

[87] DFRLab, 2018a.

claim of prior approval for this IRA actor.[88] Similar coordination is certainly plausible behind less benign information campaigns.

More often, campaigns that appear coordinated consist of ad hoc—and post hoc—actions by actors seizing opportunities created by others. In Germany's notorious 2016 Lisa case, as Galeotti points out, original social media accounts of a fabricated story that a Russian-German girl was raped by Arab or Muslim immigrants were picked up by the Russian media and cited by Sergei Lavrov, Russia's foreign minister. In this case, as in many others, "initiative is taken by individual agents and actors," and the "government was simply reacting to, and trying to exploit, something that started independently."[89] But other cases suggest a lack of coordination where it should have been possible: For example, the sometimes concurrent and redundant operations of the GRU, the IRA, and APT29 in targeting the 2016 U.S. presidential election probably demonstrated some degree of disconnect.[90]

## Scale of Russian Social Media Information Warfare

Obvious difficulties arise when attempting precise determinations of the people and resources that Moscow has at its disposal specifically to spread disinformation through social media. Among these difficulties are the high levels of secrecy that Russian officials assign to influence activities and the involvement of numerous nonstate actors. As we noted in Chapter One, Russia does not firmly distinguish between cyber and information warfare or between information-technical and information-psychological activities. Thus, when it comes to assessing the resources or capabilities used or available for disinformation on social media, we concluded that it is not possible or useful to separate the two aspects.

---

88 DFRLab, 2018a.

89 Galeotti, 2017c.

90 Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *CrowdStrike*, June 15, 2016. Similarly, DFRLab details two parallel and similarly themed digital influence efforts conducted by the GRU and IRA, see DFRLab, "#TrollTracker: Russia's Other Troll Team," *Medium*, August 2, 2018e.

Therefore, assessing the scale of Russia's social media disinformation apparatus in relative terms is difficult. Were we to compare the scale of the broad set of capabilities that have contributed to Russian social media activity (i.e., information-technical and information-psychological), then, as evidence suggests, Russia's investment is likely modest compared with analogous capabilities possessed by its rivals. However, these rivals, such as the United States, do not and likely would not use some of the analogous capabilities for information efforts on social media, rendering the comparison not entirely informative. It is difficult to frame a comparison focused narrowly on known spending on activities that take place at least in part on or through social media—because most of its rivals do not, to our knowledge, conduct extensive disinformation on social media. Importantly, much of Russia's social media–based activity appears inexpensive, which means that even modest investments can have an outsize effect.

## People

### *State Actors*

Public sources containing information on the strength of Russian organizations responsible for waging information confrontation are limited, and they provide only snapshots of possible staffing levels. Unit 26165 (or the 85th Main Special Service Center), a key part of Moscow's information confrontation organization as evidenced by the U.S. Department of Justice indictments after 2016, fell during the Cold War under the GRU's Sixth Directorate, which was responsible for cryptography and signals intelligence.[91] At that time, the directorate consisted of four departments; the first one, which focused on intercepting and decrypting foreign communications, numbered 300 service members and up to 1,500 civilians.[92] More recently, two investigative outfits (Bellingcat and *The Insider*) found that as many as 305 personnel work at Unit

[91] "In the Footsteps of the GRU Officers. New Details in the 'Case of Russian Hackers' [По следам офицеров ГРУ. Ровые детали в «деле русских хакеров»]," Radio Svoboda [Радио Свобода], July 17, 2018.

[92] Alexander I. Kolpakidi and Dmitry P. Prokhorov, "Military Intelligence and the Epoch of Détente [Военная разведка и эпоха разрядки]," Militera.lib.ru, undated.

26165's headquarters. (The investigators reached this number by assessing ownership of vehicles registered to the unit's address.)[93] Even less information is available about the FSB and SVR. According to an associate of the FSB's Center for Information Security, that unit has only a small collection of technical experts, which leads to frequent recruitment of independent hackers.[94] Nevertheless, German intelligence in 2016 claimed that Russia employed as many as 4,000 hackers (this estimate includes not only state actors [the military, FSB, SVR], but also independent activists and cut-outs) in its "offensive cyber force," though the data feeding this assessment remain undisclosed.[95]

Although few open sources detail the strength of Russia's military psychological operations forces, the military appears to have had troubles developing and employing such a force after the collapse of the Soviet Union through the Georgian War in 2008. Drawing lessons from the First Chechen War, a former senior staff officer concluded that the GRU should develop a training center for junior technical specialists and that psychological operations needed modern equipment to raise effectiveness.[96] Little improvement seems to have been made between then and the Georgian War, when the military had only 50 psychological operations specialists on hand—and few of those had technical expertise, such as conducting television broadcasts.[97]

Following the Georgian War, Russian psychological operations planners appear to have taken steps to improve technical training for spe-

---

[93] "305 Car Registrations May Point to Massive GRU Security Breach," Bellingcat, October 4, 2018.

[94] Turovsky, 2019, p. 149.

[95] John R. Schindler, "False Flags: The Kremlin's Hidden Cyber Hand," *Observer*, June 18, 2016.

[96] V. Potapov, *The Activity of Joint Formations and Units of Ground Forces in Conducting Special Operations to Disarm Illegal Groups in 1994–96 in the Chechen Republic [Действия соединений, частей и подразделений СВ при проведении специальной операции по разоружению НВФ в 1994-96 гг. на территории Чеченской республики]*, report to the South-Caucasus Military District, undated.

[97] Anatoliy Tsyganok, "The First Casualties of New-Generation Weapons [Первые Жертвы Оружия Нового Поколения]," *Independent Military Review [Независимое военное обозрение]*, No. 44, 2018.

cialists, according to insider accounts.[98] Unverified sources point to some 40–60 Russian psychological operations specialists operating in Ukraine during the earlier stages of the conflict, supported through digital operations by an undetermined number of specialists far from Ukraine's borders, which some Ukrainian sources estimate at approximately 1,000 service members.[99] The GRU's social media–based influence campaigns in early 2014 during the crisis likely reflect changes to technical training and staffing enacted after the Georgian War.[100] The GRU's main center for psychological operations (Unit 54777), which conducts much of its operations online through social media, began its social media influence operations in the run-up to the Maidan revolution.[101]

### *State-Affiliated Actors*

Importantly, Russia's shortfalls in personnel are likely mitigated by the ability of the Russian state to tap into a vast network of nonstate institutions to supplement its operations.[102] The IRA (and other similar but less well-known entities) undoubtedly adds muscle to the Russian military's ability to conduct influence campaigns via social media. The *New York Times* reported that the IRA's English-capable outfit numbered around 80,[103] but most insider accounts relate that, overall, per-

---

[98] S. A. Cheshuin, "Features of Modern Information Confrontation and Taking Them into Account in Preparation of Specialists of Foreign Military Information in the Military University [Особенности современного информационного противоборства и их учёт при подготовке специалистов зарубежной военной информации в Военном университете]," Pandia.ru, undated (anonymous copy).

[99] "Details on the 'Psychos' of Russia's Armed Forces Have Become Known [Стали известны данные о войсках «психов» России]," Tribune [Трибун], February 6, 2018; "The Forces of Russia's Information Operations: What Should Ukraine's Response Be? [Силы информационных операций России каким должен быть ответ Украины?]," Sprotyv.info, April 10, 2014; Ari Pesonen, "Russian Psychological Warfare Units Were Created in the Reform of the Armed Forces [Venäjän psykologisen sodankäynnin yksiköt luotiin puolustusvoimauudistuksessa]," New Finland [Uusi Suomi], March 1, 2018.

[100] Nakashima, 2017b.

[101] Troianovski and Nakashima, 2018.

[102] See Soldatov and Borogan, 2015; Turovsky 2019; "In the Footsteps . . . ," 2018.

[103] Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election," *New York Times*, September 20, 2018.

sonnel (i.e., including non-English speakers) has numbered more than 1,000.[104] Two leading Russian cybersecurity researchers, Andrey Soldatov and Irina Borogan, concluded in 2015 that the IRA in its earlier stages consisted of some 250 personnel.[105] The discrepancies among various personnel estimates could be explained by the IRA's quick growth after its creation.[106] Importantly, the IRA is likely not the only entity that might staff Russia's ranks of trolls.

## Money

### *State Actors*

As with personnel counts, details are scare regarding Russia's expenditures on information confrontation broadly or on social media–based disinformation specifically. A 2017 survey by a defense ministry–linked Russian cybersecurity firm claimed that Russia's overall budget for cyberoperations—which appear to include "information wars" and cyberattacks designed to affect the "mood and behavior" of civilian populations (along with espionage and other cyberattacks)—amounted to around $300 million annually.[107] In 2016, Russian experts asserted that Moscow would expend as much as $250 million to bolster its offensive cybercapacity in response to plans announced by U.S. Cyber Command (CYBERCOM) in 2015.[108] How much Russia dedicates to social media–based disinformation specifically is difficult to say, but the figures are likely modest.[109]

---

[104] Adrian Chen, "The Agency," *New York Times*, June 2, 2015.

[105] Soldatov and Borogan, 2015.

[106] Mueller, 2019, pp. 73–80.

[107] "Cybertroops Are Deployed on the Internet [В интернет ввели кибервойска]," *Kommersant [Коммерсантъ]*, No. 2, January 10, 2017.

[108] Eugene Gerden, "Russia to Spend $250m Strengthening Cyber-Offensive Capabilities," *SC Media*, February 4, 2016. Whether this sum was included in the previously cited $300 million is unclear.

[109] In the early days of internet activity, the SVR allocated about $460,000 to social media capabilities, such as monitoring networks and placing "special information" on targeted sites—although it is unclear how much of this was intended for offensive operations. Yuriy Vasilev and Dinara Setdikova, "The SVR: A Million Dollars—On Blogs [СВР: миллион долларов - на блоги]," Radio Svoboda [Радио Свобода], August 27, 2012.

### *State-Affiliated Actors*

Since 2016, more public information has been made available regarding the Kremlin's budget for overt propaganda outlets and the IRA. Although these figures also include funding for traditional media, social media is an increasingly integral part of what state-affiliated media organizations do. The U.S. intelligence community in 2017 stated that the Kremlin spent $190 million annually on RT's programming and broadcasting, although other estimates are somewhat higher and the draft budget for 2020 asked for $370 million.[110] Rossiya Segodnya, the company that operates Sputnik and several other news outlets, had a budget of about $110 million (6.7 billion rubles) in the 20202 budget.[111] Zvezda, the Ministry of Defense television, radio, and online broadcaster, is budgeted to receive $32.3 million.[112] In total, Russia's budget for 2020–2021 showed all state-owned (both foreign and domestic-facing) media receiving 69.5 billion rubles ($1.1 billion) a year, and that number was set to increase considerably (as of late 2020).[113]

As for the IRA, the U.S. Department of Justice indictment against an IRA employee in late 2018, for example, revealed that the IRA's Project Lakhta—its campaign targeting the 2016 U.S. presidential election—maintained a budget of roughly $12 million per year in both 2016 and 2017, respectively.[114] Between January and June 2018, the project's budget reportedly exceeded $10 million.[115]

### Social Media Accounts

As of October 2018, the IRA appears to have used at least 3,613 accounts to disseminate English-language and Russian-language messaging—

---

[110] ODNI, 2017; "Figure of the Week: 1.3 Billion," *EUvDisinfo*, October 1, 2019.

[111] "Proposal to Triple Financing of Mass Media [Финансирование СМИ из бюджета предложено увеличить на треть]," Interfax, September 26, 2019.

[112] "Figure of the Week . . . ," 2019.

[113] Proposal to Triple Financing . . . ," 2019.

[114] *United States v. Khusyaynova*, criminal complaint, case 1:18-MJ-464, E.D. Va., September 28, 2018.

[115] U.S. Attorney's Office, Eastern District of Virginia, "Russian National Charged with Interfering in U.S. Political System," news release, October 19, 2018.

and that is likely an underestimate because it excludes accounts that were suspected but deleted prior to Twitter's count.[116] This number also excludes fake accounts that the IRA operated on other platforms, such as Instagram and Facebook. To be sure, determining the number of accounts cannot provide an estimate of resonance with a particular target audience: One account ("PoliteMelanie") associated with the IRA attracted 25,000 Twitter followers in six months and was retweeted more than 125,000 times.[117] Other accounts might not gain nearly as many followers.

The numbers of social media accounts operated by the GRU (or the other intelligence agencies) are unknown but are in all likelihood quite a bit smaller than those affiliated with the IRA and other trolls. Both the U.S. Department of Justice indictments against GRU officers and the previously referenced report published by the DFRLab point to only a handful of fake accounts generated by GRU specialists, and most of their social media accounts only posted once before deletion.[118] Some GRU accounts (such as the fictitious Alice Donovan) attempted to direct attention via social media to articles that were very likely at least partially written by GRU officers. A DFRLab report attributes to Russian intelligence a digital influence operation (dubbed "Second Infektion"—so named because of its resemblance to a Soviet-era "Operation Infektion" that claimed the United States created the AIDS virus) that consisted of "dozens" of fake accounts on 30 different platforms and disseminated content in nine languages.[119]

---

[116] Twitter, "Data Archive," webpage, undated.

[117] Much of the content was apolitical in a likely attempt to gain credibility with followers. Darren L. Linvill and Patrick Warren, "Russian Trolls Can Be Surprisingly Subtle, and Often Fun to Read," *Washington Post*, September 10, 2018.

[118] *United States of America v. Viktor Boris Netyksho, Boris Alekseyevich Antonov et al.*, Criminal No. 18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq., United States District Court for the District of Columbia, July 13, 2018; U.S. Department of Justice, Office of Public Affairs, 2018; DFRLab, 2018e.

[119] DFRLab, "Top Takes: Suspected Russian Intelligence Operation," *Medium*, June 22, 2019.

### Assessment of Scale

Although nearly all of the figures cited should be presumed to be imprecise and uncertain, they might be useful in conveying an order of magnitude. As emphasized, an apples-to-apples comparison of Russia's resources devoted to disinformation on social media with those of its rivals is not feasible. But some sense of U.S. resources might be useful to simply provide perspective—and to offer insight into Russia's perceptions of its own capabilities. The estimates of Russia's cyber and psychological warfare personnel (i.e., state actors) that we have provided are almost certainly smaller than the size of U.S. Cyber and PSYOPS forces.[120] The same is true about U.S. spending on such capabilities: Comparing the budget for the U.S. military's offensive cyber arm—CYBERCOM—with the (admittedly very rough) partial expenditure estimates for cyber resources on the Russian side suggests that the latter amounts are likely more modest.[121]

To put Russia's spending on known state-affiliated actors in perspective, Russia likely has been spending less than $500 million annually on RT, Sputnik, and the IRA whereas the U.S. Agency for Global Media (USAGM, formerly the Broadcasting Board of Governors, or BBG)—the U.S. information agency that supervises Voice of America and Radio Free Europe/Radio Liberty along with other foreign-facing

---

[120] For instance, CYBERCOM alone consists of 133 teams and 6,200 personnel, which overshadows even the high-end German estimate of Russia's offensive cyber warrior ranks at 4000 (see the "State Actors" portion of the section titled "People" earlier in this chapter). DoD, "Cyber Mission Force Achieves Full Operational Capability," May 17, 2018. For a sense of perspective regarding the numbers of PSYOPS officers, see Jeff Gerth, "Military's Information War Is Vast and Often Secretive," *New York Times*, December 11, 2005.

[121] In 2015, CYBERCOM's budget was $509 million. Michael S. Rogers, testimony presented before the Senate Committee on Armed Services, Washington, D.C., March 19, 2015; Sean D. Carberry, "CyberCom Seeks 16 Percent Budget Surge for 2018," *FCW*, May 23, 2017. For fiscal year 2020, $532 million was reportedly to go to support cyberoperations, with another $1.9 billion earmarked for new buildings and infrastructure. Aaron Boyd, "What DOD Plans To Do With $9.6 Billion in Cyber Funding," *Nextgov*, March 14, 2019. The estimates for Russia's expenditures on some indeterminate subset of activities likely by state actors are in the $300 million range (see the "State Actors" portion of the section titled "Money" earlier in this chapter).

media—spent approximately $794 million in 2017.[122] The two sets of activities are not directly comparable, and neither is limited to social media specifically—but the numbers suggest that Russia spends somewhat less on foreign-bound propaganda than the United States spends on fostering transparent global media.

Such comparisons are not wholly informative about investments into social media–based information warfare in large part because, in contrast to Russia, the United States does not involve any such resources in offensive social media efforts. Nonetheless, the disparities in cyber and psychological resources likely do affect Russian perceptions of those capabilities. There is evidence that, whatever the facts of the matter, Russia perceives its information-warfare arsenal generally to be smaller than those of other states and those of the United States in particular. For example, a Russian information security company, which lists the defense ministry as a client, published a report that said that the U.S. cyberoperators who are engaged in information warfare, cyberattacks, and espionage outnumbered Russia's by nine to one.[123] The methods and sources used to produce this report are not clear, but it ranks Russia as fifth in the world, with 1,000 "cybertroops" and annual financing amounting to $300 million. The United States ranked first, with 9,000 cybertroops and $7 billion in financing.[124] The evidence backing these assessments are questionable, but these are the kinds of comparisons that appear to inform Russia's assessment of the balance of power in the information domain.[125] Similarly, although

---

[122] See the "State-Affiliated Actors" portion of the section titled "Money" earlier in this chapter for a breakdown of Russia's budget. For USAGM budgets, see U.S. Advisory Commission on Public Diplomacy, *2018 Comprehensive Annual Report on Public Diplomacy and International Broadcasting*, Washington, D.C.: U.S. Department of State, November 20, 2018, p. 32.

[123] See Nikolai Litovkin, "Russia's Cyber Army Hacks a Spot in the Top 5," *Russia Beyond the Headlines*, January 12, 2017.

[124] China's cybertroops numbered 20,000, with an annual budget of $1.5 billion, and the United Kingdom was assessed to have 2,000 cybertroops and annual financing of $450 million. Litovkin, 2017.

[125] The survey attracted significant attention in the Russian press and stirred debate regarding both methodology and how data were acquired, but most of the doubt seemed to sur-

UAGM programming is not analogous to RT or Sputnik activity, Russians often cite it by way of comparison.[126]

Although the figures available for various aspects of Russia's operations are not large in an absolute sense, even modest expenditures can buy a fair amount of activity. The Oxford University's Computational Propaganda Project's analysis offers a glimpse of the cost of specific social media campaigns: For example, the IRA spent around $74,000 to influence target audiences on Facebook in its effort to affect the U.S. presidential elections—spending more than $15,000 on ads aimed at "Conservative Politics and Culture" and more than $11,000 on "African American Politics and Culture," which were the two highest-funded Facebook campaigns.[127] The IRA spent about $1,650 on its top ten most-expensive ads on Facebook.[128] Activities by state actors might not be any more costly: The GRU's "Victor for Peace" campaign, which attempted to propagate official Russian narratives surrounding World War II through social media, used digital advertisements that attracted some 213,000 viewers—and cost only $280.[129]

Also important is the fact that the Russian state has cheap resources outside the state that it can leverage on an ad hoc basis. To demonstrate how inexpensive third-party social media influence services are in Russia, a group of cybersecurity researchers in 2018 hired Russian operators for $250 to go after a fake website that attacked Stalin; within two weeks, the operators posted 730 Russian-language

---

round the other Western countries mentioned in the survey. See, for example, ""Cybertroops Are Deployed . . . ," 2017.

[126] "Editor-in-Chief of RT Commented on Power's Statement on the Budget of the Channel [Главный редактор RT прокомментировала слова Пауэр о бюджете телеканала]," RIANovosti, January 18, 2017.

[127] Howard et al., 2018, Table 4.

[128] It is possible that the organization was able to generate revenue through its own merchandise promotion through Instagram, though no sales data are available and merchandising might have simply provided a means to gather consumer information. DiResta et al., 2018, pp. 29–31.

[129] Renee Diresta and Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, Stanford, Calif.: Internet Observatory, Cyber Policy Center, Stanford University, white paper, 2019, p. 47.

tweets from 25 different Twitter accounts attacking the website while generating 100 posts to different forums and blogs.[130]

Moscow similarly provides state-affiliated actors with funding to perform technical operations that increasingly support digital influence efforts, such as staging DDoS attacks to block rival information outlets or hacking that provides sensitive documents to exploit. In 2017, Kaspersky Labs found that the average cost of a DDoS attack using a botnet of a thousand desktop computers cost as little as $25 an hour, though such attacks against government or other well-defended websites could be significantly more expensive.[131] Attacks on English-speaking websites were cheaper than attacks on Russian-language sites.[132] More-sophisticated efforts can, of course, be much more costly: One DDoS system used to attack Ukraine's Defense Ministry as of 2015, for example, allegedly $1 million.[133] Importantly, as described earlier, many Russian military experts view social media influence and computer-network operations as a cost-effective means of engaging a conventionally superior adversary with a much larger pocketbook.

## Social Media Actors' Headquarters

Russian military units and other organizations responsible for recent digital information confrontation campaigns targeting the West are mostly headquartered in Russia's two most populous cities, St. Petersburg and Moscow. Two Russian military units responsible for offensive computer-network operations are the GRU's Unit 26165 (the 85th Main Special Service Center) and Unit 74455, both of which

---

[130] Andy Greenberg, "Alphabet-Owned Jigsaw Bought a Russian Troll Campaign as an Experiment," *Wired*, June 12, 2019b.

[131] "KL Calculated the Average Cost of Custom DDoS-Attacks [ЛК подсчитала среднюю стоимость заказной DDoS-атаки]," SecurityLab, March 24, 2017.

[132] "KL Calculated . . . ," 2017.

[133] In 2015, two Russian businessmen probably connected to the Kremlin revealed the cost of the DDoS attacks that were allegedly leveled by an independent programmer against the Ukrainian defense ministry's website. Kramer, 2016. For more information on this case, see Turovsky, 2019.

are based in Moscow.[134] The same is true about the foreign military information department at the defense ministry's academy, a known pipeline to the GRU.[135] Rooting these units in Moscow likely enables leaders to communicate more directly with senior government figures and maintain firm relationships for recruiting purposes with many of Russia's leading academic institutions.[136] The IRA is located in Russia's second major city of St. Petersburg, alongside Russia's Federal News Agency, which also supported the multimillion-dollar social media campaign to target U.S. audiences. The majority of the organizations indicted by the United States that are known components of Yevgeniy Prigozhin's social media manipulation machine are likewise based in St. Petersburg.[137]

## Aims Pursued Through Social Media in Information Warfare

Russia employs social media primarily for four general, non–mutually-exclusive aims (Table 3.2): to facilitate kinetic action, to support Russian foreign policy narratives, to achieve specific outcomes in other countries, and to exacerbate internal divisions within and between Western states. Arguably, the latter two categories represent the more-aggressive

[134] "In the Footsteps . . . ," 2018.

[135] Moscow-Russia.ru, "Military University of the Ministry of Defense of the Russian Federation [Войнный университет министерсвта обороны Российской Федерации]," webpage, 2019.

[136] For examples of the relationship between cyber units and Russian academia, see Peter Mironenko and Anastasia Yakoreva, "Cryptographers from Military Units: What We Know About the Accused Russian Hackers," *The Bell*, July 14, 2018; Kovalev and Bodner, 2017; Kevin Poulsen, "This Hacker Party Is Ground Zero for Russia's Cyberspies," Daily Beast, August 4, 2018. Daniil Turovsky, a leading journalist on Russian cyberwarfare, points out that the likely bedrock for Russia's contemporary cyberprogram is Soviet-era research institutions—such as the Moscow-based 27th Central Scientific Research Institute, which is close to GRU headquarters and was founded in the late 1950s to conduct computer science research. Turovsky, 2019, p. 163.

[137] Chen, 2015; Virtual Globetrotting, "MediaSintez LLC—Division of Internet Research Agency—Russian 'Troll Farm,'" webpage, undated.

**Table 3.2**
**Main Aims, Examples, and Targets of Social Media–Based Information Warfare**

| Aim | Examples | Primary Targets |
|---|---|---|
| Facilitate kinetic action | • Annexation of Crimea<br>• Conflict in East Ukraine<br>• Syrian conflict | • Adversary governments<br>• Adversary military units |
| Support Russian foreign policy narratives | • Poisoning of former KGB agent Sergei Skripal<br>• Downing of MH-17<br>• Anti-NATO narratives | • U.S. and allied governments, officials, and prominent figures<br>• NATO<br>• EU |
| Achieve specific outcomes in other countries | • 2016 U.S. election<br>• France's 2017 election<br>• Referendum on UK withdrawal from EU (Brexit)<br>• Netherlands EU-Ukraine Association referendum<br>• Candidates and political forces unfriendly to Russia<br>• Political forces favoring national or Western unity or Western international institutions | |
| Exacerbate internal divisions within and between Western states | • Race relations in United States<br>• Separatist sentiments<br>• Anti-immigrant, anti-Muslim sentiments<br>• Religious divisions in Europe | • Groups on both sides of significant social, political, cultural, or ethnonational divides<br>• Political forces favoring national or Western unity or Western international institutions |

and more-expansive manifestations of information confrontation while the first two categories resemble more-ordinary information operations or military deception and public diplomacy, respectively.

### Facilitating Kinetic Action

Russia uses social media both to shape the narratives surrounding conflicts and to facilitate operational and tactical activities of Rus-

sian forces.[138] In general, Russia has employed social media to create a "smokescreen" intended to "deceive, delay, and disrupt."[139] For example, as will be discussed later, during the height of the fighting in Ukraine, Russian actors vilified the Ukrainian government; fomented antigovernment actions through fake groups set up to look Ukrainian; and used social media to undermine morale and intimidate or turn Ukrainian soldiers fighting Russia-backed separatists in the Donbass,[140] going so far as to target individual soldiers and their families.[141] Similarly, GRU PSYOPS units were involved in the Kerch Strait incident, sending text messages to Ukrainian service members as Russia's border forces seized three Ukrainian ships.[142]

Similarly, Russia emphasized information efforts on both traditional and social media during the Syrian conflict. Overtly, the Russian defense ministry frequently promulgates information in Arabic, mostly through Twitter and—since at least 2016—supporting the Russian Centre for Reconciliation of Opposing Sides and Refugee Migration Monitoring in Syria.[143] RT's Arabic-language outlet issued steady Assad-friendly coverage, which ensured widespread support from pro-Assad forces, allowing RT swift access to frontline locations.[144] Since 2016, Sputnik has produced a daily hour-long news segment for one

---

[138] For further discussion of Russia's use of information efforts in the prelude to its annexation of Crimea, see Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Santa Monica, Calif.: RAND Corporation, RR-1498-A, 2017, pp. 12–16, 28–29, and 50–54.

[139] Mark Laity, "Chief Strategic Communications at SHAPE: 'Perception Becomes Reality,'" presentation, October 2014 (quoted in Giles, 2016, p. 46).

[140] See, for example, Nataliia Popovych and Oleksiy Makhuhin, "Countering Disinformation: Some Lessons Learnt by Ukraine Crisis Media Center," Ukraine Crisis Media Center, April 20, 2018.

[141] Aaron Brantly and Liam Collins, "A Bear of a Problem: Russian Special Forces Perfecting Their Cyber Capabilities," Association of the United States Army, November 28, 2018.

[142] Trioianovski and Nakashima, 2018.

[143] Russian Defense Ministry [Минобороны России], @mod_russia, Twitter account, undated.

[144] "The Russian Offensive in Syria You Haven't Heard About," .coda, November 28, 2017.

of Syria's most-popular news stations (Sham FM), which supports Assad.[145] Both media outlets have reportedly gained traction with Syrian audiences, supplanting such once-dominant regional media outlets as Al Jazeera and Al Arabiya as Syrians' main source of information in government-controlled areas.[146] These traditional media outlets also team up with social media efforts to disseminate disinformation, such as delivering narratives that seek to discredit investigations tying Assad's regime to chemical-weapon use and repeating allegations that the White Helmets (also known as the Syrian Civil Defence, a search-and-rescue organization based in opposition-held areas) are involved in chemical attacks in Syria.[147]

### Supporting Russian Foreign Policy Narrative

Russia's social media efforts often are designed to advance Russian foreign-policy narratives in parallel with official statements and traditional media. Much social media–based information activity is intended to deflect criticism; muddy the waters; or defend Russia when the Russian state is accused of wrongdoing, such as accusations by the United Kingdom and the West regarding the Kremlin directing the 2018 poisoning of Skripal, Russian responsibility for the downing of flight MH-17,[148] the multiple doping violations by Russian athletes and

[145] "The Russian Offensive . . . ," 2017.

[146] "The Russian Offensive . . . ," 2017.

[147] Donald N. Jensen, "Russia in the Middle East: A New Front in the Information War?" Jamestown Foundation, December 20, 2017; Louisa Loveluck, "Russian Disinformation Campaign Targets Syria's Beleaguered Rescue Workers," *Washington Post*, December 18, 2018. The accusations against the White Helmets have been debunked by Bellingcat, among others ("Chemical Weapons and Absurdity: The Disinformation Campaign Against the White Helmets," Bellingcat, December 18, 2018).

[148] For example, see "British Officials Probe 2,800 Russian Bots That 'Spread Confusion' After Salisbury Nerve Agent Attack on Former Spy," *Daily Mail*, March 23, 2018; Ben Nimmo, "How MH17 Gave Birth to the Modern Russian Spin Machine," *Foreign Policy*, September 29, 2018.

Russia's exclusion from the Olympics,[149] Russian meddling in other countries' political processes, and so on.

Russia's social media efforts often aim to drown out the evidence-based accounts with multiple—and often highly implausible and contradictory—stories. For instance, the EU's East StratCom Task Force counted more than 40 different accounts of the Skripal poisoning as of early 2019.[150] The operations likely aimed to create an impression that truth is unascertainable and that only various versions of events exist.[151] NATO StratCom CoE Director Janis Sarts described this tactic as creating an "'information fog' that undermines the ability of societies to establish a factual reality."[152] As Russia expert Mark Galeotti puts it, "[t]he next best thing to being able to convince people of your argument, after all, is to make them disbelieve all arguments."[153] Accordingly, Russian actors opt for quantity over quality, apparently aiming to dominate the social media conversations pertaining to these actions. As an analysis by the Atlantic Council's DFRLab showed, two out of three articles pertaining to the Skripal poisoning shared over the course of a week in 2018 via four key social media platforms—Facebook, Twitter, LinkedIn, and Pinterest—"came from Kremlin-funded media outlets."[154]

Russian disinformation often targets NATO. Pro-Russian media produce a steady stream of disinformation and propaganda about every

---

[149] Jack Stubbs, "#NoRussiaNoGames: Twitter 'Bots' Boost Russian Backlash Against Olympic Ban," Reuters, December 8, 2017.

[150] "Year in Review: 1001 Messages of Pro-Kremlin Disinformation," *EU vs. Disinfo*, January 3, 2019.

[151] Jenny Yang, "Information: The Perfect Weapon in Today's Wired World, A Three-Part Series," NATO Association of Canada, August 8, 2015. Also see Robinson et al., 2018, p. 65; Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera, *Information Manipulation: A Challenge for Our Democracies*, Paris: Policy Planning Staff of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research of the Ministry for the Armed Forces, August 2018, p. 75.

[152] Janis Sarts, "Russian Interference in European Elections," testimony presented before the U.S. Senate Select Committee on Intelligence, June 28, 2017, p. 31.

[153] Galeotti, 2017c, p. 6.

[154] DFRLab, "#PutinAtWar: Social Media Surge on Skripal," *Medium*, April 5, 2018c.

instance of potential NATO expansion (e.g., Montenegro's accession, Macedonia's name change that would make accession possible), deployments (e.g., Enhanced Forward Presence in Eastern Europe), and exercises. The NATO Strategic Communications Centre of Excellence in Latvia and the Atlantic Council's DFRLab note several attacks that target NATO's enhanced forward presence in the Baltics.[155] The messaging painted NATO in a sinister light and was disseminated through multiple social media platforms in multiple languages.[156] Often, stories accusing NATO and its forces of various horrors appear in Russian or in the local language of the community affected by the NATO action at hand.[157]

Social media campaigns are also aimed at Western audiences. Apart from social media activity tied to kinetic action in Syria, much of Russia's Syria-related efforts have tried to shape international public opinion along the line of Russian foreign policy. Between February 2015 and at least December 2018, the IRA created more than 3,000 posts about Syria on Facebook and Instagram that framed Russian military operations supporting Syrian President Assad as necessary to defeat the Islamic State of Iraq and the Levant (ISIL).[158] The Syria Justice and Accountability Center in late 2018 linked roughly 1,500 Twitter accounts (created mostly between late 2013 and early 2014) attributed to the IRA to about 33,000 tweets (mostly in English and Arabic) rel-

---

[155] Jeff Seldin, "Russia Influence Operations Taking Aim at US Military," *Voice of America*, November 2, 2018.

[156] Ben Nimmo, "Russian Narratives on NATO's Deployment," StopFake, April 2, 2017.

[157] Nimmo, 2017; Karl-Heinz Kamp, *Russia's Myths About NATO: Moscow's Propaganda Ahead of the NATO Summit*, Berlin, Germany: Federal Academy for Security Policy, Working Paper No. 15/2016, 2016. Also see DFRLab, "#BalticBrief: The Kremlin's Loudspeaker in Latvia," *Medium*, November 19, 2018d.

[158] DiResta et al., 2018, p. 58. It is worth noting that there is a nexus between information operations and kinetic operations in Syria: Evgeniy Prigozhin's IRA frequently used the Syrian conflict in its influence operations through social media, and he is reportedly behind the private security company Wagner, which has been operating extensively in Syria. See Andrew E. Kramer, "Russia Deploys a Potent Weapon in Syria: The Profit Motive," *New York Times*, July 5, 2017.

evant to the Syria crisis aimed at Western audiences.[159] Russia also tried to erode support of U.S. and allied efforts in Syria. For example, the IRA disseminated an Instagram message aimed at African Americans claiming that the U.S. intervention in Syria was futile and the country should instead focus on domestic problems.[160]

The German Marshall Fund's Alliance for Securing Democracy's Hamilton 68 team reports that although these accounts focused on timely political or social controversies,

> over time, the geopolitical interests of the Kremlin— specifically, the wars in Syria and Ukraine, but also Russian reputational issues (e.g., Olympic doping and the poisoning of the Sergei and Yulia Skripal) and efforts to divide transatlantic allies (e.g., the promotion of anti-NATO narratives and the amplification of Islamic terrorism threats in Europe)— emerge as clear messaging priorities.[161]

Moreover, as Hamilton 68 finds, IRA-affiliated accounts "[f]old[ed] pro-Kremlin messages into daily chatter about American issues"—for example, spreading Russia's narratives on Syria by an account impersonating a politically left-leaning social justice persona.[162]

### Accomplishing Specific Outcomes in Other Countries

Apart from shaping foreign policy narratives, Russian social media operations sometimes seek to affect the outcomes of elections, refer-

---

[159] Syria Justice and Accountability Centre, "Russia's Twitter Campaign: Influencing Perceptions of the Syrian Conflict," December 12, 2018.

[160] DiResta et al., 2018, p. 58.

[161] Schafer, 2018, p. 6; DiResta et al., 2018, p. 12.

[162] Schafer, 2018, p. 9; see also Laura Rosenberger, "Foreign Influence Operations and Their Use of Social Media Platforms," Alliance for Securing Democracy, July 31, 2018; U.S. House of Representatives Permanent Select Committee on Intelligence, "Social Media Advertisements: 2017: Quarter 2, May: Ad ID 981," webpage, undated-a; U.S. House of Representatives Permanent Select Committee on Intelligence, "Social Media Advertisements: 2017: Quarter 2, May: Ad ID 1262," webpage, undated-b; U.S. House of Representatives Permanent Select Committee on Intelligence, "Social Media Advertisements: 2017: Quarter 2, May: Ad ID 3023," webpage, undated-c.

enda, and other specific events. As Sarts sums up, Russian election-focused influence efforts aim "to either promote candidates friendly to the Kremlin or those trying to undermine the EU and NATO and hurt the candidates the Kremlin perceives as undesirable."[163] Information campaigns surrounding elections are also likely motived by the desire to simply "delegitimize the democratic process."[164] As is now amply documented, Russia used social media extensively to interfere in the 2016 U.S. election.[165]

Social media also played a role in Russian efforts to influence other elections and referenda. In France, for instance, Russian actors likely hacked Emmanuel Macron's campaign, which was leaked on Archive.org, PasteBin, and 4Chan, and then picked up and spread by Twitter.[166] The same actors appear to be behind the #MacronGate and #MacronCacheCash allegations that Macron has a secret offshore account, which first surfaced on 4chan and spread via Twitter.[167] Disinformation spread about Macron through social media mirrored content aired by Russian state-controlled traditional media.[168] Additionally, Facebook confirmed that it deactivated fake accounts posing as acquaintances of people close to Macron that were set up in efforts to obtain intelligence but were identified by anonymous Facebook employees and

---

[163] Sarts, 2017, p. 31. Also see European Commission, "A Europe That Protects: The EU Steps Up Action Against Disinformation," press release, December 5, 2018.

[164] Esther King, "Russian Hackers Targeting Germany: Intelligence Chief," Politico, November 29, 2016; also see Stelzenmüller, 2017.

[165] The operation to influence the 2016 U.S. presidential election entailed extensive social media activity. See DiResta et al., 2018; Howard et al., December 2018; ODNI, 2017; and Andrew Weisburd, Clint Watts, and J. M. Berger, "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy," *War on the Rocks*, November 6, 2016.

[166] Vilmer et al., 2018, pp. 106–116.

[167] Vilmer and colleagues conclude that the social media dissemination was highly likely to have involved Russian participation. They also concludes that the same actors were behind MacronLeaks and MacronGate (Vilmer et al., 2018, pp. 106–116).

[168] For example, Russian media alleged that Macron was secretly gay, controlled by the U.S. banking system, and supported by Saudi Arabia ("Ex-French Economy Minister Macron Could be 'US Agent' Lobbying Banks' Interests," Sputnik, February 4, 2017).

U.S. government sources as being linked to the GRU.[169] A year prior and across the English Channel in the United Kingdom, Russian actors—notably the IRA—are believed to have conducted a coordinated trolling campaign on Twitter using the hashtag #ReasonsToLeaveEU and #Brexit, with "some of the posts [coming] from accounts masquerading as news organizations or journalists," and others from "internet personalities crafted over years by Russian hackers."[170] The parliamentary committee investigating these efforts also claims that IRA's activity included purchasing political ads aimed at the United Kingdom on social media.[171] In Catalonia, it is highly likely that Russian-connected actors swarmed the social media conversation about Catalan independence on Twitter.[172] According to analysis by scholar Javier Lesaca, RT and Sputnik were in the top five most-used sources retweeted in relation to the referendum; the campaign heavily relied on *bots* (automated accounts); and content tended to favor independence but also sought to inflame both sides to the question.[173]

### Increasing Divisions Within and Between Western States

Russians employed social media to exacerbate social, political, economic, and cultural divisions and sources of internal instability within Western societies and institutions—goals that numerous experts ascribe to Russian influence efforts.[174] These efforts might, of course, occur in

---

[169] Joseph Menn, "Exclusive: Russia Used Facebook to Try to Spy on Macron Campaign—Sources," Reuters, July 27, 2017.

[170] Matthew Field and Mike Wright, "Russian Trolls Sent Thousands of Pro-Leave Messages on the Day of Brexit Referendum, Twitter Data Reveals," *The Telegraph*, October 17, 2018.

[171] Digital, Culture, Media and Sport Committee, Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Interim Report*, London, United Kingdom: United Kingdom House of Commons, Fifth Report of Session 2017–19, July 29, 2018.

[172] Spanish intelligence confirmed that social media was used by Russian-based groups to spread misinformation, although the involvement of the government cannot be confirmed. See Vasco Cotovio and Emanuella Grinberg, "Spain: 'Misinformation' on Catalonia Referendum Came from Russia," CNN, November 14, 2017.

[173] Javier Lesaca, "Why Did Russian Social Media Swarm the Digital Conversation About Catalan Independence?" *Washington Post*, November 22, 2017.

[174] Vilmer et al., 2018, p. 53; Stelzenmüller, 2017, p. 3.

the context of influencing specific outcomes, but divisive activity is not always tied to specific political events. As one of the leading experts on Russian information warfare explains, Russia is pursuing a "broad-based, long-term weakening and undermining of adversary societies overall, without necessarily any specific short-term goal other than increasing Russia's relative strength in a classic zero-sum approach."[175]

The IRA's activity in the United States again furnishes one of the best-studied illustrations. IRA-linked accounts across major social media platforms—including Facebook, Instagram, and Twitter—sought to exacerbate divisions over such controversial issues as immigration, race relations, treatment of veterans, gun violence, and the Second Amendment.[176] For instance, the largest share of videos produced by the IRA on YouTube dealt with Black Lives Matter and U.S. police brutality.[177] From Texas secessionism to the Catalan cause to Bosnian Serb nationalism, Russia's agents appear to have sought to inflame separatist sentiments through social media–focused information efforts.[178] The IRA often exploited specific events to intensify the controversy, such as the Unite the Right rally in Charlottesville, Virginia, and the mass shooting in Las Vegas, Nevada, in 2018—in keeping with its directive to create "political intensity" by supporting radical groups and to "effectively aggravate the conflict between minorities and the rest of the population."[179]

Operations aimed at inflaming divisions are likewise common in Europe. For example, Russian actors in September 2018 spread fake information through social media about ethnic clashes between Ukrainians and Hungarians in Western and in central Ukraine, and

---

[175] Giles, 2016, p. 24.

[176] Howard et al., December 2018, p. 39.

[177] DiResta et al., 2018, p. 16.

[178] For example, see Tim Lister and Clare Sebastian, "Stoking Islamophobia and Secession in Texas— from an Office in Russia," CNN, October 6, 2017; Dijedon Imeri, "Recent Twitter Activity Indicates Russian Plan to Destabilise Bosnia Ahead of General Election in October," *Jane's*, January 24, 2018; and Vilmer et al., August 2018, p. 94.

[179] *United States v. Khusyaynova*, 2018, p. 13.

a fictitious murder of a Ukrainian boy by Hungarians.[180] Four years earlier, during the early stages of the Ukraine crisis, the GRU disseminated messages on social media claiming that "brigades" of "zapadentsy" (Westerners) were going to "rob and kill" other Ukrainians, and emphasizing divisions between "ordinary" Ukrainians and those protesting then-President Viktor Yanukovych.[181] IRA Twitter accounts also sought to fuel divisions, including religious tensions, in Western Europe in the aftermath of the Westminster, Manchester, London Bridge, and Finsbury Park terror attacks in the United Kingdom.[182] In the 2016 Lisa case, Russian actors on social media, media outlets, and even Foreign Minister Sergei Lavrov sought to inflame German anti-migrant and anti-Muslim sentiments by spreading a story (which turned out to be fabricated) that a Russian-German girl was raped by Arab or Muslim immigrants.[183]

In the words of Anders Fogh Rasmussen, former head of NATO and prime minister of Denmark, Russia's efforts to divide go as far as "undermin[ing] the political cohesion in Western institutions."[184] For example, to make the ill-fated EU-Ukraine Association Agreement unpalatable to the Dutch—who put it to a referendum—Russian actors created a fake video, impersonating members of the Ukrainian radical-right Azov battalion and threatening terrorist attacks in Holland if the Dutch voted against the Agreement. A Bellingcat investigation concluded that the video, placed on YouTube, is most likely a product of the IRA.[185]

---

[180] Interview with Ukrainian security experts, Kyiv, Ukraine, March 6, 2019.

[181] Nakashima, 2017a.

[182] Martin Innes, "Russian Influence and Interference Measures Following the 2017 UK Terrorist Attacks," Cardiff University Crime and Security Research Institute, December 18, 2017.

[183] Stefan Meister, "The 'Lisa Case:' Germany as a Target of Russian Disinformation," *NATO Review Magazine*, 2016.

[184] Joe Parkinson and Georgi Kantchev, "Document: Russia Uses Rigged Polls, Fake News to Sway Foreign Elections," *Wall Street Journal*, March 23, 2017.

[185] "Behind the Dutch Terror Threat Video: The St. Petersburg 'Troll Factory' Connection," Bellingcat, April 3, 2016.

## How the Russians Use Social Media in Information Warfare

To illustrate how Russian actors are using social media, we selectively highlight some of the tactics and techniques that Russian actors have used to date that might be applicable to multiple aims and encompass both overt and covert efforts.

### Multiplicity of Platforms

Although Facebook and Twitter have received the lion's share of attention from analysts and U.S. policymakers, Russian social media efforts appear across many different social media platforms. YouTube and Instagram have been particularly prominent.[186] The Alliance for Security Democracy finds that the "Russian government and its proxies have infiltrated and utilized nearly every social media and online information platform—including Instagram, Reddit, YouTube, Tumblr, 4chan, 9GAG, and Pinterest."[187] They note that some platforms "have been used to target specific communities: Tumblr, for instance, was used to target African Americans."[188] Importantly, local social media and Russian-language platforms, such as VKontakte (VK) and Odnoklassniki (OK), sometimes feature more centrally than bigger international platforms in Russia's social media activity. Russians have also employed—or sought to employ—encrypted messaging apps, such as Telegram and WhatsApp.[189] Blogging platforms, such as LiveJournal,

---

[186] Paresh Dave and Christopher Bing, "Russian Disinformation on YouTube Draws Ads, Lacks Warning Labels: Researchers," Reuters, June 7, 2019; DiResta et al., 2018, pp. 29–31; Paris Martineau, "How Instagram Became the Russian IRA's Go-To Social Network," *Wired*, December 17, 2018.

[187] Rosenberger, 2018. Regarding Reddit, see Benjamin Plackett, "Russian Spam Accounts Are Still a Big Problem for Reddit," Engadget, April 2, 2019.

[188] Rosenberger, 2018; interview with NGO expert, Washington, D.C., February 21, 2019. Regarding the particularly prominent role of Instagram in the United States, see Martineau, 2018.

[189] Interview with NGO expert, Washington, D.C., February 21, 2019; also see Nina Jankowicz, "How the U.S. Can Fight Russian Disinformation for Real," Atlantic Council blog post, July 11, 2019.

also play an important role: As one study finds, disinformation campaigns can be waged primarily through blogs and "strategically link to a variety of other social media platforms."[190] A recent investigation by DFRLab points to the significance of other online forums—such as *Medium*, homment.com (based in Berlin), and indybay.org (based in San Francisco).[191] Russia also operates in the comments sections of news websites with public comment capabilities—spreading disinformation or propaganda, inflaming divisions, or directing users to malware.[192] Russians have also used smaller or even custom-made filesharing websites rather than the well-known WikiLeaks and DCLeaks to leak material.[193] Importantly, Russian actors can plan a single social media operation to be carried out in a coordinated fashion across platforms.[194]

### Variety of Deceptive Identities

Russian actors sometimes build wholly fictitious individuals, often employing actual persons' photographs for the social media profile. For example, many IRA accounts made up names and identities supplemented with stock or random photos.[195] Other times, Russian actors create individual social media accounts that purport to belong to real, well-known persons—for instance, a senior Labour party figure, whose fake Facebook page features his genuine photo and bio.[196] Some

---

[190] Nitin Agarwal and Kiran Kumar Bandeli, Examining Strategic Integration of Social Media Platforms in Disinformation Campaign Coordination, *Defence Strategic Communications*, Vol. 4, Spring 2018e.

[191] DFRLab, 2019.

[192] See Helmus et al., 2018, p. 22.

[193] For example, PasteBin was used to leak MacronLeaks; custom sites—btleaks.info and btleaks.org—apparently were set up to leak material stolen in the Bundestag hack (which never occurred).

[194] For example, see DRFLab, 2019; and John D. Gallacher and Rolf E. Fredheim, *Division Abroad, Cohesion at Home: How the Russian Troll Factory Works to Divide Societies Overseas but Spread Pro-Regime Messages at Home*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2019, p. 61.

[195] For example, see Seldin, 2018.

[196] Luke Harding, "Russians 'Spread Fake Plot to Assassinate Boris Johnson' on Social Media," *The Guardian*, June 22, 2019.

fictitious accounts have extensive online backgrounds and histories; others are used once and then discarded. During the 2016 election-meddling campaign, for example, GRU officers used a variety of fake social media accounts—including the aforementioned Alice Donovan account—to promote the DCLeaks website.[197] Alice Donovan, a freelance writer, cultivated a varied online existence, posting dozens of articles on different outlets and tweeting. Similarly, some of the IRA's best-known accounts are prolific tweeters—such as @TEN_GOP, an account manned by a persona posing as a member of the Tennessee Republican Party.[198] By contrast, the aforementioned Second Infektion campaign overwhelmingly used social media cut-outs only once to publish an article or message.[199] Curiously, the GRU's primer on using Facebook for digital operations recommended using profile photos of users who were mostly inactive and had "very few friends."[200] Social media groups also can have deceptive identities, such as United Muslims of America and Secured Borders (two IRA-created groups in the United States).[201] An impersonated account, moreover, can be operated to appear genuine: For example, the fraudulent account for the Labour party leader noted earlier posted real articles from the Labour Party and Jeremy Corbyn.[202]

### High Volume

Russia often privileges quantity over quality in operations that involve social media efforts, placing volume over plausibility or consistency

---

[197] *United States of America v. Viktor Boris Netyksho, Boris Alekseyevich Antonov et al.*, case 1:18-cr-00215-ABJ, July 13, 2018.

[198] Ryan Broderick, "Here's Everything the Mueller Report Says About How Russian Trolls Used Social Media," *BuzzFeed News*, April 18, 2019.

[199] According to DFRLab analysis, this might have provided operational security, but it did severely limit the impact of the operation: The profiles failed to gain traction with other users because of their short existence. DFRLab, 2019.

[200] Nakashima, 2017b.

[201] These groups attracted on the order of 200,000 to 300,000 followers each before Facebook took them offline. See Broderick, 2019.

[202] Harding, 2019.

of disseminated narratives.[203] Russian actors achieve high volumes through several tools.[204] Bots are responsible for a disproportionate share of disseminated content, especially on Twitter.[205] Russian actors also use other tactics to similar effect: For example, Russian social media accounts might spread ordinary content as a way to gain more followers and then inject propaganda, disinformation, or divisive content.[206] Russia also exploits search algorithms to return Russian sources as the top results for particular topics.[207] According to the U.S. criminal complaint against an IRA employee, the IRA contained a search engine optimization department.[208]

### Microtargeting and Individual Targeting

Russian actors exploit the vast amounts of data available about social media users to microtarget content to those who are most susceptible to the message. The IRA accounts exploited Facebook's advertising algorithms to microtarget U.S. audiences: One Facebook ad, for instance, "geotargeted several regions in Pennsylvania, then added additional interest targeting to reach 18- to 65-year-olds with the interest 'Donald Trump for President, Job title: Coal Miner,'" with the goal of populating a rally for miners.[209] The same is the case with social media accounts operated by the Russian military.[210] Similarly, efforts to hack and take

---

[203] Christopher Paul 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.

[204] Helmus et al., 2018, p. 22.

[205] For an overview, see Helmus et al., 2018, p. 25.

[206] David Salvo and Bradley Hanlon, "Key Takeaways from the Kremlin's Recent Interference Offensive," Alliance for Securing Democracy, October 11, 2018.

[207] Daniel Boffey, "Europe's New Cold War Turns Digital as Vladimir Putin Expands Media Offensive," *The Guardian*, March 5, 2016; Bradley Hanlon, "From Nord Stream to Novichok: Kremlin Propaganda on Google's Front Page," Alliance for Securing Democracy, June 14, 2018; Rosenberger, 2018.

[208] *United States v. Khusyaynova*, 2018.

[209] See, for example, DiResta et al., 2018, p. 35; Helmus et al., 2018, p. 21.

[210] Calabresi, 2017.

over social media accounts of U.S. and Western users have relied on microtargeting to more effectively lure victims to click on their bait.[211]

Apart from microtargeting based on user characteristics, Russia also targets specific individuals to intimidate, harass, or demoralize—typically Russia critics or those exposing Russian misdeeds. These activities are typically accomplished by a variety of trolls.[212] Russian actors also hack high-level officials or other well-known individuals such as athletes, to obtain content they can then leak, sometimes in altered form.[213] Similarly, Russian actors can seek intelligence or personal information from specific individuals, a function that the so-called *honeypot* (attractive female) trolls commonly perform.[214] Russia also targeted specific individuals to use as conduits for further dissemination of content that Russia would like to spread.[215]

### Amplification of Native Content

Russia not only produces its own content, it also promotes native content. For instance, the world's biggest neo-Nazi website, *The Daily Stormer*, was promoted on social media "by a suspected Russian bot network."[216] Likewise, Russian actors offer platforms for fringe or radi-

---

[211] Calabresi, 2017.

[212] For the example of attacks on Finnish journalist Jessika Aro, see "Jessikka Aro: How Pro-Russian Trolls Tried to Destroy Me," BBC, October 6, 2017. For the example of the campaign to discredit Eliot Higgins of Bellingcat, see Steven Livingston, "Disinformation Campaigns Target Tech-Enabled Citizen Journalists," Brookings Institution, March 2, 2017; and Ben Nimmo, "Putin Sets His Disinformation Trolls on the MH 17 Investigators," *Newsweek*, September 28, 2016.

[213] See Salvo and Hanlon, 2018.

[214] Weisburd, Watts, and Berger, 2016.

[215] Senior intelligence officials have relayed that they "have seen evidence of Russia using its algorithmic techniques to target the social media accounts of particular reporters . . . 'who might be a little bit slanted toward believing things, and they'll hit him' with a flood of fake news stories" (Calabresi, 2017).

[216] Luke O'Brien, "The Making of an American Nazi," *The Atlantic*, December 2017; U.S. Senate Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, Washington, D.C.: U.S. Government Publishing Office, January 10, 2018.

cal native figures: In Germany, for example, Sputnik provided a platform for quotes from German far-right political parties, featuring such claims as "rape is increasing due to Merkel's policy."[217] Russian actors also help particular messages originated by native speakers go viral, as was the case, for example, with the allegation by the notorious pharmaceutical executive Martin Shkreli that Hillary Clinton had Parkinson's disease.[218] Russian media outlets and state-affiliated actors have promoted the work of Belarusian officials and authors who say they believe that their country should unite with Russia: Since mid-2018, for example, Sputnik has reportedly offered pro-Russian Belarusian compensation for writing articles and blogposts.[219]

### Organization of Real-Life Events

What happens on social media does not stay on social media—in numerous instances, Russian actors use social media to organize real-life events, such as protests. For instance, one of the most popular IRA Facebook groups, the Heart of Texas, organized a Stop Islamization of Texas rally.[220] Individual IRA accounts have also sought to orchestrate protests and other collective actions in the United States through social media—for instance, an anti-Trump flash mob at the White House.[221] Across the Atlantic, suspected Russian state-sponsored actors attempted to pit anti-fascist demonstrators against Germany's far-right movement in Berlin during the most recent European Parliament elections.[222] Apart from protests, some social media–centered activi-

---

[217] Anne Applebaum, Peter Pomerantsev, Melanie Smith, and Chloe Colliver, *"Make Germany Great Again": Kremlin, Alt-Right and International Influences in the 2017 German Elections*, London: Institute for Strategic Dialogue, 2017, p. 12.

[218] Calabresi, May 2017.

[219] International Strategic Action Network for Security, 2019, pp. 24–26, 46.

[220] See, for example, Lister and Sebastian, 2017.

[221] *United States v. Khusyaynova*, 2018, p. 20.

[222] Available digital forensics indicate that the same actors who broke into the U.S. Democratic National Committee servers in 2016 set up the anti-fascist and far-right confrontation in Berlin. Matt Apuzzo and Adam Satariano, "Russia Is Targeting Europe's Elections. So Are Far-Right Copycats," *New York Times*, May 12, 2019b.

ties appear calculated to produce mass panic or disorder: In the 2014 Columbia Chemical Hoax, IRA operators disseminated fake messages about an explosion at a chemical plant in a Louisiana town, complete with numerous fake accounts and fabricated news reports from actual news outlets.[223]

### Campaigns with a Focus on U.S. Military, Associates, and Veterans

Although the number of what might loosely be described as information social media campaigns waged by Russia is large, some have special relevance to USAF and the U.S. armed forces: those that have focused on the U.S. military, veterans, and their families—all of whom have been a consistent focus of Russian social media–based influence campaigns since at least 2013.

Russian actors have threatened particular individuals, apparently to support Russian foreign policy narratives. The GRU Threat Group—which includes outfits identified as APT28, Sofacy, Sednit, Fancy Bear, and Pawn Storm—used social media to impersonate Islamic State users and intimidate military wives. Several women, likely identified by their public roles on military issues, received individualized death threats on Facebook and Twitter from Cyber Caliphate, a now-defunct loose association of hacking groups that claimed to operate on behalf of ISIL. Cybersecurity experts and intelligence services of at least three Western countries have identified the Cyber Caliphate as one of Russia's proxies.[224] In one case, an account for the charity Military Spouses of Strength, which was operated by one of the targeted women, was hacked and exploited to broadcast threats to others.[225] The campaign was intended to inflate perceptions of the Islamic State threat in much the same way the IRA trolls

---

[223] Chen, 2015.

[224] "Proof that the military wives were targeted by Russian hackers is laid out in a digital hit list provided to the [Associated Press] by the cybersecurity company Secureworks last year" (Raphael Satter, "Russian Hackers Who Posed as ISIS Militants Threatened Military Wives," Talking Points Memo, May 8, 2018; also see "Threat Group-4127 Targets Google Accounts," *Secureworks*, June 26, 2016). Generally, that Cyber Caliphate is a Russian operation became "the consensus view among Western intelligence services" (Schindler, 2016).

[225] Satter, 2018.

operated around the 2016 presidential campaign—and potentially to deflect attention away from Russia's actions in Ukraine and encourage support for Russia's action to fight Islamic states and the Assad regime in the Syrian conflict.[226] The Cyber Caliphate previously used the U.S. Central Command's official Twitter and YouTube sites in 2015 to broadcast threats to U.S. soldiers and leak personal identifying information and nonpublic military documents.[227] Similar activity has been undertaken by actors who likely *are* associated with the Islamic State—for instance, in March 2015, the Islamic State Hacking Division posted names, photos, and addresses of 100 service members—including Air Force personnel assigned to the 2nd and 5th Bomb Wings—to a kill list in an ostensible retaliation for U.S. attacks on ISIL in Syria, Iraq and Yemen.[228] The similarity and proximity of these operations demonstrate the difficulties in definitively attributing this activity to specific actors.[229]

The following year, the same actors hacked the Gmail account of Gen Philip Breedlove, the former Supreme Allied Commander of NATO, publishing hacked content on DCLeaks.[230] This appears to have been an attempt to embarrass NATO by lending support to the long-standing Russian foreign policy narrative of NATO aggression: In reporting on the hacked emails, for example, RT claimed that

---

[226] The incidents predated Russian military involvement in Syria, but Russia has been supporting President Assad since the early stages of the conflict, presenting his regime as the only force strong enough to overcome the terrorist threat.

[227] "Most of the material was labeled "FOUO," which means "For Official Use Only," but none of it appeared to be classified or sensitive information." Lolita C. Baldor, "Key US Military Command's Twitter, YouTube Sites Hacked," APNews, January 12, 2015; also see Schreckinger, 2017.

[228] Michael S. Schmidt and Helene Cooper, "ISIS Urges Sympathizers to Kill U.S. Service Members It Identifies," *New York Times*, March 21, 2015.

[229] Pierluigi Paganini, *ISIS Cyber Capabilities*, Madison, Wisc.: Infosec Institute, May 9, 2016.

[230] Michael Riley, "Russian Hackers of DNC Said to Nab Secrets from NATO, Soros," Bloomberg, August 11, 2016; Schreckinger, 2017.

Breedlove's emails demonstrated the "ex-NATO general plotting U.S. conflict with Russia."[231]

In 2017, U.S. counterintelligence reportedly concluded that Russian hackers "were targeting 10,000 Department of Defense employees with highly targeted messages on Twitter designed to trick them into downloading malware that could compromise their Twitter accounts, computers and phones."[232] Russians "expertly tailored messages carrying malware" using individual interests—for example, offering "links to stories on recent sporting events or the Oscars."[233] Clicking on the link would allow the Russians to take control of the victims' devices and Twitter accounts.[234] The danger is that Russian operators can gain and exploit control over real military Twitter accounts to simultaneously broadcast fake information—causing alarm or confusion or prompting behaviors adverse to U.S. interests.

Russian actors have also sought to expose military and veteran audiences to divisive content and other propaganda. A considerable number of IRA accounts, for example, impersonate individuals with links to the military and then connect to real military audiences on social media. Some accounts attracted thousands of followers—such as the account profiled by Voice of America in the graphic reproduced in Figure 3.2.[235] Importantly, the extent of Russian social media penetration of military audiences is unknown. As Bret Schafer of the German Marshall Fund's Alliance for Securing Democracy points out, "a lot of this probably would be happening more in closed Facebook groups, of which there are many with the military, and frankly, nobody has any

---

[231] "Breedlove's War: Emails Show Ex-NATO General Plotting U.S. Conflict with Russia," RT, July 1, 2016. The attack on Breedlove is not an isolated incident; the military is frequently a target of hacking attempts. A "security oversight" by Fancy Bear (GRU) revealed thousands of targets of phishing attempts (outside the FSU) in 2015, of which 41 percent were current or former military, according to SecureWorks. See Schreckinger, 2017.

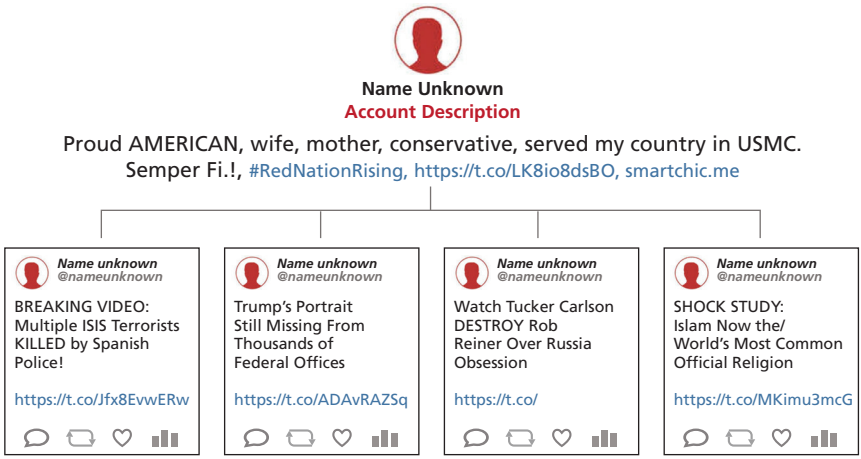
[232] Calabresi, 2017.

[233] Calabresi, 2017.

[234] Calabresi, 2017.

[235] Seldin, 2018.

**Figure 3.2**
**Sample IRA Military Account**




SOURCE: Seldin, 2018.

idea what's really happening for those groups, because of course Facebook doesn't share those with researchers."[236]

Russia also seeks to coopt existing U.S. outlets that cater to military audiences. For example, *Veterans Today* is a fringe, homegrown site that purports to publish news, has a penchant for conspiracy theories, and offers help to former service members with jobs and medical bills.[237] In 2013, it partnered with *New Eastern Outlook*, a geopolitical journal of the government-sponsored Russian Academy of Sciences and began publishing their content. In 2015, it also partnered with Southfront, an anonymously authored military affairs website registered in Moscow and well known for its pro-Kremlin messaging.[238] Simultaneously, the related Veteransnewsnow.com began posting information

[236] Seldin, 2018.

[237] Schreckinger, 2017.

[238] Schreckinger, 2017; Greg Gordon and David Goldstein, "Russian Propaganda Targeted US Vets and Service Members Via Social Media," *Task and Purpose*, October 9, 2017. Regarding Southfront, see Jessikka Aro, "The Cyberspace War: Propaganda and Trolling as Warfare Tools," *European View*, Vol. 15, June 1, 2016, p. 121.

from the Moscow think tank Strategic Culture Foundation.[239] Content from these sites spreads a garden-variety combination of conspiracy theories and stories echoing Russian foreign policy narratives.[240] Extreme right-wing (and to a lesser extent, extreme left-wing) accounts then disseminate content from these publications on social media, increasing the reach of that material.[241] Although none of the Russian partners to the American sites is openly connected to any of Russia's intelligence services, the GRU exploited the same publication: One of its social-media cut-outs, Alice Donovan, lambasted Turkey on *Veterans Today* after that country downed a Russian military aircraft in late 2015.[242]

Russian actors have also used military and veterans' issues to exploit social divides. The recent study of IRA activity, which drew on data provided by the three primary social media platforms to the U.S. Senate Select Committee on Intelligence, identified veterans' issues as one of the key themes that IRA-linked accounts "repeatedly emphasized and reinforced across their Facebook, Instagram, and YouTube content."[243] The IRA used veterans' issues to "create and reinforce tribalism," particularly among the political right—for example, by alleging that President Barack Obama treated veterans worse than refugees.[244] The IRA's choice of content and target audience appears to have been

---

[239] Schreckinger, 2017; Gordon and Goldstein, 2017.

[240] Schreckinger, 2017; Gordon and Goldstein, 2017.

[241] The study finds that

> on Twitter, there are significant and persistent interactions between current and former military personnel and a broad network of Russia-focused accounts, conspiracy theory focused accounts, and European right-wing accounts. These interactions are often mediated by pro-Trump users and accounts that identify with far-right political movements in the US (John D. Gallacher, Vlad Barash, Philip N. Howard, and John Kelly, "Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns Against US Military Personnel and Veterans," ComProp Data Memo 2017.9, October 9, 2017).

[242] Alice Donovan, "Does America Need Such Friends," *Veterans Today*, February 25, 2016.

[243] DiResta et al., 2018, p. 11.

[244] *United States v. Khusyaynova*, 2018.

a success: Content pitting immigrants against veterans was one of the IRA's top five posts on Facebook.[245]

Finally, Russian actors have exploited the permissive environment of social media to gather intelligence on the military community. Intelligence collection might be simply that—but it also might serve as a prelude to microtargeting content, blackmail, leaks, or a takeover of social media accounts to transmit messaging harmful to U.S. interests.[246]

As of late 2018, multiple U.S. defense and security officials said that Russia's targeting of U.S. personnel during influence campaigns was a concern, leading one expert to conclude that Russia had "won over a huge base of support" among enlisted service members.[247] Breedlove, the former supreme commander of NATO forces, claimed that "[w]hat Russia is doing across the gamut from our internal audience to military audiences and others is quite astronomical."[248] The impact of Russia's activity remains uncertain empirically. Nonetheless, because of the importance of these audiences, particular care should be taken to monitor Russian information activity on social media and to inoculate the U.S. military against the harmful effects of such activity.

## Russian Assessment of Its Social Media Efforts

Whether and how Russia will wage information warfare on social media in the future depend in large part on how successful it believes it has been in using this tool. The amount of attention and alarm that Russia's information efforts, including those on social media, have attracted might suggest that Russia has been quite successful. Objec-

---

[245] Howard et al., 2018, p. 7.

[246] Schreckinger, 2017. For another example of the uses that Russia has made of social media data on allied soldiers, see Sebastian Bay, Giorgio Bertolin, Nora Biteniece, Edward H. Christie, Anton Dek, Rolf E. Fredheim, John D. Gallacher, Kateryna Kononova, and Tetiana Marchenko, *Responding to Cognitive Security Challenges*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, January 2019, p. 16.

[247] Seldin, 2018.

[248] Schreckinger, 2017.

tive evidence suggests that the impact of its social media–based disinformation has been mixed or remains unknown. On the one hand, opinion polls show robust levels of support for narratives commonly promoted by Russia in some countries.[249] Recent research also suggests that, within the former Soviet Union, exposure to Russian television was associated with opinions more consistent with Russian narratives on the Ukraine crisis, and Russian television substantially increased average electoral support for pro-Russian parties and candidates in Ukraine's 2014 elections.[250] At the same time, the few methodologically rigorous recent studies of Russian disinformation and propaganda do not yield unambiguous conclusions about Russia's ability to influence politically significant behaviors or opinions in Western countries.[251] Even the volume or reach of Russian disinformation is at times difficult to assess.[252] Evidence that social media and related information campaigns actually redound to Russia's strategic advantage is

[249] For example, see "Disinformation Operations in the Czech Republic," European Values Center for Security Policy, blog post, September 13, 2016; GLOBSEC Policy Institute, "Central Europe Under the Fire of Propaganda: Public Opinion Poll Analysis in the Czech Republic, Hungary and Slovakia," September 2016.

[250] Theodore P. Gerber and Jane Zavisca, "Does Russian Propaganda Work?" *Washington Quarterly*, Vol. 39, No. 2, Summer 2016; Leonid Peisakhin and Arturas Rozenas, "Electoral Effects of Biased Media: Russian Television in Ukraine," *American Journal of Political Science*, Vol. 62, No. 3, 2018.

[251] For examples of such recent studies, see Christopher A. Bail, Brian Guay, Emily Maloney, Aidan Combs, D. Sunshine Hillygus, Friedolin Merhout, Deen Freelon, and Alexander Volfovsky, "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *Proceedings of the National Academy of Sciences*, Vol. 117, No. 1, January 7, 2020. For a brief summary of some of the relevant literature on the effects of political campaigns, see Justin Grimmer, "Cyberwar: How Russian Hackers and Trolls Helped Elect a President—What We Don't, Can't, and Do Know," *Public Opinion Quarterly*, Vol. 83, No. 1, Spring 2019.

[252] For example, two expert groups assessed Russia's impact on the Brexit debate on Twitter, and came to different conclusions: The communications agency 89up found that RT and Sputnik "won the Twitter war" by being more popular than other pro-leave groups, whereas Oxford's Computational Propaganda Research Project found that Russian Twitter activity contributed relatively little to the overall Brexit conversation. Erik Brattberg and Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, May 23, 2018, pp. 14–15.

also mixed, at best.[253] Generally, impact of Russia's social media–based disinformation on specific politically significant outcomes remains difficult to assess.[254] This is because increasing political polarization, decreasing regard for professional media and expert knowledge, and the rise of populism in some Western countries all produce an environment that both generates and embraces the same kinds of narratives that are promoted by Russia.[255]

It is likely that some discrete social media campaigns have successfully attained their goals. An early 2014 GRU campaign in Ukraine garnered 200,000 Facebook views in a single day, which led the GRU officers to declare the campaign a success in their report to their superiors, stating that the "overwhelming majority of social media users agreed with the posted arguments and supported the authors' positions."[256] Other efforts clearly flopped. Although calculating the dissemination of particular pieces of disinformation is not a reliable way to measure success, not reaching audiences is a definite indication of failure—and at least some of Russia's social media information initiatives have failed to get any traction.[257]

Notwithstanding the uncertainty surrounding ultimate impact and some evident failures, Russians have generally conveyed the impression of their own success. Regarding Russian interference

---

[253] For example, a study of Russia's effects on electoral outcomes finds "little evidence thus far that Russia has had much of an impact on Western democracies." Lucan Ahmad Way and Adam Casey, Stanford University, *Is Russia a Threat to Western Democracy? Russian Intervention in Foreign Elections, 1991–2017*, Stanford, Calif.: Stanford University, November 3, 2017.

[254] The absence of proverbial natural experiments makes it difficult to isolate causes of particular opinions or behaviors. When it comes to the observed effects of Russian television, for instance, the impact of Russian broadcasts is tough to discern because people who already harbor pro-Russian sentiments are more likely to seek out Russian television channels to begin with.

[255] For example, see Way and Casey, 2017, p. 1.

[256] This appears to have been achieved in part by buying advertisements to boost the popularity of the material. Nakashima, 2017b.

[257] As DFRLab found regarding an information campaign (dubbed Secondary Infektion) that it attributes to Russian intelligence, "almost none of the operation's stories had significant traction." See DFRLab, 2019.

in U.S. elections, Director for National Intelligence Daniel Coats assessed that "there should be no doubt that Russia perceives its past efforts as successful."[258] Various individuals boast of Russia's successes with information confrontation more broadly and with social media–based efforts specifically. For example, Andrey Krutskikh, a Putin adviser, compared Russia's information warfare capabilities to obtaining a nuclear weapon, claiming that Russia is "at the verge of having something in the information arena which will allow us to talk to the Americans as equals."[259] Commenting on Russia's performance in Syria, Colonel-General Aleksandr Dvornikov, the commander of Russia's Southern Military District, emphasized the importance of information warfare: "[I]nformational resources became one of our most effective weapons," and "without information operations, we would not have success in Aleppo, Deir-ez-Zor, and Gutta."[260] More squarely addressing social media–based information efforts, Konstantin Rykov (a businessman, propagandist, and member of Russian parliament) has claimed that "We succeeded, Trump is president," adding that "[u]nfortunately, Marine [Le Pen] did not become president [of France in the 2017 election]. One thing worked, but not the other."[261] Such statements are almost certainly self-serving in part, driven at times by institutional self-interest, as funding for various actors and lines of effort is likely tied to perceived success or publicity seeking.[262] Nonetheless, Russia has persisted even when met

---

[258] Matthew Rosenberg, Charlie Savage, and Michael Wines, "Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn," *New York Times*, February 13, 2018.

[259] David Ignatius, "Russia's Radical New Strategy for Information Warfare," *Washington Post*, January 18, 2017.

[260] Aleksandr Dvornikov, "Headquarters for New Wars [Штабы для новых войн]," *Military-Industrial Courier [Военно-промышленный курьер]*, No. 28, July 24, 2018.

[261] Jean-Baptiste Jeangène Vilmer, *The "Macron Leaks" Operation: A Post-Mortem*, Washington, D.C.: Atlantic Council, June 2019, p. 21.

[262] Interview with academic, Washington, D.C., February 11, 2019. For an example of likely publicity-seeking pronouncements of success, see Scott Stedman, "Kremlin Propagandist Boasted of His Hacking Efforts, Strongly Implied Colluding with Trump Team in Facebook Posts," *Medium*, November 21, 2017.

with specific failures: Although Russia's attempts to influence the Macron election in France largely failed, evidence suggests that Russians are persisting in their efforts to fuel conflict in France—such as by spreading disinformation pertaining to the yellow vest protests.[263] Russia also has persisted in its social media subterfuge, even as efforts are detected and Russian connections unmasked and blocked from social media platforms.[264] Combined with Russia's conviction that the modern age is one of global information confrontation, we cannot but infer that Russia finds these efforts worthwhile—and that Russian social media–based information warfare is here to stay.

---

[263] On failure of French campaign, see Adam Nossiter, David E. Sanger, and Nicole Perlroth, "Hackers Came, but the French Were Prepared," *New York Times*, May 9, 2017. On the disinformation spread by pro-Kremlin accounts about yellow vests, see DiResta et al., 2018; Gabriella Gricius, "How Russia's Disinformation Campaigns Are Succeeding in Europe," *Global Security Review*, May 11, 2019.

[264] For further discussion of the effects of Western countermeasures on Russian social media activity, see Chapter Four.

CHAPTER FOUR

# Regional Experiences and Responses to Russian Disinformation

Intensifying Russian information warfare has raised increasing alarm among U.S. allies and partners, prompting a variety of national and international responses. A companion report in this series covers the U.S. government and the tech sector responses;[1] here, we focus on NATO, the EU and select European states and civil society. With a few exceptions, for the most part, the West's response to Russian state-sponsored social media influence operations has been checkered and disjointed. Partly as a result of Western countermeasures, decisionmakers and some social media consumer audiences are increasingly aware Russia's activities, and new institutions have been stood up to confront information threats. Still, as this chapter suggests, there is little evidence to suggest that existing countermeasures have prevented or deterred Russia's engagement in information warfare online.

## Framing the Response

We can think of social media–based information operations in terms of stages, from *production* of the content (which might entail creating or stealing or hacking), the *distribution* of content through social media channels, and the *consumption* of content by audiences of social media

[1] See Raphael S. Cohen, Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwille, Elina Treyger, Nathan Vest, *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*, Santa Monica, Calif.: RAND Corporation, RR-4373/1-AF, 2021.

users. Countermeasures might be aimed at any one or more stages in that chain.[2] Countermeasures might also accomplish the logically prior functions of awareness-raising or institution-building. Table 4.1 lays out these categories of countermeasures with select examples of each type.

Countermeasures aimed at the production stage are those that aim to prevent Russian actors from producing or ordering production of content—i.e., creating false or manipulated information or engaging in cyberattacks to obtain protected information. Prevention can mean deterrence by punishment: economic sanctions, diplomatic isolation,

**Table 4.1**
**Countermeasures**

| Production (prevent actors from producing or ordering production of content) | Distribution (restrict actors from distributing content) | Consumption (build audience resilience, lower susceptibility to content) |
|---|---|---|
| • Deterrence by denial<br>• Deterrence by punishment<br>• Blocking of Russian actors | • Deterrence by denial<br>• Deterrence by punishment<br>• Blocking of Russian actors<br>• Banning or restricting social media channels<br>• Algorithmic, legal, and manual limits on spread of disinformation | • Debunking<br>• Media literacy<br>• Proactive public diplomacy<br>• Positive strategic communication and message discipline<br>• Reducing credibility of messengers and/or messages |
| **Detection and Awareness-Raising**<br>• Identifying and analyzing the actors and mechanisms inside the disinformation life cycle<br>• Raising awareness of threat among decisionmakers and other audiences | | |
| **Institution-Building**<br>• Creating institutions with authority and capabilities to combat Russian disinformation | | |

[2] Prior RAND research has conceptualized countermeasures to information warfare in these terms. See Matthews et al., 2021. For a largely similar approach, see Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence*, Santa Monica, Calif.: RAND Corporation, RR-2740-RC, 2018.

criminal indictments—consequences that exceed the gains from the offending action. These measures can aim at the state as a whole or at specific individuals. CYBERCOM's recent activity is an example of the latter: In late 2018, CYBERCOM began sending warning messages to individual Russian disinformation specialists to cease their operations.[3] Prevention can also mean deterrence by denial, or making actors believe they will fail to attain their goals either by making it difficult to conduct social media operations or by making these operations less profitable.[4] Other production-side countermeasures might seek to prevent or block the ability of producers to place disinformation on social media—demanding identity verification, for example, or conducting cyberoperations that take trolls offline, as was done by CYBERCOM to IRA trolls on the day of the 2018 U.S. midterm election.[5]

Measures aimed at the distribution stage are those that prevent the spread of disinformation or propaganda. Such measures include methods of identifying and thwarting social media accounts that spread disinformation or restricting channels available for Russian actors to do so. The same kinds of countermeasures that target original producers are available to target distributors—for example, threatening prosecution or increasing the difficulty of spreading content on social media platforms by blocking accounts. The spread of disinformation also might be lim-

---

[3] Julian E. Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," *New York Times*, October 23, 2018. It should be noted that some experts doubt the applicability of deterrence to cyberspace. For example, see Max Smeets, "Europe Slowly Starts to Talk Openly About Offensive Cyber Operations," Council on Foreign Relations blog post, November 6, 2017.

[4] Glenn Herald Snyder, *Deterrence and Defense: Toward a Theory of National Security*, Princeton, N.J.: Princeton University Press, 1961. The scholarly literature distinguishes between *deterrence by denial*, which refers to measures taken prior to an attack, and *defense*, which refers to measures taken once an attack is occurring. However, as prior RAND work points out, this distinction is not very helpful with regard to activities that tend to be continuous rather than to come in discrete attacks. See Bodine-Baron et al., 2018, p. 21. Thus, although some measures are perhaps best viewed as defense, they are treated here as deterrence by denial.

[5] Catalin Cimpanu, "US Wiped Hard Drives at Russia's 'Troll Factory' in Last Year's Hack," *Zero Day*, February 28, 2019; David Ignatius, "The U.S. Military Is Quietly Launching Efforts to Deter Russian Meddling," *Washington Post*, February 7, 2019; Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019.

ited by use of algorithms that filter out items identified as fake, laws and regulations that prohibit or censor certain content or content creators, and manual processes that filter out disinformation or propaganda.

Measures aimed at the consumption stage seek to build resilience, reduce susceptibility, or inoculate audiences against Russian information operations. Activities that can help meet these goals include *debunking* (i.e., exposing disinformation or information that is otherwise manipulated) and education, particularly *media literacy*. Exposing audiences to proactive public diplomacy or positive strategic communication also might reduce susceptibility to disinformation about those subjects. Countermeasures can also be taken to try to reduce the credibility of particular messages or messengers, such as through warnings, tagging of information that is suspected of being false, or identifying particular sources as suspect.[6]

Outside the production-to-consumption chain, *institution-building* entails creating institutions with the requisite authority and capabilities to counter Russian information operations online. *Awareness-raising* measures increase the awareness of Russia's disinformation and propaganda activities online by key Western actors who are in a position to act on a threat. This can be accomplished through detection and through research and analysis. *Detection* means identifying covert actors as Russian operators; this is also a prerequisite to several other measures. *Research and analysis* goes beyond detection and aims at better understanding the nature of social media–based information warfare and potential countermeasures. Detection and research and analysis, when publicized to social media users, also address users' consumption, potentially reducing their susceptibility to disinformation.

Not all countermeasures are adopted primarily with the Russian threat in mind. Digital identity verifications or comprehensive laws, such as the General Data Protection Regulation, likely make the social media landscape more difficult for Russian actors to navigate, but they also come with trade-offs, the evaluation of which is beyond the ambition of this study.

---

[6] See, for example, Digital, Culture, Media and Sport Committee, 2018, p. 85.

For the most part, intergovernmental and nongovernmental responses have generally focused on awareness-raising and consumption. Moreover, because the threat of information manipulation on social media is recent and novel, Western governments have devoted considerable effort to institution-building. Countermeasures aimed at the distribution stage tend to be within the province of social media companies. Individual European states' responses vary from virtual inaction to a menu of countermeasures across all categories; here, we highlight only select aspects of these responses.

## International Responses

NATO's most noteworthy institution-building achievement is the 2014 creation of the StratCom CoE in Riga, Latvia. The center advances NATO's operations and counters adversaries' information operations through public diplomacy, civilian and military public affairs, and information and psychological operations.[7] StratCom CoE's efforts have been concentrated on improving understanding of hostile information efforts, including via social media, and identifying how NATO and its member states can counter hostile cyber and information activities.[8]

NATO also has a team of approximately a dozen people (as of 2018) to detect disinformation operations, in addition to the individual efforts of NATO states.[9] For example, after suspected Russian actors planted a fake report about German soldiers stationed in Lithuania raping a local girl, Lithuanian communications specialists quickly flagged the report for other NATO members. Its swift action was pos-

[7] NATO StraCcom CoE, "About Strategic Communications," webpage, undated.

[8] For example, Bay et al., 2019, presents several studies and research related to Russian information operations. And further institution-building is afoot: In 2018, officials endorsed a framework to stand up a NATO Intelligence Academy. See NATO, "Allied Intelligence Chiefs Discuss Countering Cyberattacks, Disinformation," November 29, 2018.

[9] Vilmer et al., 2018, p. 135.

sible due to these specialists' historical analysis of related case studies and early warning provided to key officials.[10]

NATO also has stepped up its public diplomacy efforts on social media, in parallel with debunking Russian disinformation. In 2017, NATO launched the "We Are NATO" campaign online to "explain NATO's core mission of guaranteeing freedom and security" to educate and inform younger generations in NATO member states and the wider world about NATO's role in global security.[11] NATO gives a prominent place to debunking Russian accusations on its website.[12] In 2015, NATO's Science and Technology Organisation developed the *Digital and Social Media Playbook*, described as a "continually updated, information-environment assessment tool aimed at understanding the goals and methods used by adversaries in the information space."[13] Finally, NATO has worked on training allied troops to raise their resilience to social media operations, partly by integrating social media–based information operations into its military exercises. During Trident Juncture in 2015, for instance, NATO commanders and specialists developed social media applications on the exercise's internal network that provided training on how to quickly produce high volumes of pro-NATO content through official social media accounts to counter anti-NATO messaging.[14] Another exercise was conducted with the help of StratCom CoE, whose researchers acted as a red team, "to test just how much they could influence soldiers' real-world actions through social media manipulation."[15]

---

[10] Deutsche Welle, "Russia's Information Warfare Targets German Soldiers in Lithuania," Atlantic Council, February 24, 2017.

[11] Jane Cordy, *The Social Media Revolution: Political and Security Implications*, NATO Parliamentary Assembly Committee on the Civil Dimension of Security, October 7, 2017, p. 12.

[12] NATO, "NATO-Russia, Setting the Record Straight," August 5, 2019.

[13] Cordy, 2017, p. 12. (The playbook is not available.)

[14] Gregory M. Tomlin, "#SocialMediaMatters: Lessons Learned from Exercise Trident Juncture," *Joint Force Quarterly*, No. 82, July 1, 2016.

[15] Issie Lapowsky, "NATO Group Catfished Soldiers to Prove a Point About Privacy," *Wired*, February 18, 2019.

In parallel with the NATO efforts, the EU created the East StratCom Task Force in 2015 (as part of the Strategic Communications Division of the European External Action Service). This task force's activity is concentrated at the consumption stage, focused on debunking; positive strategic communication; and, to some extent, supporting professional media (in Eastern European countries).[16] The task force partners with local civil society groups that track Russian disinformation, such as Ukraine's StopFake, and the task force's work is publicized on *EU vs. Disinfo* website and on social media as EU Mythbusters. The focus in these activities is on Russian-language disinformation—including on Russian television, which an expert referred to as the "cradle of Russian disinformation"—and on disinformation aimed at the Eastern Partnership countries. But the majority of the task force's resources go toward positive strategic communication about European institutions, primarily to Eastern Partnership countries in local languages.[17]

Apart from the East StratCom Task Force, the EU Intelligence and Situation Center facilitates the exchange of information to enable EU members to better detect Russian disinformation attempts.[18] The European Commission pushed an EU-wide Code of Practice on Disinformation that commits signatory social media platforms to implement a variety of measures aimed at distribution and consumption stages, such as closing fake accounts and identifying bot-spread content.[19] In 2019, a Rapid Alert System, a common information-sharing platform was created to "facilitate the sharing of data and assessments of disinformation campaigns and to provide alerts on disinformation threats in real time."[20] EU-NATO cooperation is also increasing; a new European Centre for Countering Hybrid Threats launched in 2017 and has 28 member states as of 2020.[21] Its activity is concentrated on research

[16] Interview with U.S. government officials, Washington, D.C., November 29, 2018.

[17] Interview with U.S. government officials, Washington, D.C., November 29, 2018.

[18] Vilmer et al., 2018, p. 134.

[19] European Commission, 2018.

[20] European Commission, 2018.

[21] Hybrid CoE, "What Is Hybrid CoE?" webpage, undated.

and on the consumption stage, increasing the resilience of member states.[22] Finally, the EU also engages in positive communications about itself to EU citizens on social media.[23]

### Successes and Shortcomings

These international countermeasures have raised the level of awareness about Russia's social media–based information operations and Western vulnerabilities to these operations. This awareness is essential for the possibility of affecting any other aspect of Russia's information warfare, whether at the production, dissemination, or consumption stages.

NATO's exercise with StratCom CoE, for example, produced important insights. Although many details surrounding the effort remain classified, the replicated adversary was able to gather a great deal of information about the soldiers and track their movements through the experimental social media platforms.[24] The study also found lapses in social media companies' abilities to counteract suspicious activity that targeted NATO soldiers: Two of five fake profiles used during the research went undetected, and closed (private) groups established by the researchers also went without interdiction throughout the course of the study.[25]

Similarly, East StratCom Task Force's *EU vs. Disinfo* site had identified more than 2,500 instances of disinformation in 18 languages by 2017.[26] It has more than 80,000 followers on Twitter and on Facebook, and its weekly disinformation review boasts 20,000 readers—mostly experts and journalists, who are able to give broader exposure to the

---

[22] Bentzen, 2018; Associated Press "European Union to Stage War Games to Prepare for Hybrid Threats," *Los Angeles Times*, June 27, 2019.

[23] European Commission, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the Implementation of the Action Plan Against Disinformation*, Brussels, June 14, 2019.

[24] Lapowsky, 2019. For the full study, see Bay et al., 2019.

[25] Lapowsky, 2019.

[26] Vilmer et al., 2018, p. 130.

debunking.[27] Its positive communication campaigns specifically target audiences that are most likely to misunderstand EU institutions.[28] Local media also further distribute the material.[29] That said, the audiences for the task force's disinformation monitoring tend to be concentrated in countries that are already less susceptible to Russian disinformation and have greater awareness of the threat.[30] This in part is because their output is produced in English and Russian.[31]

Budget considerations appear to hamstring the international responses. The NATO CoE's 2017 budget amounted to more than $4 million, but that is roughly one-quarter of the Russian IRA's spending on Project Lakhta.[32] The East StratCom Task Force is likewise underresourced.[33] The EU's new Rapid Alert System has never issued an alert because of officials' indecision about whether an incident was sufficiently serious to warrant an alert.[34]

These shortcomings are partly because of the novelty of the threat but also because of a lack of political will.[35] Some member states appear uninterested in participating in EU-wide countermeasures.[36] The European Parliament noted "limited awareness amongst some of its Member States that they are audiences and arenas of propaganda and disinformation."[37] Political sensitivities related to calling out these very

---

[27] Interview with U.S. government officials, Washington, D.C., November 29, 2018.

[28] Interview with U.S. government officials, Washington, D.C., November 29, 2018.

[29] Interview with U.S. government officials, Washington, D.C., November 29, 2018.

[30] Interview with U.S. government officials, Washington, D.C., November 29, 2018.

[31] Interview with U.S. government officials, Washington, D.C., November 29, 2018.

[32] U.S. Advisory Commission on Public Diplomacy, 2018.

[33] Vilmer et al., 2018, p. 130.

[34] Matt Apuzzo, "Europe Built a System to Fight Russian Meddling. It's Struggling," *New York Times*, July 6, 2019.

[35] Vilmer et al., 2018, p. 130.

[36] For example, the *New York Times* reports that most countries do not contribute information to the Rapid Alert System (Apuzzo, 2019).

[37] European Parliament, resolution on EU strategic communication to counteract propaganda against it by third parties, November 23, 2016.

member states as effectively being abettors in Russian efforts limit the EU's response.[38] Thus, the East StratCom Task Force monitors Russian media but cannot extend its scope to European websites or media. As the *New York Times* points out, "[i]t is one thing for analysts to call out Russian stories about Ukraine as disinformation. When those exact claims are repeated by the Hungarian government, however, things get complicated."[39]

Similarly, NATO is divided on whether it should focus on NATO-targeted disinformation or all Russian disinformation.[40] Alliance members also divided on whether to "beat Russia at its own game" by offering revised versions of history or spreading doubt about Moscow's activities and goals.[41] For the time being, such strategies appear foreclosed.[42]

Generally, little evidence suggests that any of the international responses have deterred Russian information warfare against NATO or EU states. After the 2019 European Parliamentary elections, EU officials announced that "the actions taken by the EU—together with numerous journalists, fact-checkers, platforms, national authorities, researchers, and civil society—have *helped to deter attacks* and expose attempts at interfering in our democratic processes."[43] Yet European officials reportedly "privately acknowledge that they have no evidence that their efforts specifically deterred Russian propaganda."[44]

---

[38] Interview with U.S. government officials, Washington, D.C., November 29, 2018; Apuzzo, 2019.

[39] Apuzzo, 2019.

[40] Vilmer et al., 2018, p. 136.

[41] Vilmer et al., 2018, p. 136.

[42] Cordy, 2017, p. 13.

[43] European Commission, 2018.

[44] Apuzzo, 2019.

## National Country Responses

European governments' responses to Russian disinformation have varied greatly. The European Values Center for Security Policy, a Czech think tank, illustrates that range through its ranking of European states based on the robustness of their responses to the entire domain of the Kremlin's subversive influence activities.[45] The Baltic states, Sweden, and the United Kingdom have adopted the most-aggressive and widest-ranging countermeasures to Russian subversion. This group is followed by nine countries, including Finland, Poland, Germany, Czech Republic and France. European Values classifies Hungary, Austria, Luxembourg, Malta, Portugal, and Slovenia as "countries in denial" of Russian information warfare and other hostile influence operations, and it classifies Greece and Cyprus as "outright Kremlin collaborators."[46]

Although one might disagree with the method or particular rankings, the core proposition that Western states vary greatly in the robustness and nature of their responses is a valid one. Experts consistently point to a need for a networked or holistic response to the Russian threat because that threat cuts across jurisdictions or competences of various state bodies.[47] Thus, the most-robust national responses have included institution-building: Sweden, Finland, Denmark, the United Kingdom, the Netherlands, and Latvia have set up *networked*, or cross-cutting, institutions for this purpose. The United States, the Czech Republic, and Sweden have also set up centers devoted to the threat.[48] Similarly, experts

---

[45] We mention this to illustrate one way of capturing the differences in state responses; we do not necessarily endorse the assessment of any individual country or the methodological approach. Kremlin Watch Team, *2018 Ranking of Countermeasures by the EU28 to the Kremlin's Subversion Operations*, Prague, Czechoslovakia: European Values Center for Security Policy, June 13, 2018.

[46] Kremlin Watch Team, 2018.

[47] For example, "a consensus prevails: the nature of the problem requires a global approach, a decompartmentalized, holistic response from services that are generally fragmented" (Vilmer et al., 2018, p. 117). Also see Alina Polyakova and Spencer P. Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Washington, D.C.: Brookings Institution, March 2018; and Giles, 2016.

[48] Bentzen, 2018, p. 7; Vilmer et al., 2018, p. 117.

pointed to a need for public-private cooperation, such as the Swedish Civil Contingencies Agency cooperating with social media companies to better detect Russian information operations on their platforms.[49]

Beyond institution-building, many countries' security services have taken up the mission of monitoring the online landscape for disinformation.[50] Some countries have pioneered new detection methods: The Lithuanian defense ministry in 2018 claimed to have invented an artificial intelligence program to identify disinformation within two minutes of its publication.[51] Aiming to disrupt the production stage, states have engaged in defensive cyberoperations, imposed sanctions, penalized RT, and banned Russian-affiliated media.[52] To disrupt distribution, some states have pressured social media companies to take accounts offline.[53] Some European states also prohibited certain kinds of content, requiring social media platforms to take such content offline.[54] Some countries are standing up new military units dedicated to the modern-day social media–based information warfare, such as the UK 77th Brigade, which is intended to leverage social media to "control the narrative."[55] Germany's military in 2017 established the Cyber and Information Space (Cyber-und Informationsraum) outfit

---

[49] Gabriel Cederberg, *Catching Swedish Phish: How Sweden Is Protecting Its 2018 Elections*, Defending Digital Democracy Project, August 2018, pp. 26–27.

[50] For example, "In Sweden, the Swedish Civil Contingencies Agency, which usually prepares for chemical spills, bomb threats and natural disasters, is also monitoring websites for exaggerated news stories about refugees and crime" (Dana Priest and Michael Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years," *Washington Post*, June 25, 2017).

[51] Iryna Somer, "Lithuanians Create Artificial Intelligence with Ability to Identify Fake News in 2 Minutes," *Kyiv Post*, September 21, 2018.

[52] "Latvia Shuts Down Sputnik Propaganda Website," Latvian Public Broadcasting, March 29, 2016.

[53] Priest and Birnbaum, 2017.

[54] Of these, Germany's Netzwerkdurchsetzungsgesetz (NetzDG) law is likely most aggressive, giving social media platforms only 24 hours to remove unlawful content. "Germany Fines Facebook for Underreporting Hate Speech Complaints," *DW*, July 2, 2019.

[55] Ewen MacAskill, "British Army Creates Team of Facebook Warriors," *The Guardian*, January 31, 2015. Also see Carl Miller, "Inside the British Army's Secret Information Warfare Machine," *Wired*, November 14, 2018.

within the Bundeswehr to consolidate "[information technology] IT, cybersecurity, military reconnaissance, and geo-information as well as psychological warfare," while developing defensive and offensive cyber-capabilities.[56] To build up the resilience of consumers to Russian information operations, states such as Canada, Australia, and Sweden incorporated media literacy training into their youth education systems.[57]

### Civil Society Responses

Civil society actors often have focused on debunking, and raising awareness of, Russian disinformation and propaganda. By one count, 149 fact-checking websites were active in 2018, though many predate that and/or do not focus exclusively on Russia.[58] Bellingcat, an open-source investigative outfit, conducts investigative research and analysis to assess potential disinformation. Other outfits that focus on Russia are StopFake.org in Ukraine, Estonia-based Propastop, the Atlantic Council's DFRLab in the United States, and the EU Disinfo Lab in Belgium. Hamilton 68 tracked the topics favored by Russian-affiliated social media accounts.[59] The European Values think tank in Prague engages in research and analysis of Russian hostile influence and European countermeasures.[60] Some civil society organizations have also been active in other consumption-side measures, such as media literacy training.[61]

#### *Successes and Shortcomings of National and Civil Society Responses*

A comprehensive assessment of national governmental or civil society responses is beyond the scope of our study. We observe that some of the

---

[56] Justyna Gotkowska, "The Cyber and Information Space: A New Formation in the Bundeswehr," *Fortuna's Corner*, April 12, 2017.

[57] Priest and Birnbaum, 2017.

[58] Vilmer et al., 2018, p. 137; Duke Reporters' Lab, homepage, undated.

[59] The second version of the dashboard, Hamilton 2.0, broadened the scope of the effort. See Alliance for Securing Democracy, Hamilton 2.0 Dashboard, undated.

[60] European Values Center for Security Policy, homepage, undated.

[61] For example, see IREX, "Learn to Discern (L2D)—Media Literacy Training," webpage, undated.

countries believed to be most successful at combating disinformation, such as Finland or Sweden, also tend to boast a highly educated, high-income, and civic-minded populace and to have highly professional media.[62] Consequently, it is difficult to disentangle the success of any particular countermeasures from these underlying societal vulnerabilities. Here, we expand on one country's experience and highlight a few relevant broader trends to illustrate the uncertainties inherent in assessing effects of existing countermeasures.

### The German Experience

Arguably the economic and geopolitical linchpin of the EU and a major hub for U.S. forces, Germany ranks among the more-energetic responders to Russia's subversive activities, partly because of a history of Russian activities targeting German audiences.[63] In the lead-up to its 2017 elections, Germany was particularly concerned about Russia interfering in the same way it had done in the United States and France. Prominent cases of disinformation, trolling, a large-scale hack of the Bundestag in 2015 that was attributed to ATP 28, and the registration of two leak websites (btleaks.info and btleaks.org) led Germans to expect an outbreak of Russian information warfare targeting the elections.[64] As German expert Constanze Stelzenmüller testified to the U.S. Senate in June 2017, "there is a general consensus in my country that there will be meddling; the only question is when and what form that will take."[65] High-level German officials, including the head of its domestic intelligence service (the Federal Office for the Protection

---

[62] For one assessment of Sweden's success, see Margaret L. Taylor, "Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe," Brookings Institution, July 31, 2019; for Finland's success, see Eliza Mackintosh, "Finland Is Winning the War on Fake News. What It's Learned Might Be Crucial to Western Democracy," CNN, May 2019. On Russian influence activities in Bulgaria and Serbia generally, see Dimitar Bechev, *Rival Power: Russia's Influence in Southeastern Europe*, New Haven, Conn.: Yale University Press, 2017.

[63] See, for example, the Lisa case in Germany (Meister, 2016).

[64] As Stelzenmüller, 2017, notes with regard to the Bundestag hack: "Sixteen gigabytes were taken away; we haven't seen them yet."

[65] Stelzenmüller, 2017.

of the Constitution, or BfV), voiced an expectation that Putin would order an electoral interference campaign.[66]

Thus, the German government and nongovernmental actors tried to deter and limit the impact of Russian interference. The German domestic intelligence BfV shared information with political parties on potential threats (a detection measure) and set up an official government Twitter account to quickly debunk any disinformation (a debunking measure).[67] The political parties also reached a "gentlemen's agreement" not to use bots on social media or exploit any hypothetical leaked information.[68] Facebook and Google trained political parties in defensive measures.[69] Media organizations beefed up their fact-checking operations (detection and debunking).[70] Germany also sent a message to the Kremlin that any interference would not redound to Russia's benefit (deterrence by punishment). German President Frank-Walter Steinmeier stated plainly that "[w]ere Moscow to interfere in the election of the Bundestag, then the share of commonalities will necessarily decrease further. That would be damaging for both sides."[71]

Contrary to expectations, no detectable Russian interference took place apart from ordinary background social media activity. Unlike the U.S. case, there were no leaks, no spectacular targeted disinformation campaigns, and no social media ad purchases. The central question, as a *New York Times* headline put it, was "Why no Russian meddling?"[72] Erik Brattberg and Tim Maurer, experts at the Carnegie Endowment for International Peace, suggest that the "government's active preparations" and the "high-level officials' clear warnings to Russia against interfer-

---

66 Tyson Barker, "Germany Strengthens Its Cyber Defense: How It's Meeting the Russian Threat," *Foreign Affairs*, May 26, 2017.

67 Brattberg and Maurer, 2018, p. 18.

68 Brattberg and Maurer, 2018, p. 18.

69 Eric Auchard and Toby Sterling, "Google and Sister Company to Offer Cyber Security to Election Groups," Reuters, March 21, 2017.

70 Brattberg and Maurer, 2018, p. 18.

71 Brattberg and Maurer, 2018, pp. 17–18.

72 Michael Schwirtz, "German Election Mystery: Why No Russian Meddling?" *New York Times*, September 21, 2017.

ing" might have had the desired effects.[73] In other words, the cumulative force of these countermeasures—particularly the implied threat of imposing costs contained in high-level official communications—might have deterred the Kremlin from ordering or tacitly encouraging a focused information campaign.

However, there are reasons to moderate faith in the deterrent effect of such countermeasures. As a foreign affairs expert Tyson Barker observes, "compared to the precipice elections in the United States, France, and Italy, Germany's election is shaping up to be a bit of a non-event," with "the pro-EU and internationalist consensus still hold[ing] in Germany."[74] Thus, "[u]nlike France or Italy, Germany is unlikely to change its position on the big issues that Russia cares about—including the EU, NATO, and the Ukraine crisis—regardless of the election's outcome."[75]

Of course, Russian social media–based campaigns are also motivated by goals other than concrete outcomes, and the election still presented a chance to stoke divisions and undermine faith in democratic institutions. In that regard, as experts point out, Germany presented a harder target with robust trust in political institutions and traditional media—and "unlike Americans . . . wary of information disseminated on Facebook and Twitter."[76] In other words, Russians might well have abstained from putting effort into an information campaign because of the low likelihood of success in serving any of Russia's usual purposes irrespective of election-specific countermeasures.

### Effects of Other Countermeasures

On the production side, evidence that Russian actors have been successfully deterred from producing disinformation and propaganda has been generally scant. Even if Russia was deterred from meddling in Germany's 2017 election, some experts were warning by the 2019 EU

---

[73] Brattberg and Maurer, 2018, p. 20.

[74] Barker, 2017.

[75] Barker, 2017.

[76] Schwirtz, 2017; also see Barker 2017.

elections that Russians were back meddling in German politics via social media.[77] Actors using the same server as that used by Russian DNC hackers have incited conflict between the extreme right AfD party (long supported by Russia) and German Antifa groups.[78] Websites promoting these groups have prodded thousands of their Twitter followers to take to the streets in Berlin against the AfD; although attribution is not certain, the tactic is strongly reminiscent of those used in the United States around the 2016 election.[79]

The activity of the IRA in the United States suggests the same conclusion regarding the limits of deterrence. U.S.-imposed sanctions and filed indictments against individuals operating the IRA in response to the 2016 election interference.[80] Social media companies improved detection and removed offended accounts en masse. Nonetheless, the IRA's social media activity "shows no signs of slowing down," as "the trolls are beginning to adapt their influence strategies to find ever newer ways of spreading their venom."[81] According to the Computational Propaganda Research Project, IRA activity on those platforms increased—and not trivially—after 2016. For example, average monthly Facebook posts increased more than tenfold from 2015 to 2017, and monthly Instagram posts more than doubled over the same period. The IRA appears undaunted that its "signature" will be detected: For instance, "[a]fter the election, campaigns targeting conservative voters continued to constitute the plurality of content."[82]

In sum, the Western experience suggests skepticism about the possibilities for deterring the production of disinformation by Russian actors. Why Russia is not deterred by these measures is a complex ques-

---

[77] Apuzzo and Satariano, 2019b; Matt Apuzzo and Adam Satariano, "Russia and Far Right Spreading Disinformation Ahead of EI Elections, Investigators Say," *Independent*, May 12, 2019a.

[78] Apuzzo and Satariano, 2019b.

[79] Apuzzo and Satariano, 2019b; Apuzzo and Satariano, 2019a.

[80] "TEXT: Full Mueller indictment on Russian election case," Politico, February 16, 2018.

[81] "The St. Petersburg Troll Factory Targets Elections from Germany to the United States," *EU vs. Disinfo,* April 2, 2019.

[82] Howard et al., 2018, p. 34.

tion with several potential answers. First, given the fact that Russia is sanctioned and isolated for numerous reasons, Russia might believe that abstaining from disinformation will make little or no difference in the costs already being imposed on it by Western states. Second, the deniability, or difficulties with attribution, inherent in social media operations makes it highly likely that Russian actors would opt to evade future detection rather than abstain from disinformation campaigns. Third, the threatened imposition of costs might be perceived as a provocation by Russian actors and act as a spur to action rather than a deterrent.[83]

On the distribution side, the majority of these sorts of countermeasures that limit distribution are put in place by social media companies (discussed in a companion report); these actions also have limitations.[84] For instance, "[w]hen the Black Matters Facebook page was shut down in August 2016, organizers started a new Facebook page a few days later simply called BM."[85] As observed by the *Washington Post*, "Twitter continually shuts down accounts, such as Jihadist2nd-Wife, but the IRA . . . can afford to routinely lose accounts, given the low cost of replacement and the efficiency with which they can build followers."[86]

In the overlapping realms of consumption and awareness raising, countermeasures that detect and analyze Russian social media activity have been widely deemed successful and are widely accepted as a prerequisite for any successful response.[87] Nongovernmental actors have contributed greatly to these results, even without the resources available to state intelligence services.[88] And high levels of awareness and understanding of Russian tactics underlie examples of successful state

---

[83] For a collective expert discussion of these points, see Bodine-Baron et al., 2018, pp. 22–25.

[84] Cohen et al., 2021.

[85] Howard et al., 2018, p. 9.

[86] Linvill and Warren, 2018.

[87] For conclusions of expert workshop participants, see Bodine-Baron et al., 2018, pp. 41–44.

[88] Polyakova and Boyer, 2018, p. 12. For examples, see open-source efforts of DFRLab and Bellingcat.

responses to particular information operations: For example, a piece of disinformation about German soldiers raping a minor noted above failed to spread apparently due to Lithuania's high level of awareness and swift actions in detecting and debunking.[89]

However, there is debate over the effectiveness of detection and debunking. First, few detection methods are free of error. Russia is not the only entity to use such tools as bots and trolls to amplify its narratives, and there is a risk of overattribution of information activity to Russia. For example, following the April 2018 U.S.-led strikes against Assad's Syrian regime in response to the Douma chemical attack, the Pentagon claimed a 2,000-percent increase in Russian trolls in 24 hours. DFRLab's independent analysis found no evidence to attribute any but a small amount of trolling activity to Russia.[90]

Second, detection methods might lag behind adversary adaptations. Russian information warriors are constantly "developing tactics for defeating analytical methods used to identify false personae," as Keir Giles explains.[91] This problem will only become worse in the future, experts say; as Alina Polyakova explains, "with advances in techniques that can simulate human behavior, our ability to [detect Russian information operations] is quickly coming to an end."[92]

Third, public debunking, often the next logical step after detection, is probably insufficient to correct audience beliefs in erroneous information. Audiences targeted by Russian information operations might be among those "least likely to routinely consume or access"

---

[89] Deutsche Welle, 2017.

[90] DFRLab, "#TrollTracker: 2000% More Russian Trolls on Syria Strikes?" *Medium*, April 16, 2018d; Josh Delk, "Pentagon Reports Increase in Russian Trolls Since Syria Strike," *The Hill*, April 14, 2018. Likely overattribution is not unique to the United States: After the 2019 EU elections, for example, some experts implied that the EU's conclusions about the magnitude of Russian disinformation activity were exaggerated. See Ashish Kumar Sen, "The Importance of Working Together in the Fight Against Disinformation," Atlantic Council, June 20, 2019.

[91] Giles, 2016, p. 70.

[92] Polyakova and Boyer, 2018, p. 12. In the concluding chapter of this report, we flag some of the main adaptations we should expect.

debunking resources.[93] Moreover, much social psychology research demonstrates that people do not easily change their minds.[94] Exposure to debunking might even be counterproductive—repeating a false or misleading claim to refute it reinforces the claim by increasing audience familiarity.[95] Thus, "social scientists often advise fact-checkers to emphasize truth (such as saying "Obama is Christian") and to downplay rather than emphasize a false statement (that is, refrain from saying "Report that 'Obama is Muslim' was faked")."[96]

Finally, there is widespread enthusiasm for other consumption-side measures, such as media literacy training—but much less agreement on what form such measures should take and how successful they are. Such countries as Finland are often touted as successes when it comes to training people to identify disinformation or lies.[97] However, the experiences of such highly educated, relatively homogenous countries, long sensitized to the Russian threat, cannot be interpreted to mean that media literacy training would turn other societies into equally discerning consumers of information. Research suggests that training might be effective, but there is nothing resembling a consensus among the relevant research community that media training builds up audience resilience to disinformation and propaganda.[98]

---

[93] Helmus et al., 2018, pp. 76–77.

[94] For example, see Stephan Lewandowsky, Ullrich K. H. Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook, "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest*, Vol. 13, No. 3, 2012, pp. 106–131; for an overview, see Paul and Matthews, 2019.

[95] See, for example, Briony Swire, Ullrich K. H. Ecker, and Stephan Lewandowsky, "The Role of Familiarity in Correcting Inaccurate Information," *Journal of Experimental Psychology: Learning, Memory, and Cognition*, Vol. 43, No. 12, 2017.

[96] Herb Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," *Lawfare*, blog post, September 6, 2018.

[97] Mackintosh, undated.

[98] Bodine-Baron et al., 2018, p. 48.

## Conclusion

There is no magic bullet to address the threat of Russia's information warfare, but this does not mean that countermeasures have been futile. On the contrary, within a few short years, serious institutions have been founded to confront this threat and Western policymakers are far more familiar with the activities of such actors as the GRU, the IRA, and RT. U.S. efforts to counter disinformation would be well served by continuing efforts to raise awareness—both by the intelligence community and the FBI's foreign influence task force, and within DoD—and to strengthen institutions devoted to this threat, such as the Department of State's Global Engagement Center. Some countries have earned high marks for making their citizens into more-educated consumers of social media. At the same time, there are few reasons to think that any attempts to deter the production or dissemination of disinformation have been particularly successful. This implies the need to presume the persistence of Russia's information activities and craft defensive measures accordingly. Another volume in this series of reports addresses the role that various parts of the U.S. government do and can play in this regard.[99]

[99] Cohen et al., 2021.

CHAPTER FIVE

# Case Study: Ukraine

Of all the countries targeted by Russian disinformation efforts over the past decade, Ukraine's experiences arguably provide the best window into potential Russian tactics and responses, for three reasons. First, few countries in Russia's near abroad hold as much importance for Russia as Ukraine. Aside from Ukraine's general strategic importance as a buffer between the West and Russia, Ukraine is also home to Russia's Black Sea fleet in Crimea. Even after the 2014 conflict, Russia remains Ukraine's largest export and import market.[1] Furthermore, Russia and Ukraine are culturally and linguistically intertwined: Roughly 17 percent of Ukraine's population is ethnically Russian, almost 30 percent of Ukraine's population speaks Russian, and most of Ukraine's population identifies as Orthodox Christian, which until recently was tied to the Russian Orthodox church.[2] Few targets exist that Russia knows as well as Ukraine, and if successful disinformation campaigns are predicated on a combination of level of effort and in-depth understanding of the target population, then Russian disinformation efforts in Ukraine likely show the further reaches of Russian abilities in this sphere.[3]

Second, Ukraine provides an example of how Russia might integrate disinformation efforts with kinetic action. Especially during the

[1] Russian trade accounted for 9.2 percent of Ukraine's exports and 14.5 percent of Russia's imports in 2017. Central Intelligence Agency, "Europe: Ukraine," World Factbook website, undated.

[2] Based on 2018 estimates, Central Intelligence Agency, undated.

[3] As one Ukrainian journalist put it, "Ukraine is the petri dish for Russian disinformation efforts." Interview with a Ukrainian journalist, Kyiv, Ukraine, March 5, 2019.

height of the fighting in the Donbass between 2014 and 2015, Russia used disinformation not only as a strategic tool to shape political outcomes in Kyiv but also as an operational one to undermine military mobilization, encourage defection, and spread panic. In this respect, Ukraine's experiences provide an important case study for how Russia might employ disinformation in a future conflict with the United States, NATO, and other U.S. partners and allies.

Finally, Ukraine provides a unique example in terms of how to respond to disinformation efforts. Partly because Ukraine views Russia as existential threat, it has employed tactics that other targets of Russian disinformation have yet to do, such as mobilizing civil society, banning use of mobile phones among frontline troops, and even banning an entire social network (VK).[4] In this respect, Ukraine serves as a test case not only for Russian disinformation efforts but also for potential Western responses.

## Russian Disinformation Efforts in Ukraine Before 2014

Russian disinformation efforts in Ukraine started long before the 2014 Maidan movement and the ouster of pro-Russian President Viktor Yanukovych and his government. Some themes reiterated in Russian propaganda during the war in the Donbass—for example, that the pro-Western element of Ukraine is made up of fascists—date back at least to the 1990s.[5] Russia's propaganda effort increased in the early 2000s. In 2004, a contested presidential election—mired in accusations of voter fraud—sparked a series of protests, called the Orange Revolution, and ended Yanukovych's first bid for the presidency in favor of Viktor Yushchenko.[6] Russia saw the Orange Revolution as evidence that the United States (and the West more broadly) was interfering in Russia's

[4] Interview with a Ukrainian media expert, Kyiv, Ukraine, March 5, 2019.

[5] Interview with a Ukrainian journalist, Kyiv, Ukraine, March 5, 2019.

[6] Interview with a Ukrainian journalist, Kyiv, Ukraine, March 5, 2019.

proverbial own backyard, and Russia stepped up its own propaganda efforts in response.[7]

Russian information efforts propagated the concept of *Russkiy Mir* (Russian World)—the idea that Ukraine was part of the great Russian world.[8] It emphasized nostalgia for the Soviet Union, reiterated the Soviet Union's roles in the Second World War (or Great Patriotic War) and as the protector of the Slavic nations, and insinuated that the United States was undermining Slavic brotherhood and was the true enemy of the Ukrainian people.[9] Despite the churn in Ukrainian politics and the ups and downs in its economy, however, few Ukrainian observers believed these efforts were particularly effective.[10]

But Russia's efforts were aided by an overall favorable media environment in Ukraine.[11] Partly because of Russia's and Ukraine's historical, linguistic, and ethnic links, many Ukrainians already followed Russian print and television media, particularly in the more ethnically Russian eastern parts of the country.[12] This preference extended into the social media space; VK and OK dominated the Ukraine media market, particularly in the eastern part of the country.[13] Of the two, VK attracted a larger and younger market (mostly because it offered pirated movies, music, and pornography); OK tended to play on nostalgia for the Soviet Union and draw an older, mostly female popula-

---

7 Interview with a Ukrainian journalist, Kyiv, Ukraine, March 5, 2019.

8 Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019.

9 Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

10 Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019; interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

11 See Helmus et al., 2018, p. 16.

12 "Ukraine Profile—Media," BBC, December 10, 2018.

13 Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

tion.[14] Both networks, however, are suspected of having ties with Russia's security services.[15]

Russia also could leverage more-informal ties. Given that Russian and Ukrainian security services, military, and law enforcement trained together prior to the Maidan movement and 2014, they also tended to form mutual interest groups on social media platforms—primarily on VK, but also on OK and Facebook.[16] The standard practice, however, was for individuals to use pseudonyms in these groups, creating an opportunity for Russian operatives to mask their identities.[17] As we shall show, these groups proved a useful tool for Russian disinformation efforts specifically targeting the military during the 2014–2015 conflict.

## Russian Disinformation in Ukraine During the 2014–2015 Conflict

On November 21, 2013, under Russian pressure, then-President Yanukovych ended discussions of a Ukraine-European Union Association Agreement.[18] The decision prompted more than 100,000 Ukrainians to protest Maidan Nezalezhnosti for three months, ultimately resulting in clashes with security forces in which dozens of people were killed and thousands more were injured.[19] The so-called Euromaidan ultimately resulted in Yanukovych's ouster from power, eventually producing a new and more pro-European government under President Petro Poroshenko. The Euromaidan protests and Yanukovych's ouster set in

---

[14] Interview with data analytics firm officials, Kyiv, Ukraine, March 9, 2019; interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

[15] Interview with a Ukraine media expert, Kyiv, Ukraine, March 8, 2019. For more detail about the Russian authorities establishing influence over VK, see Franke, 2015, p. 45.

[16] Interview with former Ukrainian mid-level officers, Kyiv, Ukraine, March 9, 2019.

[17] Interview with former Ukrainian mid-level officers, Kyiv, Ukraine, March 9, 2019.

[18] Lucie Steinzova and Kateryna Oliynyk, "The Sparks of Change: Ukraine's Euromaidan Protests," Radio Free Europe/Radio Liberty, November 21, 2018.

[19] Steinzova and Oliynyk, 2018.

motion a series of events that culminated in Russia's annexation of Crimea and a sustained proxy war against Russian-backed separatists in the Donbass in eastern Ukraine.[20] Throughout the entire conflict, Russia employed disinformation extensively.

Russian disinformation targeted three populations. First and on the broadest level, Russia aimed to discredit the new Ukrainian government internationally, justify Russian actions in Crimea, and frustrate an international response to the unfolding conflict. These efforts ranged from material that painted the fall of Yanukovych as an illegal coup (or a "fascist junta"), Poroshenko as corrupt and illegitimate, and Ukraine as failed state to more-extreme material that linked Ukraine to the Islamic State.[21] Russian disinformation efforts would routinely mimic pro-Ukrainian websites and social media sites to further confound the population and the international community.[22]

Russia also promoted the concept of *Novorossiya* (New Russia)—historical Russian claims to parts of eastern Ukraine—as a new identity for the breakaway republics of Donetsk and Luhansk, emphasizing their proper place with Russia. Some of the key websites promoting the concept were set up before these groups officially declared themselves independent, presumably indicating that Russia laid the groundwork in advance.[23] Groups believed to be tied to the Russian security services also promoted the idea of Novorossiya on VK.[24]

Russia adopted a more specific approach to its annexation of Crimea. A GRU campaign on social media featured fake accounts of ordinary people in Crimea expressing popular support for Russian

---

[20] For a military analysis of the ensuing events, see Kofman et al., 2017.

[21] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019; interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019; interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[22] Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019; Edward Lucas and Peter Pomerantsev, *Winning the Information War: Techniques and Counter-Strategies to Russian Propaganda in Central and Eastern Europe*, Washington, D.C.: Center for European Policy Analysis, August 2016, p. 15.

[23] These websites included Novorus, homepage, undated; and novorossia.ru, homepage, undated (website no longer active). See Reynolds, 2016, p. 25.

[24] Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

actions.[25] Russian messaging also emphasized that the "annexation of Crimea occurred without a single shot fired."[26] Putin echoed this view in his public press conferences.[27] The line served several purposes: It emphasized Russian power (that Moscow could seize key terrain without fighting for it), undermined Ukrainian morale (because Ukraine's forces gave up without a fight), and further confounded the Western response (questioning why the West should fight for something that Ukrainians were unwilling to fight for themselves). Moreover, this campaign supported the legitimacy of Russia's actions and seemed to indicate that the Crimean people welcomed the action. The narrative of the legitimacy of Crimea's unilateral secession was key for Russia, fixated as the Kremlin is on pointing out alleged Western hypocrisy: If the international community accepts the legitimacy of Kosovo, it must, according to Russia, accept the legitimacy of Crimea.[28] As it turns out, the bloodless coup narrative is an overstatement: Although accounts are murky, there were a handful of casualties and some fatalities in Crimea.[29] Nonetheless, the theme caught on, and Western media referred to this as "bloodless coup."[30]

Second, and in addition to these overall efforts, Russia also tried to induce panic in the Ukrainian population by painting the military situation as more desperate than it was. Russian messages—spread through VK groups and other means—suggested that the Ukrainian

---

[25] Interview with a Ukrainian media analyst, Kyiv, Ukraine, March 8, 2019.

[26] Interview with a Ukrainian media analyst, Kyiv, Ukraine, March 8, 2019.

[27] "Transcript: Putin Says Russia Will Protect the Rights of Russians Abroad," *Washington Post*, March 18, 2014; "Transcript: Vladimir Putin's April 17 Q&A," *Washington Post*, April 17, 2014.

[28] See, for example, Snegovaya, 2015, pp. 133–135.

[29] "Russian Marine Kills Ukraine Navy Officer in Crimea, Says Ministry," Reuters, April 7, 2014; Interfax Ukraine, "Two Die in Rallies Outside Crimean Parliament, Says Ex-Head of Mejlis," *Kyiv Post*, February 26, 2014.

[30] John Simpson, "Russia's Crimea Plan Detailed, Secret and Successful," BBC, March 19, 2014; Misha Friedman, "The High Price of Putin's Takeover of Crimea," Bloomberg, March 31, 2017.

military was crumbling and that Kyiv itself would soon be attacked.[31] Russian narratives became more believable partly because of the actual chaos inside the Ukrainian government, especially during the early phases of the conflict. Different parts of government would often relay different accounts of the fighting and varying casualty figures to media.[32] As a result, journalists accused the Ukrainian army of whitewashing the situation and cited the higher casualty figures.[33]

Third, Russia stepped up its targeting of the Ukrainian military to disrupt the mobilization process and encourage defection. Not all of this targeting occurred on social media—or even constitutes disinformation per se. For example, Russia allowed Ukrainians to volunteer for the Russian army and extended the timelines that Ukrainians could live in Russia during the conflict to increase defection and deny Ukraine a pool of eligible recruits.[34] Because of the Donbass' proximity to Russia and the fact that Russian reconnaissance groups would sabotage Ukrainian television and radio stations, Russia also dominated television and radio broadcasts in areas of the most active fighting in Eastern Ukraine.[35] As a result, Ukrainian soldiers stationed on the frontlines ultimately would turn to Russian networks by default.[36]

The Russian military also extensively used disinformation sent via social media text messages.[37] As mentioned earlier, Russia already harvested Ukrainian soldiers' personal data, possibly through social media and electronic targeting.[38] This allowed Russia to personalize its disinformation effort. Soldiers reported receiving a series of text messages, such as "you are about to die. Go home," or "this is not your war,

---

[31] Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019; interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[32] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[33] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[34] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[35] Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019.

[36] Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019.

[37] Helmus et al., 2018, p. 16; Iasiello, 2017, p. 55; Brantly and Collins, 2018.

[38] Interview with a Ukrainian journalist, Kyiv, Ukraine, March 5, 2019.

this the oligarchs' war, your family is waiting for you."[39] In some cases, the messages looked like they came from the soldier's relatives or fellow soldiers.[40] Ukrainian soldiers' family members also reported receiving personalized messages.[41] In a telltale sign of Russian authorship, some of these text messages did not capture the linguistic nuances in dialect or the mixture of Ukrainian and Russian used by the soldiers.[42]

In some cases, these disinformation cases worked in conjunction with Russian lethal targeting. As COL Liam Collins, director of the Modern War Institute at the U.S. Military Academy at West Point, explains:

> [Ukrainian] soldiers receive texts telling them they are "surrounded and abandoned." Minutes later, their families receive a text stating, "Your son is killed in action," which often prompts a call or text to the soldiers. Minutes later, soldiers receive another message telling them to "retreat and live," followed by an artillery strike to the location where a large group of cellphones was detected.[43]

In these cases, disinformation became the bait for lethal action and what started as fake news became a tragic reality.

Russia also infiltrated veterans groups' social networks to try to undermine their commitment to fighting in Eastern Ukraine, particularly targeting recently mobilized veterans.[44] Russian messages—mostly on VK but to a lesser extent on OK—accused the Ukrainian oligarchs and general officers' corps of profiting from the conflict

---

[39] Interview with a Ukrainian journalist, Kyiv, Ukraine, March 5, 2019; interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019; Brantly and Collins, 2018; Popovych and Makhuhin, 2018.

[40] Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019; DFRLab, "Electronic Warfare by Drone and SMS: How Russia-Backed Separatists Use 'Pinpoint Propaganda' in the Donbas," DFRLab via *Medium*, May 18, 2017.

[41] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[42] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019; DFRLab, 2017.

[43] Liam Collins, "Russia Gives Lessons in Electronic Warfare," Association of the United States Army, July 26, 2018.

[44] Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019.

while shielding themselves and their families from the front lines.[45] For example, one such effort suggested that the defense minister bought a $23 million house as a result of his corrupt activity.[46]

Russia also tried to drive a wedge between the regular Ukrainian military and the *volunteer forces*—ad hoc militia groups that volunteered to fight in the Donbass. Russian propaganda tried to paint these volunteer forces as fascists and undisciplined.[47] Specifically, the messaging accused the volunteers of abandoning their positions in such key battles as Ilovaisk and Debaltseve.[48] Like many Russian disinformation efforts, the claims had some basis in reality. Unsurprisingly, given that they volunteered to fight a superior foe with inadequate weapons, the volunteers probably were less disciplined and more ideological.[49] The volunteers often posted photos and videos of themselves on social media, making them targets of Russian fires (targeting off the cell phone signals) and Russian disinformation.[50] As is the case with Russian information warfare more broadly, Russian information operations in this instance seized on existing vulnerabilities and exploited them.

## Ukrainian Responses

Partly because Ukraine viewed the Russian invasion as an existential threat, Ukraine took dramatic steps to respond. Not all of these actions were successful, nor are all these actions necessarily replicable elsewhere. Still, the Ukraine example provides an important case study

---

45 Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

46 Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

47 Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019; Andrei Soshnikov, "Inside a Pro-Russia Propaganda Machine in Ukraine," BBC, November 13, 2017.

48 Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

49 For profile of these soldiers, see Michael Cohen and Mathew Green, "Ukraine's Volunteer Battalions," *Infantry Magazine*, April–July, 2016; "Ukraine's 'Invisible' Volunteer Fighters," Hromadske International, November 18, 2018.

50 Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

of how states could respond to the disinformation efforts on both the tactical and strategic levels.

### Reorganizing for Information Warfare

Ukraine has engaged in institution building to better counter information campaigns. On December 14, 2014, Ukraine established a Ministry of Information Policy of Ukraine. Officially, this ministry has three objectives: to "develop strategies for information policy of Ukraine and the concept of information security," to "coordinate government agencies in matters of communication and information dissemination," and to "counteract informational aggression by Russia."[51] In practice, the ministry has had a hand in detecting Russian disinformation campaigns, educating the population on how to spot Russian disinformation and building its own information campaigns.[52] It also has tried telling Ukraine's story to Western audiences abroad, albeit with mixed success.[53]

The Ukrainian military also reorganized to better counter Russian information efforts. To improve command and control in the information space, the Ukrainian General Staff unified public affairs, electronic warfare, and psychological operations into a single staff section called the J39.[54] However, Ukrainian military officers reported that these efforts ran into two challenges. First, the reorganization contradicted classical military command structure, which separated these fields.[55] Second, line officers undervalued information operations as a field, relative to more-traditional maneuver forces.[56]

The Ukrainian military also leveraged civil society. Prior to the conflict, the Ukrainian government—particularly the military—realized that it lacked the skills and media savvy to effectively counter

---

[51] Ministry of Information Policy of Ukraine, "About Ministry," webpage, undated.

[52] Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

[53] Interview with a senior Ukrainian government official, Kyiv, Ukraine, March 6, 2019.

[54] Interview with midgrade Ukrainian military officers, Kyiv, Ukraine, March 7, 2019.

[55] Interview with midgrade Ukrainian military officers, Kyiv, Ukraine, March 7, 2019.

[56] Interview with midgrade Ukrainian military officers, Kyiv, Ukraine, March 7, 2019.

Russian information operations, so it turned to the private sector for this expertise. Outside media advisers were embedded in key parts of ministries, including the Ministry of Defense and the General Staff.[57] The General Staff even went one step further and built an entire media team consisting of sociologists, psychologists, camera men, and journalists to help monitor the information space for Russian disinformation and to convey the Ukrainian military's story using both traditional and social media.[58]

Finally, much of Ukraine's response to Russian information operations fell wholly outside the public sector. With the Russian onslaught, a series of private NGOs sprang up in Ukraine to counter Russian disinformation and promote the Ukrainian narrative. Such organizations as StopFake, InformNapalm, and the Ukraine Crisis Media Center all were founded in 2014 to counter Russian disinformation, and many are still in existence five years later.[59]

Together, these private and public efforts pursued a variety of different strategies to counter Russian disinformation and conduct offensive information efforts on their own, with varying degrees of success.

### Media Discipline and Disinformation Inoculation

Because Russian disinformation efforts would often capitalize on Ukrainian misinformation to depict the Ukrainian government as incompetent and the situation as more dire than it actually was, the most basic—but perhaps more important—aspect of the Ukrainian response was enforcing message discipline on the Ukrainian government. In conjunction with the Ukraine Crisis Media Center, the Ukrainian government and military implemented its One Voice Policy to ensure that the Ukrainian government was only putting out one

[57] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[58] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[59] See Ukraine Crisis Media Center, "Who We Are," webpage, undated; StopFake, "About Us" webpage, undated; InformNapalm, "InformNapalm International Volunteer Community" webpage, undated.

narrative.[60] The heads from each agency would gather daily, decide on a common narrative, and hold an official press conference at Ukraine Crisis Media Center.[61] This created the image of a single, unified front. Additionally, the Ukrainian military designated a handful of selected spokespersons to explain what was occurring at the front lines.[62]

Ukraine also made a proactive effort to advance its own version of events. For example, in 2016, the Ukrainian military—in conjunction with the NGOs—released a full-scale documentary on the Battle of Debaltseve (February 15–18, 2015) in which 110 Ukrainian service members were killed and another 270 wounded.[63] The producers viewed the documentary, which aired on four Ukrainian television stations, as vital to debunking the Russian version of events and the popular perception that the senior Ukrainian political and military leadership was inept.[64] The documentary cast the action as being more complex than it seemed and maintained that evidence from the battle was later used to help advance Ukraine's cause in the Minsk agreement negotiations.[65]

Ultimately, it is difficult to measure of the effect of these efforts. Proponents argue that the One Voice Policy and the more-active public relations campaign by the Ukrainian Army contributed to the growth in the trustworthiness of the armed forces, despite battlefield losses.[66] Some media analysts make a similar claim that Battle of Debaltseve documentary also boosted popular perceptions of the armed forces.[67]

---

[60] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019; interviews with midgrade Ukrainian military officers, Kyiv, Ukraine, March 7, 2019.

[61] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019; interviews with midgrade Ukrainian military officers, Kyiv, Ukraine, March 7, 2019.

[62] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019.

[63] "Documentary about Battle of Debaltseve to be Aired on February 17," 112.International, February 16, 2016.

[64] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[65] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

[66] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019.

[67] Interview with Ukraine media expert, Kyiv, Ukraine, March 8, 2019.

But it is not entirely possible to isolate the effect of any individual measure on overall public opinion or to quantify the impact of the public and private efforts to debunk Russian disinformation. Although the Ministry of Information Policy has launched its own attempts to educate the public about Russian disinformation, it has not yet been able to prove the effectiveness of these campaigns.[68]

What is quantifiable, however, is that the demand for products from private counter-disinformation advocacy groups continue to expand. StopFake, for example, now produces content in 11 languages—Russian, English, Spanish, Romanian, Bulgarian, French, Italian, Dutch, Czech, German and Polish.[69] In addition, the organization now boasts podcasts, three television shows, and radio shows that are syndicated to Hromadske radio and broadcast across the contact line in the Donbass—and the group is working with Radio Free Europe/Radio Liberty to broadcast across Crimea.[70]

### Small and Large Bans

Ukraine also tried to combat disinformation through more-extreme measures. The military banned soldiers' use of mobile phones on the front lines for a mixture of operational security and counter-disinformation reasons,[71] but the most pressing concern likely was Russia targeting soldiers based on their phone locations.[72] According to many Ukrainian officers, however, banning phones proved impossible to enforce and soldiers found ways to smuggle them to the front.[73] The Ukrainian military also experimented with technical means to obscure which cell towers their soldiers were using, mitigating Russian efforts to geolocate Ukrainian formations (although admittedly

---

[68] Interview with a senior Ukrainian government official, Kyiv, Ukraine, March 6, 2019.

[69] StopFake, undated.

[70] Interview with a Ukrainian journalist, Kyiv, Ukraine, March 5, 2019.

[71] Interview with midgrade Ukrainian military officers, Kyiv, Ukraine, March 7, 2019.

[72] Interview with a Ukrainian cyber company, Kyiv, Ukraine, March 7, 2019.

[73] Interview with midgrade Ukrainian military officers, Kyiv, Ukraine, March 7, 2019.

not fixing the disinformation problem).[74] The effort worked work for a time but, according to Ukrainian cyber experts, is now obsolete.[75]

Ukraine experimented with more-draconian bans, as well. On May 15, 2017, Ukraine banned the Russian social network VK, among a series of sanctions on 468 Russian companies.[76] Because VK was a popular social network in Ukraine at the time, the ban proved controversial and even proponents say the rollout could have been handled better.[77] Nonetheless, the argument was that VK's and OK's close ties to the Russian security services posed an unacceptable risk.[78]

Although Ukrainians could access VK through virtual private networks, the ban prevented Ukrainians from accessing VK directly and dramatically decreased the network's popularity.[79] According to analysis by the data analytics firm Singularex, Ukrainian posts dropped in half as the ban was going into effect (Figure 5.1).[80] A second smaller drop in usage occurred several months later, between February and April 2018, perhaps because users lost interest in VK as the bulk of their friends migrated to other platforms.[81] After the ban went into effect, the popularity of Facebook and YouTube increased dramatically in Ukraine.[82]

However, the evidence remains mixed regarding whether the ban actually proved effective in the counter-disinformation fight. The ban clearly did reduce Russia's access to Ukrainians' personal information and likely complicated disinformation efforts, if for no other reason

---

74 Interview with a Ukrainian cyber company, Kyiv, Ukraine, March 7, 2019.

75 Interview with a Ukrainian cyber company, Kyiv, Ukraine, March 7, 2019.

76 Anton Dek, Kateryna Kononova, and Tetiana Marchenko, "The Effects of Banning the Social Network VK in Ukraine," in *Responding to Cognitive Security Challenges*, Riga, Latvia: NATO StratCom CoE, January 2019, p. 39.

77 Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019.

78 Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019.

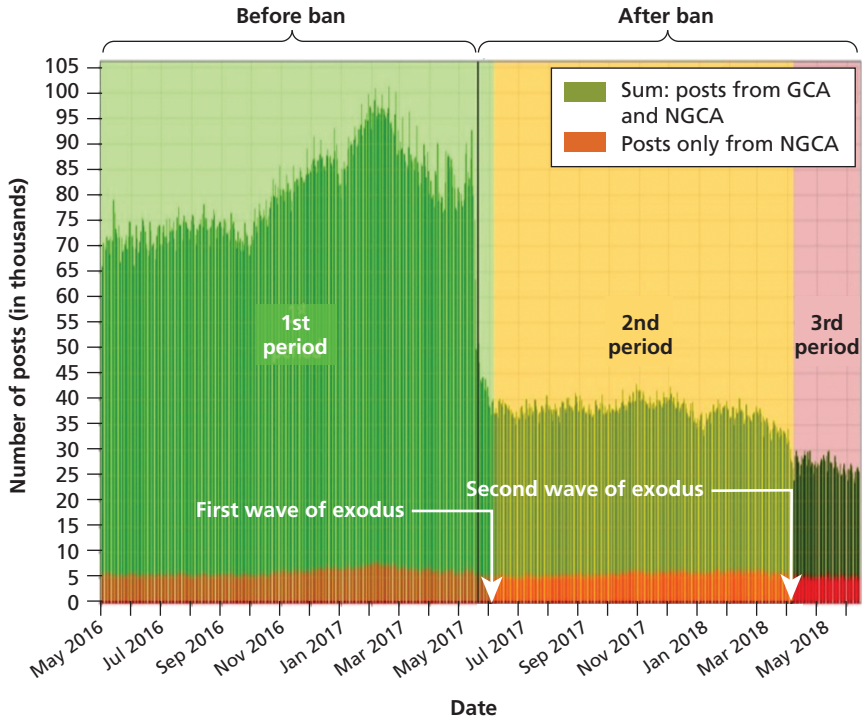
79 Interview with a data analytics firm, Kyiv, Ukraine, March 9, 2019.

80 Interview with a data analytics firm, Kyiv, Ukraine, March 9, 2019.

81 Interview with data analytics firm , Kyiv, Ukraine, March 9, 2019.

82 Dek, Kononova, and Marchenko, 2019, p. 41.

**Figure 5.1**
**Social Media Platform Users Over Time, in Millions of Users**




SOURCE: Dek, Kononova, and Marchenko, 2019, p. 43.

than the fact that Russian had to operate on American social media platforms rather than Russian ones. But there is the question of what happened to the Ukrainians who chose to stay on VK after the ban. As noted, if a user was motivated and moderately technically savvy, he or she could still use virtual private networks to circumvent the ban. Perhaps unsurprisingly, then, Singularex found that VK's remaining Ukrainian users after the ban tended to be younger (perhaps reflecting technical savviness) and more ideological.[83] The number of ideological posts increased by 1.22 times after the ban, most notably in pro-

[83] Dek, Kononova, and Marchenko, 2019, pp. 45, 57.

Russian propaganda.[84] In other words, by pushing most of the apolitical Ukrainian user base off of VK, the Ukrainian government might have made VK a more virulent (albeit smaller) platform for Russian disinformation.

### Offensive Information Efforts

Finally, aside from simply countering Russian disinformation attempts, the Ukrainian military also launched information efforts of their own to influence Russian forces and the separatists in the Donbass. Some of these efforts were relatively benign attempts to undermine the Russian narrative. For example, when the leaders of the breakaway republics Donetsk and Luhansk put out a message that the Ukrainian military was going to ban Victory Day celebrations because of its Soviet origins, the Ukrainian military along the line of contact went to mass media to show that they were allowing the celebrations to go forward.[85]

Other Ukrainian efforts could be classified as classic military deception. For example, during the Battle of Debaltseve in 2015, the Ukrainian Army held a salient against a Russian pincer move and showed mass media outlets (including Russian ones) fortifications on part of the line as part of a ruse to give the impression that certain areas were better fortified than others.[86]

The Ukrainian military also made an active effort to induce defections among separatists and Russian soldiers serving in eastern Ukraine. It broadcasted over television, radio, and (to a lesser extent) social media about the better pensions—and economic conditions—in Ukraine compared with the separatist regions and about the improvements in the Ukrainian military.[87] What impact (if any) these efforts had at inducing defections, however, remains more nebulous.

More-targeted efforts to induce defections—usually at least partially grounded in reality—proved more effective. According to one

---

[84] Dek, Kononova, and Marchenko, 2019, pp. 48, 50.

[85] Interview with midgrade Ukrainian military officers, Kyiv, Ukraine, March 7, 2019.

[86] Interview with midgrade Ukrainian military officers, Kyiv, Ukraine, March 7, 2019.

[87] Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

of our interviewees, for example, a separatist tank commander from Donetsk allegedly defected to the Ukrainian side after her actions led to the destruction of several tanks.[88] Ukraine sent messages via social media to both the commander and her children promising them that they could defect to Ukraine without retribution and warned that if she stayed she would likely be held accountable for mishap by Russian forces.[89] Ukrainian military sources offer an example of another operation in 2016, when Ukraine allegedly took out the entire 7th Brigade by using instruments atypical for wartime—direct addresses to a military prosecutor. They prepared documents, which appeared to be signed by 17 Russian soldiers serving in the brigade in the Donbas, alleging misbehavior by one of the brigade's senior officers.[90] As a result, the brigade was reportedly taken off the front for several months for the investigation. The commander, who was set to go to general staff college was instead sent to a psychological institution, demoted, and sent back to the field where he was ultimately killed. The Russians claimed that he died fighting in Dagestan, but Ukraine used the implausibility of this story to force Russia into admitting that they had active Russian military officers in Ukraine.[91] Coverage of the death in the Ukrainian press insinuates that the officer's death was orchestrated by Russia itself, but it is difficult to corroborate these claims or the existence of a Ukrainian information operations effort preceding the death.[92]

---

88 Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

89 Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

90 Ukrainian sources describe the alleged misbehavior and errors of this commander, but it is difficult to tell whether these are based on fact. See "Commander of the RF Armed Forces Bushuev Perished in the Donbass: How This Came to Pass [На Донбассе погиб полковник ВС РФ Бушуев. Как это было] " Inshe.TV, July 4, 2016.

91 Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019. A local Russian press outlet confirmed the death of the same military officer from a landmine, see "In Blagochavensk, They Say Goodbye to a Fallen Soldier [В Благовещенске Прощаются с Погибшим Военнослужащим]," Amurinfo, July 7, 2016.

92 For an example of Ukrainian press reporting on the incident, see "Bushuev, a Russian Military Colonel (aka 'Dawn') Was Killed in the Donbass [На Донбассе погиб полковник ВС РФ Бушуев «Заря»]," Trust.ua, July 4, 2016.

## Russian Disinformation in Ukraine After 2015

Thanks to Ukraine's counter-disinformation efforts and a shift in the war in the Donbas from an active conflict to a frozen one, Russian disinformation likewise has had to evolve. In general, Russian messaging returned to a softer tone, emphasizing a common Russian-Ukrainian "brotherhood" and blaming a small pro-Western faction for the conflict.[93] Russia is also allegedly pushing Ukraine to sue for peace quickly and attempting to undermine Ukrainian will and demoralize Ukrainian service members serving along the line of contact by saying that a successful outcome in the Donbass is impossible.[94]

As Ukrainians have shifted away from VK, Russia has had to change its social media approach, shifting to Facebook and YouTube (which are increasingly populated with Russian-friendly commentators producing content for the Ukrainian audiences).[95] Although conducting a disinformation campaign on either platform is comparatively more difficult than doing so on VK, these platforms do remain exploitable. For instance, there is a black market for fake Facebook accounts. Unlike accounts that were opened by bots and can be detected by automated means, these fake accounts have been groomed by individuals—sometimes for years on end—with posting seemingly natural activity to make their behavior look more credible.[96] These accounts are then sold to support criminal activity or state-based disinformation campaigns.[97] Potential buyers can also buy "likes" from these fake accounts to falsely inflate a post's popularity.[98] According to data analysts, these services are fairly cheap and readily accessible—particularly on Rus-

---

[93] Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019.

[94] Interview with former Ukrainian mid-level officers, Kyiv, Ukraine, March 9, 2019; interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

[95] Interview with a Ukrainian politician, Kyiv, Ukraine, March 5, 2019.

[96] Interview with Ukrainian law enforcement officials, Kyiv, Ukraine, March 7, 2019; interview with data analytics firm officials, Kyiv, Ukraine, March 9, 2019.

[97] Interview with Ukrainian law enforcement officials, Kyiv, Ukraine, March 7, 2019; interview with data analytics firm officials, Kyiv, Ukraine, March 9, 2019.

[98] Interview with data analytics firm, Kyiv, Ukraine, March 9, 2019.

sian language sites—because Google filters are optimized to counter such activity in English.[99]

Russia also exploited Facebook's and other non-Russian platforms' terms of service for its own counter-information campaigns, pushing the social media giants to ban certain NGOs and remove their content, claiming it represented extremist content and other prohibited speech.[100] Russia allegedly used bots to post complaints about certain Ukrainian accounts, causing Twitter to block those users.[101] Presumably, the logic is that if Russia can use the these companies' own regulations to curb pro-Ukrainian content, then Russian-neutral or perhaps pro-Russian content could fill the information void.

Russia also shifted back to more-traditional media for its disinformation campaigns. Specifically, Ukrainian politician and oligarch Viktor Medvedchuk has close ties to Putin and is suspected to have gained control over Ukraine News 1 and over Channel 112, one of Ukraine's largest television networks.[102] After Medvedchuk took over the networks, they severed ties with the U.S. Global Media Agency and U.S. Agency for International Development and adopted a more pro-Russian line.[103] Some analysts even accused Medvedchuk of being a "direct Kremlin agent" and actively pushing disinformation.[104]

In practice, Channel 112 and News 1's disinformation seems subtler than Russian disinformation during the height of the conflict. Many of the television hosts on these channels date to the pre-2014 Ukraine period and, according to some more-nationalist Ukrainians, harbor stronger pro-Russian views.[105] These channels also intersperse

---

[99] Interview with data analytics firm , Kyiv, Ukraine, March 9, 2019.

[100] Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019.

[101] Giles, 2016.

[102] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019; interview with Ukraine media experts, Kyiv, Ukraine, March 7, 2019.

[103] Interview with Ukraine media experts, Kyiv, Ukraine, March 7, 2019.

[104] Interview with Ukraine media experts, Kyiv, Ukraine, March 7, 2019. For criticism of the channels, see Anastasiia Grynko, "Fake Narratives in Times of Presidential Elections: How Hybrid War Reshapes the Agenda of Ukrainian TV," StopFake, February 21, 2019.

[105] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019.

news and opinion segments, bringing on Ukrainian so-called experts who are portrayed as buffoons next to their more-sophisticated pro-Russian counterparts.[106] Both channels received multiple warnings from Ukrainian regulators for potentially violating Ukrainian laws about advancing Russian interests through these practices.[107] The suspicion is that Russia might be targeting older Ukrainians who still get most of their news through traditional media (rather than social media) and who tend to vote more than younger audiences.[108]

Russia is also suspected of backing agents of influence, particularly supporting Ukraine's far-right political parties.[109] Media analysts note that every time there is a far-right protest or rally, Russian news cameras show up; they say this is an effort to paint Ukraine as fascist.[110] The Ukrainian government accuses the Russians, more nefariously, of planting a story in September 2018 about the supposed murder of an ethnic Ukrainian by ethnic Hungarians in Zakarpattia in Western Ukraine and then using the story to stir up far-right Ukrainian sentiments by spreading inflammatory messages on social media.[111]

The Ukrainian arms industry says Russia has also targeted it. Members of the industry allege that Russia routinely and falsely claims that Ukraine is incapable of maintaining and building Soviet-designed

---

[106] Interview with a Ukrainian journalist, Kyiv, Ukraine, March 5, 2019.

[107] Interview with a Ukrainian journalist, Kyiv, Ukraine, March 5, 2019; Interfax Ukraine, "Parubiy Signs Resolution on Sanctions Against 112 Ukraine, NewsOne Channels," *Kyiv Post*, October 20, 2018.

[108] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019.

[109] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019. For general context and an overview of Russia developing ties with political parties, particularly from the far right, see Raphael S. Cohen and Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat*, Santa Monica, Calif.: RAND Corporation, RR-1793-A, 2019.

[110] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019.

[111] Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019. Although this specific allegation cannot be independently verified, this border region has routinely been a flashpoint in Ukrainian-Hungarian tensions, including during this period. For example, see "Hungary Protests Ukrainian Military Moves, 'Death List' of Dual Citizens," Radio Free Europe/Radio Liberty, October 11, 2018; "Police Open Criminal Case over Provocative Anti-Hungarian Billboards in Zakarpattia Region," *Unian*, October 22, 2018.

equipment and trots out lists of so-called experts to attest to this fact.[112] Russia further alleges that the Ukrainian arms industry is corrupt and a pawn of the United States.[113] However, some Russian claims about the industry can be chalked up to normal competition among business rivals and multiple states (including the United States)—and other outside investigations have cited problems in the Ukrainian industry. In light of this, it is hard to determine whether Russian messaging in this regard constitutes disinformation.[114]

Finally, Russia continued targeting the Ukrainian military, albeit to a lesser extent. In November 2018, a Russian member of parliament made a public statement on traditional media that Ukraine would provoke an altercation on the Black Sea.[115] Russia seized Ukrainian patrol boats passing through Kerch Strait a few days later, and Ukraine declared martial law.[116] The real-world incident provoked a series of targeted disinformation campaigns. Reservists received false text messages saying they were being mobilized.[117] Troops reported receiving targeted text messages claiming that their family members would be kidnapped.[118] Locals in the Sumy region of Ukraine—near the Russian border—reported receiving text messages that they were falsely being drafted into the military.[119] Although Russia reserves these text

---

[112] Interview with defense industry experts, Kyiv, Ukraine, March 6, 2019.

[113] Interview with defense industry experts, Kyiv, Ukraine, March 6, 2019.

[114] For example, see Marie Yovanovitch, "Remarks by Ambassador Yovanovitch on the Occasion of the 5th Anniversary of the Ukraine Crisis Media Center's Founding," U.S. Embassy Kyiv, Ukraine, March 5, 2019; Olga Oliker, Lynn E. Davis, Keith Crane, Andrew Radin, Celeste Gventer, Susanne Sondergaard, James T. Quinlivan, Stephan B. Seabrook, Jacopo Bellasio, Bryan Frederick, Andriy Bega, and Jakub P. Hlavka *Security Sector Reform in Ukraine*, Santa Monica, Calif.: RAND Corporation, RR-1475-1-UIA, 2016.

[115] Interview with a think tank analyst, Kyiv, Ukraine, March 5, 2019.

[116] "Russia-Ukraine Tensions Rise After Kerch Strait Ship Capture," BBC, November 26, 2018.

[117] Interview with Ukraine media experts, Kyiv, Ukraine, March 7, 2019.

[118] Interview with Ukraine media experts, Kyiv, Ukraine, March 7, 2019.

[119] Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019.

message disinformation barrages for crises, Ukrainian experts agree that these efforts have grown more sophisticated as of late.[120]

## Lessons Learned

In many ways, Ukraine is a best-case scenario for Russian disinformation. Russia knows Ukraine better and is far more intimately connected to Ukrainian culture, history, and politics than to most other countries. Consequently, Russia might not be able to replicate in another context all of the tactics that it employed in Ukraine. Nonetheless, Ukraine as a case study provides several important insights regarding Russian disinformation tactics on the operational level and illuminates some best practices that USAF and the joint force should consider if the need arises to respond to such activities in the future.

### Social Media: One Instrument in a Larger Toolkit

In Ukraine, Russian disinformation campaigns worked through several different media—social media, text messages, agents of influence, and traditional media. When Russia encountered an obstacle in one medium (such as the ban on VK), it simply shifted to another (traditional media). In this sense, Russia proved remarkably versatile in adapting its tactics. Russia also showed that it could coordinate disinformation with other tools of power. Perhaps this is best seen in how Russia used disinformation to enable its efforts to geolocate troop formations in the Donbass and target them through artillery strikes. These examples demonstrate that disinformation might not be a separate realm in the context of conflict; rather, it is integrated into conventional military operations.

### Troops and Their Families at Risk

Whether sending fake text messages to soldiers' family members or infiltrating veterans' groups, Russia's operations in Ukraine show that it singles out current and former service members and their families for

[120] Interview with Ukrainian security officials, Kyiv, Ukraine, March 6, 2019.

disinformation efforts. As discussed in the previous chapters, Russia has also targeted U.S. service members and their families. Consequently, any response conducted by USAF and the joint force needs to look at the entire military community—not just deployed service members.

### Positive and Negative Aspects of Bans

In terms of possible responses, Ukraine's experiences show that more-active measures to counter disinformation by banning mobile phone use by soldiers (or even more-draconian policies, such as banning entire social networks) produce mixed results. Forbidding service members to use mobile phones comes at a cost to troop morale (at the very least) and requires significant amounts of discipline to enforce, raising questions of whether such a policy would be practical, even in highly professional militaries, such as that of the United States. Banning entire social networks also presents significant downsides—even leaving aside free-speech concerns—as shown in Ukraine by the increased concentration of pro-Russian political sentiment on VK and the shifting of Russian information efforts to more widely available traditional media after the ban.

### Message Discipline, Openness, and Transparency

On a more positive front, Ukraine's response shows how efforts to combat disinformation start with limiting misinformation. Although proving its effectiveness remains difficult, Ukraine's One Voice Policy at least minimized Russia's opportunities to exploit the Ukrainian government's confusion. This is an important accomplishment because Russia often based its disinformation on partial facts to lend credibility to its narrative. Russia's disinformation efforts in Ukraine also showed the downsides to secrecy; Russian disinformation would often fill the voids left—deliberately or accidently—by the Ukrainian government and military. For USAF and the joint force, both lessons are relevant: Getting one narrative out in the public early and generally being as transparent as possible are strong and required first steps in fighting any sort of Russian disinformation efforts.

### Civil Society's Role

Finally, the Ukraine case study reflects how combating disinformation is not simply a whole-of-government concept but rather a whole-of-society fight. Ukraine experience shows that the nongovernmental sectors might in some cases be better prepared to fight disinformation than the government organizations. There a wealth of talent resident in the private sector (e.g., journalists, sociologists); in addition, fact-checking from an outside independent source, such as StopFake, might be considered more credible than material coming from the military or the government. Particularly because Russia and other states also might try to pressure social media companies like they did in Ukraine, NGOs might have more sway with technology companies.[121]

---

[121] See Cohen et al., 2021.

CHAPTER SIX

# Conclusion and Recommendations

USAF has a long history of countering Russian information operations against the United States and its allies. During the Berlin Airlift in 1948, for instance, USAF flew in 13 tons of newsprint daily to combat Soviet propaganda in West Berlin.[1] In this chapter, we identify ways that USAF and the joint force could update the approaches to countering disinformation and propaganda for the social media age. We base our recommendations on the lessons derived from Russia's social media–based information operations, U.S. and other Western countries' responses to Russian information operations, and Russia's vulnerabilities. Our recommendations are also informed by the likely future course of Russia's information activities, which we discuss first.

## The Future of Russia's Social Media Campaigns

Russia can be expected to continue pursuing most of the same goals and targets it has in the past, although new targets and objectives also might appear. As the U.S. intelligence community's 2019 Worldwide Threat Assessment forecasts,

> Russia's social media efforts will continue to focus on aggravating social and racial tensions, undermining trust in authorities, and criticizing perceived anti-Russia politicians. Moscow may employ

[1] Daniel F. Harrington, *Berlin on the Brink: The Blockade, the Airlift, and the Early Cold War*, Lexington, Ky.: University Press of Kentucky, 2012, p. 112.

> additional influence toolkits—such as spreading disinformation, conducting hack-and-leak operations, or manipulating data—in a more targeted fashion to influence U.S. policy, actions, and elections.[2]

Continuity of effort is not limited to Russia's activity aimed at the United States. More recently, Russian Chief of the General Staff General Valeriy Gerasimov reaffirmed Russia's need to maintain information weapons, such as those deployed in Ukraine and Syria, to face modern adversaries.[3]

To meet Russia's social media–based threat, U.S. parties must keep in mind that Russian activity will involve more-sophisticated tactics and techniques even if the goals and targets do not change dramatically.[4] Russian actors should be expected to adapt to Western countermeasures and assimilate more-advanced technology.

On the technological front, the United States should expect more-sophisticated phishing and cyberattacks. Malware associated with Russian intelligence has grown more sophisticated and could be used to gain and exploit information for future campaigns similar to the hack-and-leak scheme used in 2016. For example, Zebrocy malware (a tool used by the GRU's Fancy Bear hackers), rapidly increased its sophistication in the intervening years.[5] That malware was used to target a wide variety of NATO, Central Asian, and other international targets from 2016 to 2019, including an extensive campaign to exploit interest in Brexit as a means of infecting targeted networks.[6] A prominent U.S.-

---

[2] Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community*, Washington, D.C.: Office of the Director of National Intelligence, January 29, 2019.

[3] Andrew E. Kramer, "Russian General Pitches 'Information Operations as a Form of War," *New York Times*, March 2, 2019.

[4] For example, see the prognosis by Lithuania's president, Dalia Grybauskaite: "What we see is a steadily growing pressure on cyber, the information front, propaganda and, recently, fake news . . . [t]heir efforts and instruments are becoming more sophisticated every day" (Barnes, 2018).

[5] "Russian Nation-State Hacking Unit's Tools Get More Fancy," Oodaloop, May 24, 2019.

[6] Charlie Osborne, "Fancy Bear Exploits Brexit to Target Government Groups with Zebrocy Trojan," Zero Day, December 14, 2018.

based cybersecurity firm found that state-sponsored Russian hackers could breach networks "eight times as fast" as the next best adversary, North Korea; the firm's senior Russia investigator concluded that "Russia is really the best adversary."[7] State-sponsored organizations also could increasingly look to freelance malware to develop fresher attacks. A senior researcher at another U.S.-based cybersecurity firm claimed that APT29, which was implicated in 2016 election-meddling, could be moving to off-the-shelf exploits despite the group's traditional use of custom malware.[8]

The United States should also expect greater exploitation of big data and AI tools. Social media companies have an immense amount of information available about individuals, and the potential for third parties—Russia emphatically included—to harvest and abuse that data it is already in evidence.[9] The techniques for (legal and illegal) data-harvesting and data privacy protections are still evolving. Although much depends on the development of legal mandates and of technical safeguards that social media companies can put in place to prevent data-harvesting, further deployment of data-harvesting capabilities increases the possibility of precise microtargeting of content.

Information warfare experts also forecast the increasing use of *deepfakes*, or highly realistic digital manipulations of audio or video.[10] The exploitation of this technology presents an immediate challenge

---

[7] Andy Greenberg, "Russian Hackers Go From Foothold to Full-On Breach in 19 Minutes," *Wired*, February 19, 2019a.

[8] Lily Hay Newman, "Russia's Elite Hackers May Have New Phishing Tricks," *Wired*, November 20, 2018. APT29 is most likely used by Russia's SVR. See Sean Gallagher, "Candid Camera: Dutch Hacked Russians Hacking DNC, Including Security Cameras," Ars Technica, January 26, 2018.

[9] For example, see Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," *New York Times*, April 4, 2018.

[10] Robert Chesney and Danielle K. Citron, *Disinformation on Steroids: The Threat of Deep Fakes*, New York: Council on Foreign Affairs, October 16, 2018; Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics," *Foreign Affairs*, January/February 2019; Nic Dias, *The Big Question: How Will 'Deepfakes' and Emerging Technology Transform Disinformation?* Washington, D.C.: National Endowment for Democracy, 2018; Donie O'Sullivan, "When Seeing Is No Longer Believing: Inside the Pentagon's Race Against Deepfake Videos," CNN, January 28, 2019.

for detection and debunking. The capabilities to detect deepfakes will also evolve; however, for a time at least, a considerable lag will exist between the launch of a fake and its debunking—and that lag can be weaponized easily. A well-timed piece of deepfake disinformation—for instance, accusations against a candidate for political office on the eve of an election, or a scandal pertaining to NATO troops right before a major exercise or actual military operation—can affect behaviors of a sufficiently large number of people to alter outcomes on the ground. Similarly, a deepfake impersonation of a U.S. or allied leader to spread false and alarming content might set off panic before it can be debunked effectively.

Conversely, some adaptations that the United States should expect do not rely on fancy technology. Instead, they consist of simpler ways to evade countermeasures, such as blocked accounts. As Keir Giles warned in 2016,

> [a] process of building up of capabilities on social media is visible, in particular in the form of accumulation of trusted social media accounts with large networks and numbers of followers. These accounts are at the present moment not used for any overtly hostile process, but engaged in establishing their credibility, and developing tactics for defeating analytical methods used to identify false personae. In particular these tactics include tailored and sophisticated features which generate followers and interaction from genuine accounts.[11]

Giles' insight proved accurate, and Russian actors have taken measures to circumvent basic detection measures and triggers for blocked accounts. For example, when Facebook took IRA's Black Matters page offline, its IRA operators simply started a new page called BM. That page behaved in ways that incorporated adaptations to countermeasures:

> [It] employed a new audience-building strategy around more positive themes of black affirmation and black beauty, seemingly to

[11] Giles, 2016, p. 70.

> avoid further detection and suspension . . . [U]nlike the older Black Matters, the BM page was keen to redirect traffic to the associated website and its new 'Meet Up' feature rather than to keep its audience engaged on the Facebook platform where its efforts had previously been detected and suspended. It is also after this initial suspension on Facebook that the IRA turned to Google Ads to promote the associated Black Matters U.S. website, with ads leveraging text, image, and video formats.[12]

Further adaptations of this sort are to be expected, among them probably an increased reliance on preexisting local persons—i.e., freelancers unaffiliated with the state who have demonstrated a long history of independent online existence. Government actors and NGO analysts in the former Soviet space indicate this appears to already be afoot. The Security Service of Ukraine, for example, reported a confession by a Russian agent that Russia tried "to circumvent Facebook's new safeguards by paying Ukrainian citizens to give a Russian agent access to their personal pages" in advance of the 2019 presidential elections.[13] A Belarusian NGO reported that prominent "bloggers and social media public group owners began receiving offers to write articles expressing given opinions for money, post advertisements or sell their passwords," and "[a]t least in one case the customer said he represented Sputnik."[14] "Journalist Nina Jankowicz likewise reports that, on the basis of recent field work in Ukraine, Georgia, and Belarus, "disinformation moves 'underground' and becomes harder to track and debunk on a case-by-case basis."[15]

---

[12] Howard et al., 2018, p. 10. The final touch to this tactic was that "[f]ollowing the initial suspension of the Black Matters Facebook page, the IRA also leveraged the Black Matter US Twitter account to complain about its suspension on the platform and to accuse Facebook of 'supporting white supremacy.'"

[13] Michael Shwirtz and Sheera Frenkel, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering," *New York Times*, March 29, 2019.

[14] International Strategic Action Network for Security (iSANS), presentation at RAND Corporation, Washington, D.C., April 23, 2019.

[15] Private Facebook groups and encrypted messengers; interview with Belarus experts, Washington, D.C., June 19, 2019; Jankowicz, 2019.

## Recommendations

The recommendations we present are those that we believe to be most relevant to the Air Force Special Operations Command (AFSOC) and the joint force.[16] Broader policy implications for the U.S. government as a whole are largely outside the scope of this study (except recommendations that pertain to USAF and DoD) and are addressed in a companion report.[17]

### Recommendation 1: AFSOC Should Be Mindful of Russia's Perceptions When Deploying Assets

AFSOC should be especially careful in areas that Russia perceives to be of strategic importance or interest. As we suggest in Chapters Two and Three, Russian defense analysts pay very close attention to U.S. capabilities and assets that might be used to conduct information or psychological operations, at times exaggerating their effects and U.S. intentions. The deployment of Commando-Solo, for example, was understood by some Russian experts as a way of eroding the adversary's will to fight—and was viewed as a very effective tool in some contexts. Therefore, AFSOC should carefully assess how the deployment of this or other military information support operations (MISO) or PSYOPS assets might be viewed by Russian observers—especially if deployed in areas that Russia views to be of strategic importance, such as the former Soviet republics or conflicts in which Russia is taking part. Were such a deployment to occur simultaneously with movements of conventional NATO or U.S. forces in the same or neighboring regions, the effect could have an unintended escalatory impact on Russia's military and security services. This is not to say that NATO or U.S. PSYOPS capabilities should never be forward-deployed to Europe—only to suggest that such maneuvers could have an outsize impact on the Russian audience.

---

[16] These recommendations articulate what we conclude are best practices and are not intended to identify AFSOC, USAF, or DoD capability gaps.

[17] Cohen et al., 2021.

### Recommendation 2: The Joint Force Should Adopt Appropriate Monitoring Processes to Improve Detection of Russian Information Operations

The joint force should focus special attention on operations of greatest concern to DoD (e.g., those that target members of the U.S. military and its associates or U.S. and NATO operations). Monitoring of social media must extend beyond Facebook and Twitter. As our overview of Russian social media operations shows, Russians are active across a gamut of online fora. Smaller platforms (e.g., Reddit, Instagram) and non–U.S.-based platforms (e.g., VK) are often more important. As suggested in our Ukraine case study, when Russian actors get pushed out of some social media platforms, they will emerge on others. Furthermore, as we show in Chapter Three, Russian-operated accounts do not behave uniformly but instead adopt a variety of deceptive identities. Monitoring processes should be responsive to the need to detect the variety of tactics and techniques that Russian actors are using on social media.

The joint force might further consider tasking MISO specialists to perform a sort of secondary analysis of Russian information operations to identify and assess the source, content, audience, media, and effect (SCAME analysis) of such operations.[18] At the operational level, these specialists can better discern an adversary's propaganda objectives, propaganda dissemination cycles, and product lines to help determine how to undermine adversarial messaging—including an ability to conduct joint analysis of publicly available information with NATO partners.[19] Evaluations of Russian activity on social media by U.S. and NATO MISO-practitioners can help identify key trends related to campaigns targeting service members and their associates.

---

[18] For more information on SCAME analysis, see Department of the Army, "Appendix D: Propaganda Assessment," *Tactical Psychological Operations Tactics, Techniques, and Procedures*, Field Manual 3-05.302 MCRP 3-40.6B, October 2005.

[19] Amy Sexhauer, Victor Mckenzie, Shari Smith, and Philip Kautz, "Optimizing Indirect MISO: MIST-Iraq and Advising at the Operational Level of War," *Special Warfare*, January–March 2018, p. 32.

### Recommendation 3: The Joint Force Should Take Measures to Reduce Overattribution in Its Detection Methods

Monitoring processes should accommodate a thorough approach to attribution and guard against overattribution. Russia's narratives and messaging resonate with many audiences across the West, and many voices independently echo the Kremlin's talking points. This means that algorithms that merely pick up bots, pro-Russian content, or both on social media are liable to overattribute. More-thorough methods are needed, and—at least at present—this is likely to require human participation to heed contextual clues, such as the rules of thumb offered by DRFLab to distinguish Russian trolls from other trolls.[20] Attribution methods will also have to keep pace with the evolution of Russian social media activity. This is admittedly not an easy task with simple solutions. Nonetheless, continuous efforts to improve attribution are necessary; pointing the finger at Russia in every instance of activity on social media resembling Russian interference distorts the understanding of the threat.

### Recommendation 4: USAF and the Joint Force Should Train Troops and Their Family Members to Recognize Disinformation

The training and education of U.S. service members on how to recognize disinformation and other information manipulation by Russian actors should be a top and ongoing priority. Training should extend to the family members of service members, considering Russia's track record of targeting this population. Training should familiarize service members with likely themes, targets, and target audiences of Russian information efforts as presented in Chapter Three. This training should emphasize predictable and common themes of Russian information campaigns relevant to the military, such as disinformation maligning NATO and the Syrian opposition and exploitation of social divisions pertaining to the U.S. treatment of its veterans and the U.S. use of force abroad. Training also should provide an overview of Russian themes that are salient in European countries, especially for service members deploying to the European area of responsibility.

---

[20] DFRLab, "#TrollTracker: How to Spot Russian Trolls," *Medium*, March 29, 2018b.

Importantly, training should also emphasize the sheer variety of forms Russian efforts take, appearing across social media platforms and in various disguises. That is, service members should be instructed in vigilance not only with regard to obvious trolls on Facebook or Twitter, but to the variety of accounts across every conceivable social media platform that appear real, including trusted or even personally known sources that might have been hacked or coopted.

Awareness training might be provided at several logical points: for example, it might be included in regular family day briefs and provided to service members and their families deploying to Europe or other areas that have been targeted by Russian espionage or information operations. Training should also go beyond instruction or briefings: Plausible disinformation scenarios can and should be incorporated into military exercises.

### Recommendation 5: USAF and the Joint Force Should Develop Policies Regarding Use of Social Media Platforms and Mobile Devices

As demonstrated in our discussion of the Ukrainian case study (as well as by other experiences, such as the NATO exercise discussed in Chapter Four), mobile phones and unrestrained social media use create a vulnerability, exposing individuals not only to geotracking but also microtargeting. Broad measures, such as banning devices or forbidding the use of social media across the board, are not likely to be effective: Apart from imposing burdensome restrictions on U.S. service members, experience shows that Russian actors adapt to bans and identify alternative channels for information warfare. By contrast, narrowly tailored restrictions, such as limits on the kind of information that might be shared on social media, might not be unreasonable.

Importantly, any restrictions should be accompanied by education and further training about Russia's exploitation of personal information posted on social media. Such training should demonstrate how even modest amounts of personal data can be exploited to manipulate perceptions and behavior. Even if USAF or DoD does not restrict what might be shared on social media, service members and their families should be aware that any such information can be exploited for microtargeting and/or hacking. Arranging for experiments similar to the

NATO exercise described in Chapter Four, which demonstrates concretely how social media information can be exploited, might provide a more compelling demonstration than pure instruction.

### Recommendation 6: USAF and the Joint Force Should Train and Educate Top Officials About Salient Risks Stemming from Hacking and Leaking Information

Considering prior attacks (such as Breedlove's hacked email and the interception of the Nuland-Pyatt phone call, both discussed in Chapter Three), persistence in targeting the military, and the increasing sophistication of Russia's technical spearfishing and cyberattack capabilities, it is important to protect against likely attacks against high-profile individuals. Information stolen from high-level officials offers the most cache to information warriors in terms of its potential to spread and influence perceptions. Efforts should be made to go beyond general cybersecurity training and to educate and train these officials to minimize the existence of exploitable information. Although no one can abstain altogether from using mobile phones or internet-based communications, top officials should be encouraged to minimize substantive communications through such channels. This will not prevent hack-and-leak information operations, nor will it completely erase the potential for adverse consequences—content has been previously manufactured by the attackers, and the same can be done again. However, offering little in the way of substantive content to leak does lessen the potential damage by depriving attackers' access to actual—and usually more plausible—information. Actual information—such as the transcript of the phone conversation between Nuland and Pyatt—can be embarrassing to the United States and exploited to buttress Russian narratives about U.S. intentions.[21] By contrast, false information might at times limit the resonance and impact of leaked materials—as appeared to be the case when Emmanuel Macron's campaign inten-

[21] For example, see Doina Chiacu, and Arshad Mohammed, "Leaked Audio Reveals Embarrassing U.S. Exchange on Ukraine, EU," Reuters, February 6, 2014.

tionally used *cyber-blurring*, or injecting clearly false information in anticipation of a hack-and-leak.[22]

### Recommendation 7: USAF and the Joint Force Should Foster Institutional Capacity for Disseminating Counternarratives and Debunking Disinformation

Debunking on its own is unlikely to persuade social media users of the falsity of particular content, but this action remains important to maintaining the capacity to set the record straight for content that implicates USAF or DoD—at least for those audiences who might have an interest in seeking out truthful information. NATO's efforts to counter an onslaught of Russian disinformation and propaganda is one example. Although Russia often targets audiences already susceptible to its messaging, that is not always the case. For example, Russia might launch a disinformation campaign about a military exercise and aim it at audiences residing near the exercise site, or communities hosting U.S. forces. Official and authoritative social media channels are useful in general, but they are especially so in these cases, when they can be used to reach the targeted audiences with corrections of the record. Building a more active social media presence generally would help USAF and the joint force reach such audiences.

Countermessaging to counter specific pieces of disinformation is most effective when it is consistent; in this respect, USAF and the joint force face the difficulty of harmonizing their approach with any parallel efforts by NATO, the EU, and any individual states that might be targeted by Russian disinformation or propaganda. It is likely that the optimal approach involves some actor other than the U.S. military taking the lead in countering specific kinds of disinformation; if so, USAF and the joint force social media presence should reproduce the countermessage to give it broader publicity. Who should take the lead on countermessaging, however, would have to be worked out collab-

[22] This was done intentionally by Macron's presidential campaign in anticipation of the attack, which experts cite as a contributing factor to Russia's failure in its campaign to undermine Macron's candidacy. See Vilmer, 2019.

oratively with NATO and the EU—and ongoing coordination would likely be necessary.

### Recommendation 8: USAF and the Joint Force Should Maintain Clear, Consistent Public Messaging

As past RAND research points out, it is impossible to make after-the-fact corrections to all disinformation pertaining to U.S. and allied militaries authored by Russian actors.[23] It is thus important to get ahead of the disinformation pertaining to ongoing U.S. and allied activity and matters of public controversy implicating the U.S. and allied militaries and to tell the U.S.–allied story proactively: Clear and compelling narratives should reduce the resonance of Russia's disinformation. As the Ukrainian case study shows, secrecy and confused public messaging create fertile ground for hostile disinformation. Clarity and consistency of communications directed at U.S. troops and other audiences might reduce audience susceptibility to disinformation. Implementing this recommendation requires balancing the need for secrecy with closing vulnerabilities to disinformation, but the latter consideration should not be underestimated. An active social media presence, beyond enabling debunking of disinformation, could also enable a steady communication of positive narratives.

### Recommendation 9: USAF and the Joint Force Should Work Through NGOs to Debunk Disinformation

Although USAF and the joint force should build up their own social media capabilities to debunk disinformation pertaining to their own activities, it is advisable to rely on NGOs to do so in other contexts. As Ukraine's experience shows, NGO actors are often better equipped to accurately debunk disinformation and propaganda and to disseminate that information. NGOs' superior familiarity with local settings could enable them to act more expediently and reach broader audiences than might be accomplished by similar efforts by the U.S. military.

Moreover, civil society groups have a likely advantage over state actors—as well as over professional media organizations—in their

[23] Helmus et al., 2018, p. 88.

potential to present credible, nonstate, transparent adjudications of what is fact and what is false. Especially in the context of U.S. culture surrounding speech and the boundaries on government action in this realm, there is a widely held belief that organs of the state should refrain from directly adjudicating truths and untruths.

## Final Thoughts

For several reasons, the recommendations we identify concentrate on countermeasures aimed at awareness-raising and at the consumption stage. Most of the countermeasures aimed at limiting distribution tend to be within the purview of social media companies and subject to potential legal regulation in the future. Measures aimed at preventing production call for policy decisions at the U.S. government level (e.g., sanctions), or their efficacy is largely speculative. Among the latter group are deterrence measures aimed at individual Russian actors, which we identified as potential opportunities for exploitation in Chapter Six. Although there is reason to explore these opportunities, little evidence exists at the moment about the effects of such measures. Considering Russia's prior escalatory behaviors in response to the Western impositions of costs (such as sanctions), these actions need to be carefully assessed.

APPENDIX

# Russian Vulnerabilities to Social Media–Based Information Operations

As we observed in Chapter Two, Russia's approach to social media is, to a significant extent, a product of its own anxieties about the potential effects of the internet and social media. In this appendix, we address the nature of these anxieties in greater detail and identify several of Russia's vulnerabilities that underlie these anxieties. Moscow harbors two main sources of anxiety—the potential of social media to empower domestic opposition and the potential of social media to be exploited by Russia's adversaries to demoralize or gain advantages over its armed forces. Although some of these anxieties are exaggerated, underlying perception of the regime's vulnerability to information flow through social media is not without cause. Neither are those anxieties pertaining to the vulnerability of the military to psychological influence through social media. These vulnerabilities could hypothetically be exploited to encourage dissent and division, but there are multiple reasons to be cautious in this regard. Some vulnerabilities present opportunities for offensive action that carry fewer risks: Targeting individual actors within Russia's information confrontation machinery with tailored messaging, in particular, might present a relatively low-cost, low-risk deterrence measures.

## Anxieties about Social Media–Based Information Operations

The Putin regime has deep-seated anxieties about the internet generally and social media in particular. As we have noted, Russia's anxieties

received a considerable boost from the Arab Spring and the 2011–2012 protests in Moscow, which military thinkers and Russian political leaders attribute, at least in part, to psychological operations organized by the West with the use of social media.[1] The rise of social media against the backdrop of rising tensions with the West further fueled anxieties pertaining to regime destabilization and the exploitation of social media to demoralize or gain advantages over its armed forces.

The first source of anxiety resides in the potential of social media to empower domestic opposition—and to facilitate foreign meddling to stoke that opposition. The internet has been used as a forum for opposition figures in Russia, and social media has furnished a potential solution to the collective action problem that regime opponents worldwide face. In Russia's view, social media enables Western powers to meddle in the politics of other countries. Even prior to the rise of social media, many among Russia's elite viewed "transnational media"—along with support for civil society and democracy promotion—as one vector of influence whereby the West affected the popular psyche, eroding patriotism and nationalism.[2] It is thus unsurprising that social media would be seen in the same light—i.e., yet another vector the West could use in seeking to undermine Russia's regime.

The Russian state's desire to control—or at least comprehensively surveil—these new forms of communications predates Putin, and its roots lie in the Soviet era.[3] Nonetheless, the Russian government has tolerated a relatively uncontrolled internet—especially in contrast with traditional media—until relatively recently.[4] However, since Putin's reelection in 2012—and especially since the Maidan revolution in Ukraine—Russia has adopted a series of measures aimed at seizing greater control over the virtual domain. As a recent RAND report

---

1 Sivkov, 2014, p. 2; Nesmeyanov, 2017, p. 7.

2 For example, see Mikryukov, 2016; and Makarenko, 2017, p. 434.

3 See Soldatov and Borogan, 2015.

4 James Dobbins, Raphael S. Cohen, Nathan Chandler, Bryan Frederick, Paul DeLuca, Edward Geist, Forrest E. Morgan, Howard J. Shatz, and Brent Williams. *Extending Russia: Competing from Advantageous Ground*, Santa Monica, Calif.: RAND Corporation, RR-3063-A, 2019; Reynolds, 2016, p. 23.

observes, "[o]nce the importance of the internet to Russian domestic discourse became apparent, the Russian government began subjecting key firms to similar mechanisms of formal and informal control as more traditional media."[5]

The series of measures adopted since 2014 include the Blogger Registration Law, which requires bloggers with more than 3,000 followers to register as a media outlet and allows the government to access users' information. To allow this access, online information must be stored on Russian servers. Another law gives the government the right to block any website without explanation; this law was used to block the sites of key opposition figures and opposition websites during the annexation of Crimea. Yet another law requires internet service providers that handle Russian customer data, including Facebook and Twitter, to physically keep their servers on Russian soil.[6]

The Russian government moved to acquire more direct control over native social media by replacing the head of VK, Pavel Durov, with Putin loyalist Alisher Usmanov. Russia has also exploited social media rules to block pro-Ukrainian groups and content: For example, "Twitter has received multiple requests from Russian governmental agencies to remove content and close accounts"—notably, "1,735 such requests were submitted in the second half of 2015—a twenty-five-fold increase compared with other periods."[7] Newer and smaller social media platforms also did not escape official attention: The FSB went after the encrypted messaging app Telegram (founded by the same Pavel Durov who was pushed out of VK) seeking the ability to access user information, which authorities claimed was necessary to fight extremism and terrorism.[8] Telegram resisted demands to hand the state access to its users, which infamously led the FSB to an unsuccessful attempt to take

---

5 Dobbins et al., 2019.

6 For a discussion of these laws, see Reynolds, 2016, p. 23.

7 Reynolds, 2016, p. 24.

8 Lysenko, Yakov, "Terrorists Used Telegram [Террористы использовали Telegram]," Gazeta.Ru, April 27, 2018.

the platform offline by blocking IP addresses—disrupting many internet services in the process.[9]

In 2019, Russia adopted a fake-news law, penalizing the distribution of fake news by websites and individuals and requiring immediate removal of such material.[10] Individual violators can be fined, and websites can be blocked—handing yet another pretext to the government to interfere with the flow of information that it finds problematic. Russia's media regulator, Roskomnadzor, has claimed that it will set up a public registry of fake-news sources.[11] The rapid accretion of these measures is a testament to the gravity of Russia's growing anxieties about social media and the internet. "These occurrences," conclude experts at the NATO StratCom CoE, "are representative of the Kremlin's fear that it is losing control of the information environment."[12] It has been sometimes remarked among Russia watchers that Putin wants nothing so much as to cancel the internet. This is more than a joke, it turns out: Some officials reportedly raised the possibility of "creating a 'kill switch' that could isolate Russian citizens from the global internet at a moment's notice."[13]

The second, more specific source of Russia's anxieties is the prospect that social media will be exploited by adversaries to demoralize or gain advantages over its armed forces. Russian defense elites have harbored profound anxieties about Western PSYOPS targeting its own ranks even prior to the rise of social media. Russians ascribe much power to PSYOPS generally: The "consequences of information-psychological operations can lead to a significant reduction in the combat capability

---

[9] Lysenko, 2018. For more on the uses of Telegram in Russia, see Ol'ga Churakova, Elena Mukhametshina, Elizaveta Ser'gina, and Ekaterina Bryzgalova, "Channels on Telegram Have Become the New Market for Political Advertisement [Каналы в Telegram стали новым рынком политической рекламы]," *Vedomosti* [*Ведомости*], September 27, 2017.

[10] Mikhail Zelensky, "Russia Will Soon Require Digital Journalists to Delete 'Fake News' 'Instantly.' Here's What That Actually Means," *Meduza*, March 6, 2019.

[11] "Roskomnadzor Will Create a Public Registry of Fake-News Sources [Роскомнадзор создаст публичный реестр источников фейк-ньюс]," TASS, May 15, 2019.

[12] Reynolds, 2016, p. 24.

[13] Dobbins et al., 2019, pp. 157–158.

of units, and in some cases—to its complete loss," according to military authors writing for the journal *Military Thought*.[14] Russian military commentator and retired Colonel Victor Baranets, for example, points specifically to Western propaganda as a threat: "The army is becoming a serious trump card in the hands of a certain liberal community . . . to say nothing of the fact that Western propaganda attempts to brainwash our service members through all kinds of stratagems, to sow doubt in the rightness of our government's political course."[15]

Russia's anxieties about Western PSYOPS against the military are combined with anxieties about Western technological superiority. Perceived NATO innovations in information operations through advancements in communications technology and organizational changes probably aroused fears among at least some Russian defense experts as early as the 1990s. For instance, a Russian author in 1999 expressed the belief that NATO sought to contest the information space through new technology, such as the Commando-Solo airborne television and radio broadcasting platform, adding that this form of conflict presented a dire threat to Russia's security.[16] An information confrontation textbook published by a Russian electronic warfare officer in 2017 claimed that the United States had developed Persona Management Software that would allow specialists to propagandize social media partly through fake accounts and disinformation.[17] Perhaps no developments were more influential in promoting these fears than the Stuxnet virus, the establishment of CYBERCOM, and the

---

[14] E. O. Ostrovsky and A. S. Sizov, "The Approach to Modeling the Cognitive Sphere of Operational Intelligence Objects [Подход к моделированию когнитивной сферы объектов оперативной разведки]," *Military Thought [Военная мысль]*, No. 2, February 2016.

[15] Viktor Baranets and Oleg Falichev, "Soldier's Truth [Солдатская правда]," *Military-Industrial Courier [Военно-промышленный курьер]*, December 25, 2018.

[16] "Military Sites at the Festival for Author's Song [Военные площадки на фестивалях авторской песни]," Desantura.Ru, undated; Yevgeniy Georgievich Zushin, "Power Has No Equal in Strength [Власть, не имеющая равных по силе воздействия]," *Independent Military Review [Независимое военное обозрение]*, No. 16, April 30, 1999.

[17] Makarenko, 2017, p. 388.

leaked information provided by former National Security Agency contractor Edward Snowden.[18]

Thus, alongside measures aimed at greater control over the internet and social media, Russia has taken steps to insulate the military from online influences. A February 2019 law bans soldiers from using smartphones while on duty.[19] Intelligence concerns were probably paramount behind this measure—Russian soldiers' use of social media was used to track their operations in such theaters as Ukraine and Syria—but social media–based influence campaigns also likely played a role.[20] Restrictions were also imposed on soldiers' and military contractors' social media activity for similar reasons. As the Ministry of Defense explained in connection with these measures:

> the material published [on social media] by the members of the military is more and more frequently exploited by the special services of particular states, as well as terrorist and extremist organizations—for information-psychological influence, aimed at the destabilization of the internal political and social situation around the world.[21]

Such insecurity likely contributed to Russia's own consumption-side measures intended to fortify the military's capacity for resist-

---

[18] A. Krikunov, "Cyberspace of Leading States in the Context of Modern Challenges and Threats [Киберпространство ведущих государств в контексте современных вызовов и угроз]," *Naval Digest [Морской сборник]*, No. 11, 2011; Viktor Sokirko, "Symmetrical Answer: With Which Weapons Can Russia Answer America [Симметричный ответ: Каким оружием Россия может ответит США]," *Flag of the Motherland [Флаг Родины]*, No. 87, November 13, 2015; "U.S. Tried to Slow Down North Korea's Atomic Program [США пытались затормозить ядерную программу КНДР]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 6, 2015, p. 107.

[19] "Russia Bans Smartphones for Soldiers over Social Media Fears," BBC, February 20, 2019.

[20] Reid Standish, "Russian Troops Are in Syria, and We Have the Selfies to Prove It," Foreign Policy, September 8, 2015; Dmitry Volchek and Claire Bigg, "Ukrainian Bloggers Use Social Media to Track Russian Soldiers Fighting in East," The Guardian, June 3, 2015.

[21] Svetlana Bocharova and Aleksei Nikol'skiy, "Ministry of Defense Explains Ban on Troops Posting About Themselves on Social Media [Минобороны объяснило запрет военным писать о себе в соцсетях]," *Vedomosti [Ведомости]*, October 4, 2017.

ing information operations and PSYOPS. The aforementioned decision to resurrect the military's political directorate in 2017 appears to be largely a defensive mechanism against adversaries' perceived information-psychological attacks.[22] The military's political directorate during the Soviet era ensured adherence to Marxist-Leninist principles and party loyalty among service members, but it is far less clear what ideological identity will be the focus of the new Main Military Political Directorate (which carries the Russian acronym GVPU). The commander of the new political directorate, Colonel-General Andrey Kartapolov, indicated that Orthodox Christianity will play a significant role[23]—that is, Orthodox Christian values will underlie Russia's efforts to improve its military's resilience to psychological and information influences from the West. Further demonstrating concern for the robustness of the military psyche, Russia's Duma adopted a law in February 2017 mandating psychological evaluations for both soldiers and candidates for military educational institutions.[24] Russia's efforts to fortify psychological defenses led a Ukrainian expert to conclude that "[t]he current wave of interest in military psychology is primarily related to Russia's strong desire to catch up with the United States, which has achieved impressive results in this domain."[25]

---

[22] Oleg Falichev and Andrey Kartapolov, "The Right Goes to the First to Rise to the Attack [Право Первым Подняться в Атаку]," *Military-Industrial Courier [Военно-промышленный курьер]*, No. 35, September 11, 2018; Anton Nechaev, "State Duma Proposed to Legislate Who Should be Responsible for the Moral and Political State of the Military [Госдуме предложили узаконить, кто должен отвечать за морально-политическое состояние военных]," *Infokam [Инфокам]*, March 5, 2019.

[23] Andrey Kartapolov and Oleg Falichev, "The Army Should Be Spiritual [Армия должна быть духовой]," *Defense and Security [Защита и безопасности]*, No. 4, 2018.

[24] Sergey Sukhankin, "Military Psychology—New Pivot of Russian Military Strategy," *RealClearDefense*, March 15, 2018.

[25] Sukhankin, 2018.

## Vulnerabilities to Social Media–Based Information Operations

Although Russian anxieties about Western actions are exaggerations bordering on fantasy, the underlying perception of the regime's vulnerability to information flow through social media is not without cause. Opposition to Putin's regime, such as it is, does rely on social media. Thus, social media can be used to distribute content that feeds discontent—as Navalny, Putin's most visible opponent, routinely does. (One of his most successful documentaries, on Prime Minister Dmitriy Medvedev, reached 20 million views on YouTube.[26]) Although the Kremlin has clamped down on the internet and dominates the information environment, social media remains a potential conduit for content not sanctioned by the state to reach the Russian public. Although avenues are fewer and narrower, social media can still be used by critics and opponents to galvanize and organize collective action, and it can also be used to channel content that galvanizes the opposition. Although Putin's support remains relatively high, he and his regime are not invulnerable. As of 2020, discontent appears to be growing—waves of protest activity have occurred since 2017 on a variety of issues, including anticorruption, raising the pension age, and defense of a popular investigative reporter in 2019.[27]

Several particular points of vulnerability have the potential to erode popular support for Putin's regime and/or grow the ranks of regime opponents:

- **Corruption.** The scale of corruption in Putin's Russia is legendary.[28] Although his own popularity persists, there are reasons to

---

[26] Julia Ioffe, "What Russia's Latest Protests Mean for Putin," *The Atlantic*, March 27, 2017; "Navalny Video Accusing Medvedev of Corruption Posted on Government Websites," Radio Free Europe/Radio Liberty, June 11, 2017.

[27] Frida Ghitis, "Is Putin Losing the Trust of Russians?" *Politico Magazine*, June 20, 2019; Neil MacFarquhar, "Reporter's Arrest Sets Off Widespread Protests in Russia," *New York Times*, June 10, 2019.

[28] For accounts of the corrupt origins of Russia's oligarchic class, see Karen Dawisha, *Putin's Kleptocracy: Who Owns Russia?* New York: Simon and Schuster, 2014.

think that Russians are not impervious to demonstrations of that corruption.[29] The popularity of Navalny and his YouTube channel exposing the corruption of Russia's top officials and oligarchs (and the turnout at the subsequent protests in 2017) demonstrate that corruption is a live, motivating concern for at least some audiences in Russia.[30]

- **Economic distress.** Putin's popularity was buoyed by Russia's economic rise in the 2000s. Russia experts often observe that the stability of the regime rests on a kind of implied social compact in which Russians tolerate corruption and repression as long as they are economically better off than they were in the early post-Soviet era of the 1990s. The economic downturn since the 2008 crisis, and even more so since the 2014 fallout over Ukraine combined with oil price trends, have strained that compact. Thus, commentators point to Putin's (likely) declining popularity ratings and the increased propensity to strike and protest for economic reasons, such as unpaid wages and the unpopular decision to raise the pension age.[31]
- **Ethnic and religious cleavages, in society and military.** Russia is a multiethnic, multiconfessional, and multicultural country that has not resolved the tensions between those existing identities and elements of its still-emergent national identity—such as Christian Orthodoxy, Russian ethnicity, and language.[32] Russia has sought to position and define itself as a defender of traditional values in contrast with the morally decadent West. The

---

[29] For evidence that experience of corruption affects Russians' opinions of the regime, see William M. Reisinger, Marina Zaloznaya, and Vicki L. Hesli Claypool, "Does Everyday Corruption Affect How Russians View Their Political Leadership?" *Post-Soviet Affairs*, Vol. 33, No. 4, 2017, pp. 255–275.

[30] The protests, prompted by Navalny's documentary on Medvedev, attracted tens of thousands of people, not only in the capital but in dozens of cities across Russia. See Ioffe, 2017.

[31] For example, see Elizaveta Fokht, "Russia and Putin: Is President's Popularity in Decline?" BBC, June 19, 2019.

[32] On the tensions inherent in Russian national identity, see Yuri Teper and Daniel D. Course, "Contesting Putin's Nation-Building: The 'Muslim Other' and the Challenge of the Russian Ethno-Cultural Alternative," *Nations and Nationalism*, Vol. 20, No. 4, 2014.

> reinvigoration of the Russian Orthodox Church in Russian public life has supported this shift in national ideological discourse. The increasing emphasis on "traditional Russian moral and spiritual values," with its distinct Christian (and ethnic Russian) flavor, has the potential to alienate Russia's ethnic and religious minorities.[33] As prior RAND work observes, "[t]he ahistorical nature and vagueness of 'traditional Russian spiritual and moral values' are strengths as well as weaknesses for the Russian state."[34] This aspect of Russian national identity discourse might be particularly problematic in the context of the military's effort to attend to the spiritual resilience of their men: If the new political directorate seeks to indoctrinate soldiers into Christian Orthodox values, this would likely alienate non-Christian service members. Following the spring draft in 2018, Moscow reinvigorated efforts to limit the number of Muslim conscripts in the military despite that demographic's rapid growth and the need to build Russia's military, chiefly because officials fear ethnic conflicts could reduce cohesion and readiness.[35]

Anxieties about the vulnerability of the military to Western PSYOPS on social media are also not unwarranted. Generally, morale in the Russian military has improved significantly since the 2008 reforms because of improvement in some of the most-egregious aspects of military life (such as hazing), but multiple causes for grievances remain.[36] For instance, the Russian government's lack of transparency

---

[33] See, for example, Dobbins et al., 2019, pp. 151–152; Russian Federation, *Russian National Security Strategy*, full-text translation, December 31, 2015.

[34] Dobbins et al., 2019, p. 152.

[35] Paul Goble, "2018 Spring Draft Highlights Russia's Demographic Decline," *Eurasia Daily Monitor*, Vol. 15, No. 54, April 10, 2018. The Soviet and Russian armies have historically had difficulties integrating Muslims into the armed forces and using this demographic to its full potential (see Thomas S. Szayna, *The Ethnic Factor in the Soviet Armed Forces*, Santa Monica, Calif.: RAND Corporation, R-4002-A, 1991).

[36] For example, see Falichev and Kartapolov, 2018. For more on the Russian military's contemporary morale problems, see Michael Peck, "The Russian Military's Worst Enemy (HINT: Not America)," *The National Interest*, April 27, 2019.

about casualties sustained in Ukraine and Syria might be adversely affecting morale.[37] The broader vulnerabilities we have discussed carry the potential to undermine morale and discipline and erode cohesion in the military. That is, the military is not immune to Russia's broader epidemic of corruption, which appears widespread in the military.[38] Soldiers' morale also might be weakened by broader societal inequality, considering the sacrifices they are asked to make.[39]

Moreover, the Russian information warfare machine consists of significant actors outside the state, as Chapter Three describes. To the extent that the Russian information confrontation machine requires the participation of these actors, they—and their likely motivations—present an additional source of vulnerabilities. Unlike members of the military, individuals outside the state who take part in information operations are not bound by military discipline and are likely more susceptible to appeals to ordinary self-interest. An IRA troll, for example, might participate for pecuniary reasons and have no particular commitment to waging Russia's information warfare on social media.[40] These actors might be more susceptible to targeted individual appeals to self-interest than members of the military. Higher-status actors—such as computer professionals—might value the ability to operate in

---

[37] Seth Jones, *Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare*, Washington, D.C.: Center for Strategic and International Studies, CSIS Brief, October 1, 2018; Sukhankin, 2018.

[38] For example, see "Corruption in Russia's Military Quadrupled in 2018, Prosecutors Say," *Moscow Times*, March 21, 2019.

[39] See, for example, the point made by Baranets:

> I think that we cannot imbue [soldiers] with patriotism if the people don't have enough borscht in their plates. If soldiers ask political workers [i.e., from a new political directorate], why is there such a chasm between the rich and the poor? Why, in such a resource-rich country, are there 20 million impoverished people? We need to answer these questions truthfully and not talk out of our asses (author translation of Baranets and Falichev, 2018).

[40] The IRA appears not to vet their employees thoroughly for patriotism or devotion to the cause of information warfare. For example, see J. J. Green, "Tale of a Troll: Inside the 'Internet Research Agency' in Russia," WTOP, September 17, 2018; Neil MacFarquhar, "Inside the Russian Troll Factory: Zombies and a Breakneck Pace," *New York Times*, February 18, 2018.

Western countries: Their children could attend other schools; they might be able to own property and vacation in Europe or the United States. The ability to travel might be quite valuable to such individuals and would be compromised by a prospect of a criminal indictment. This vulnerability was implicitly exploited by the recent CYBERCOM action against individual Russian operatives.[41]

## Opportunities for Exploitation

Some Western experts advocate an offensive approach to Russia's information operations or political warfare more broadly. For example, Seth Jones of the of Center for Strategic and International Studies argues that "Russia will continue to target the United States at home and abroad until the U.S. government implements a more aggressive offensive information campaign."[42] Such a campaign, according to Jones, would "coerce Russia to curb its information warfare campaign, punish Moscow when these incidents occur, and exploit Moscow's weaknesses and vulnerabilities."[43] In theory, all of the aforementioned vulnerabilities present opportunities for offensive social media–based information operations. As RAND's James Dobbins and coauthors speculate, "Western actors could help to diminish the domestic legitimacy of the Putin regime by conducting an information campaign to expose the corruption in Russian elections," such as by spreading reports of fraud and statistical identification of falsification through Russian-language social media.[44] Similarly, Western actors could theoretically leak evidence of Russian corruption—potentially in the manner that resembles Russia's own leaks through WikiLeaks, DCLeaks, EMLeaks and

[41] Although details of the operation are not public, officials commented that "anyone singled out would know, based on the United States government's actions against other Russian operatives, that they could be indicted or targeted with sanctions." See Barnes, 2018.

[42] Jones, 2018.

[43] Jones, 2018.

[44] Dobbins et al., 2019.

so on.[45] All sources of popular discontent and division noted above might be exploited to encourage dissent, protests, or other forms of resistance. Still, there are weighty reasons to hesitate before embracing an approach that mirrors Russia's own.

First, the West tends to view and treat much of Russia's hostile influence or information operations as an illegitimate way to behave with regard to other states. This appears particularly true of Russia's uses of deception on social media, channeled toward other countries' populations at large outside a military context and focused on those countries' domestic politics. Thus, NATO hesitates to embrace such measures: "NATO doctrine does not foresee the use of covert information operations, such as the use of fake identities, 'bots' and 'trolling', against target audiences and furthermore, *psychological operations in general can only be used in the context of a military operation declared by the North Atlantic Council*."[46] Embracing similar approaches might tarnish the image of the United States, reduce international goodwill, and narrow U.S. policy options over the long term.[47]

Second, insofar as Russia believes that the West is already conducting such operations, it is not clear what confirming Russia's paranoias would accomplish. Russia's belief that the West is engaged in a perpetual offensive against it is one of the drivers of Russia's own information warfare. As we observe with regard to social media–based operations specifically, the most-aggressive manifestations of these appear to be in response to Western countermeasures to Russia's actions in Ukraine. If so, it is doubtful whether offensive actions by the United States or its allies would deliver much in the way of deterrence. On the contrary, such actions might lead to further escalation.[48] According to some informed accounts, the DNC leak and other election-meddling tactics

[45] Dobbins et al., 2019, p. 163.

[46] Cordy, 2017, p. 13 (emphasis added).

[47] For example, these actions likely preclude norm-setting in this domain down the road, even if this prospect is dim at present. See Samuel Charap and Ivan Timofeev, "Can Washington and Moscow Agree to Limit Political Interference?" *War on the Rocks*, June 13, 2019.

[48] See Dobbins et al., p. 160; Bodine-Baron et al., 2018, p. 25.

were in large part retaliation for perceived U.S. interference in Russia.[49] Moreover, some expert accounts suggest that Putin and his close associates appear to believe that the United States had already conducted an aggressive leak operation—the Panama Papers leak, which exposed official Russian corruption.[50] According to Soldatov and Borogan (Russian investigative journalists who have written extensively on cybersecurity and the Russian internet), the Panama Papers contributed to the decisions to leak DNC emails in retaliation.[51]

Third, an offensive approach might be ineffective. Putin's regime thoroughly controls the information environment, and accessing unsanctioned content will not be straightforward and will not reach broad audiences. Russians would likely have to seek out any such content—and those who seek out information critical of the regime are likely to be critically disposed already.[52] Even if critical content could receive broader dissemination, research suggests that it would be of limited efficacy—especially if the content is perceived to originate in the West, in which case it would be most commonly dismissed as Western propaganda.[53]

Fourth, even if going on the offense is effective, it is a high-risk approach. Stirring up tensions—whether between opposition and regime or along other prominent societal cleavages—could lead to

---

[49] See Soldatov and Borogan, 2015.

[50] For example, see A. I. Kolesnikov, "Vladimir Putin Was Not at a Loss for Words Regarding His Friend [Владимир Путин за другом в карман не полез]," *Kommersant [Коммерсантъ]*, Vol. 60, April 8, 2016, p. 3. Putin drew a (nonexistent) connection between a German newspaper reporting on the Panama Papers leak and Goldman Sachs, a stand-in for U.S. elites (which Putin appears to connect to Hilary Clinton), implying that the material was ordered by the United States. See "The Kremlin Apologizes to the German Newspaper Süddeutsche Zeitung for Yesterday's Words of Vladimir's Putin [Кремль извиняется перед немецкой газетой 'Зюддойче цайтунг' за вчерашние слова президента Владимира Путина]," *Echo of Moscow [Эхо Москвы]*, April 15, 2016.

[51] In Soldatov's explanation, the DNC leak was prompted by the Panama Papers, which he linked to Hillary Clinton. See Soldatov and Borogan, 2015; Michael Kirk, "Andrei Soldatov, Co-Author of *The Red Web*," Frontline, July 25, 2017.

[52] Dobbins et al., 2019, p. 161.

[53] Dobbins et al., 2019, p. 160.

unpredictable results for Russia and other states. The emergence of even a democratic opposition has not always favored U.S. interests. Within Russia, such actions could imperil Putin's opponents and citizens who would pick up and spread the hypothetical content.[54] Externally, "even if such a strategy were successful in undermining Russian domestic stability, Moscow could respond to such efforts not by turning inward but by lashing out and pursuing a diversionary conflict with the West."[55]

All that said, however, some vulnerabilities do present opportunities for offensive actions that carry fewer risks. In particular, digital operations that target individual actors within Russia's information confrontation machinery with tailored messaging might present a relatively low-cost, low-risk deterrence measure. Such tactics or operations might be leveled at various categories of actors identified in Chapter Three. For instance, Russian programmers and IT specialists, whom Moscow needs to support its offensive digital operations inside and outside the state, generally like to travel more and pursue careers outside Russia—particularly in the United States and Europe. They might well be more vulnerable to targeted messaging that makes it clear that they have been identified and threatens them with indictments or sanctions for continued information operations.[56] CYBERCOM's limited yet sophisticated targeting of IRA operatives to thwart meddling in the 2018 midterm elections presents the clearest example of such an approach.[57] In one intelligence expert's assessment, "[e]ven the unstated threat of sanctions could help deter some Russians from participating in covert disinformation campaigns."[58] Uniformed specialists are likely more difficult to deter from following orders, given that they have dedicated at least a portion of their life and freedom to serving the

---

[54] Dobbins et al., 2019, pp. 138, 160.

[55] Dobbins et al., 2019, p. 138.

[56] "Half of Russian Scientists Want to Emigrate," *UAWire*, June 30, 2018; Atlantic Council, "The Putin Exodus: The New Russian Brain Drain," webpage, undated.

[57] Barnes, 2018.

[58] Andrea Kendall-Taylor, a former intelligence official now with the Center for a New American Security, quoted in Barnes, 2018.

Russian state. Nonetheless, pursuing individual targeting of uniformed personnel still might be worthwhile. For one thing, targeted messaging that urges individual operators or units to desist from efforts or that seeks to demotivate them might lead normally offensively oriented Russian information confrontation detachments to focus more of their efforts on defending their own forces. For another, communicating with individuals about their risk of criminal charges were they ever to travel abroad, for example, might influence individuals' choices to stay or leave the armed forces.

Such approaches are unlikely to deter the Kremlin or the Russian military from waging information warfare on social media. However, these approaches might deter individual actors and thus weaken Russia's informational arsenal. Since 2014, Russian officials—notably Prime Minister Medvedev and Deputy Prime Minister Dmitriy Rogozin—have pointed to "brain drain" as a critical national problem.[59] Dissuading would-be specialists from recruitment could exacerbate personnel issues affecting units—inside and outside the state—involved in these operations. Likewise, targeted messaging directed at members of the military can compromise cohesion and morale. Overall, the effect of such operations would be to hamper and reduce effectiveness of Russia's own information efforts.

---

[59] "Medvedev Named the 'Export of Intellect' from Russia as Unacceptable [Медведев назвал недопустимым «экспорт интеллекта» из России]," RBC [РБК], February 27, 2017; "Rogozin Urged to Stop the "Brain Drain" Abroad [Рогозин призвал остановить «вымывание мозгов» за рубеж]," RBC [РБК], February 27, 2018.

# References


"305 Car Registrations May Point to Massive GRU Security Breach," Bellingcat, October 4, 2018. As of August 10, 2019:
https://www.bellingcat.com/news/2018/10/04/305-car-registrations-may-point-massive-gru-security-breach/

Administration of the Russian President [Администрация Президента России], "Military Doctrine of the Russian Federation [Военная доктрина Российской Федерации]," webpage, February 5, 2010. As of August 12, 2019:
http://kremlin.ru/supplement/461

Agarwal, Nitin, and Kiran Kumar Bandeli, "Examining Strategic Integration of Social Media Platforms in Disinformation Campaign Coordination," *Defence Strategic Communications*, Vol. 4, Spring 2018.

Akhmadullin, Vladimir, "The Word, Equal to the Bomb [Слово, приравненное к бомбе]," *Independent Military Review [Независимое военное обозрение]*, No. 25, July 2, 1999.

———, "Informational Suppression of Ghaddafi's Colonel and His Army [Информационное подавление полковника Каддафи и его армии]," *Asia Center [Центр Азия]*, September 3, 2011.

Alliance for Securing Democracy, Hamilton 2.0 Dashboard, undated. As of November 18, 2020:
https://securingdemocracy.gmfus.org/hamilton-dashboard/

Alperovitch, Dmitri, "Bears in the Midst: Intrusion into the Democratic National Committee," *CrowdStrike*, June 15, 2016. As of August 10, 2019:
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Antonovich, P., "Key Aspects of the Information War [Ключевые аспекты информационной войны]," *Army Digest [Армейский сборник]*, No. 1, January 2014, pp. 26–29.

Applebaum, Anne, Peter Pomerantsev, Melanie Smith, and Chloe Colliver, *"Make Germany Great Again": Kremlin, Alt-Right and International Influences in the 2017 German Elections*, London: Institute for Strategic Dialogue, 2017. As of August 12, 2019:
https://www.isdglobal.org/wp-content/uploads/2017/12/Make-Germany-Great-Again-ENG-061217.pdf

Apuzzo, Matt, "Europe Built a System to Fight Russian Meddling. It's Struggling," *New York Times*, July 6, 2019.

Apuzzo, Matt, and Adam Satariano, "Russia and Far Right Spreading Disinformation Ahead of EI Elections, Investigators Say," *Independent*, May 12, 2019a. As of August 12, 2019:
https://www.independent.co.uk/news/world/europe/eu-elections-latest-russia-far-right-interference-fake-news-meddling-a8910311.html

———, "Russia Is Targeting Europe's Elections. So Are Far-Right Copycats," *New York Times*, May 12, 2019b.

Aro, Jessikka, "The Cyberspace War: Propaganda and Trolling as Warfare Tools," *European View*, Vol. 15, June 1, 2016, pp. 121–132. As of August 12, 2019:
https://journals.sagepub.com/doi/10.1007/s12290-016-0395-5

Associated Press, "European Union to Stage War Games to Prepare for Hybrid Threats," *Los Angeles Times*, June 27, 2019. As of August 12, 2019:
https://www.latimes.com/world/la-fg-european-union-war-games-20190627-story.html

"At the Exercises of 'Caucasus-2016' They Worked Out 'Information Confrontation' for the First Time [На учениях «Кавказ-2016» впервые отработали «информационное противоборство»]," *RIA Novosti [РИА Новости]*, September 14, 2016. As of August 9, 2019:
https://ria.ru/20160914/1476902330.html

Atlantic Council, "The Putin Exodus: The New Russian Brain Drain," webpage, undated. As of August 12, 2019:
https://www.atlanticcouncil.org/events/upcoming-events/detail/1-the-putin-exodus-the-new-russian-brain-drain

Auchard, Eric, and Toby Sterling, "Google and Sister Company to Offer Cyber Security to Election Groups," Reuters, March 21, 2017. As of August 12, 2019:
https://www.reuters.com/article/us-cyber-election/google-and-sister-company-to-offer-cyber-security-to-election-groups-idUSKBN16S166

Bail, Christopher A., Brian Guay, Emily Maloney, Aidan Combs, D. Sunshine Hillygus, Friedolin Merhout, Deen Freelon, and Alexander Volfovsky, "Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017," *Proceedings of the National Academy of Sciences*, Vol. 117, No. 1, January 7, 2020, pp. 243–250.

Baldor, Lolita C., "Key U.S. Military Command's Twitter, YouTube Sites Hacked," APNews, January 12, 2015. As of August 12, 2019: https://apnews.com/63701279a8dd4f5da75c1362c00b71d4

Baranets, Viktor, and Oleg Falichev, "Soldier's Truth [Солдатская правда]," *Military-Industrial Courier [Военно-промышленный курьер]*, No. 50, December 25, 2018. As of August 12, 2019: https://vpk-news.ru/articles/47252

Barker, Tyson, "Germany Strengthens Its Cyber Defense: How It's Meeting the Russian Threat," *Foreign Affairs*, May 26, 2017. As of August 12, 2019: https://www.foreignaffairs.com/articles/germany/2017-05-26/germany-strengthens-its-cyber-defense

Barnes, Julian E., "U.S. Begins Cyberoperation Against Russia in Effort to Protect Elections," *New York Times*, October 23, 2018.

Bay, Sebastian, Giorgio Bertolin, Nora Biteniece, Edward H. Christie, Anton Dek, Rolf E. Fredheim, John D. Gallacher, Kateryna Kononova, and Tetiana Marchenko, *Responding to Cognitive Security Challenges*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, January 2019.

Bechev, Dimitar, *Rival Power: Russia's Influence in Southeastern Europe*, New Haven, Conn.: Yale University Press, 2017.

"Behind the Dutch Terror Threat Video: The St. Peterburg 'Troll Factory' Connection," Bellingcat, April 3, 2016. As of August 12, 2019: https://www.bellingcat.com/news/uk-and-europe/2016/04/03/azov-video/

Belous, V., "Weapons of the 21st Century [Оружия XXI века]," *International Life [Международная Жизнь]*, No. 2, 2009, pp. 64–82.

Belozerov, Vasily, and Daria Kopylova, "Mass Media: Information Confrontation [СМИ: Информационное Противоборство]," *Orienteer [Ориентир]*, No. 5, May 2014, pp. 9–12.

Bentzen, Naja, *Foreign Influence Operations in the EU*, Brussels, Belgium: European Parliamentary Research Service, July 2018. As of August 8, 2019: http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf

Bobrov, A., "Information War: From Leaflets to Twitter [Информационная война: от листовки до Твиттера]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 1, January 2013, pp. 20–27.

Bocharova, Svetlana, and Aleksei Nikol'skiy, "Ministry of Defense Explains Ban on Troops Posting About Themselves on Social Media [Минобороны объяснило запрет военным писать о себе в соцсетях]," *Vedomosti [Ведомости]*, October 4, 2017. As of August 12, 2019: https://www.vedomosti.ru/politics/articles/2017/10/04/736578-zapret-voennim-pisat-sotssetyah

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence*, Santa Monica, Calif.: RAND Corporation, RR-2740-RC, 2018. As of August 12, 2019: https://www.rand.org/pubs/research_reports/RR2740.html

Boffey, Daniel, "Europe's New Cold War Turns Digital as Vladimir Putin Expands Media Offensive," *The Guardian*, March 5, 2016. As of August 12, 2019: https://www.theguardian.com/world/2016/mar/05/europe-vladimir-putin-russia-social-media-trolls

Borskiy, Nikolai, "Main Directions for Ensuring Information Security in the Activities of Troops (Forces) [Основные направления обеспечения информационной безопасности в деятельности войск (сил)]," *Orienteer [Ориентир]*, No. 11, November 2001.

Boyd, Aaron, "What DOD Plans To Do With $9.6 billion in Cyber Funding," *Nextgov*, March 14, 2019. As of August 16, 2019: https://www.nextgov.com/cybersecurity/2019/03/what-dod-plans-do-96-billion-cyber-funding/155564/

Boyd, Danah M., and Nicole B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, Vol. 13, No. 1, 2008, pp. 210–230.

Brantly, Aaron, and Liam Collins, "A Bear of a Problem: Russian Special Forces Perfecting Their Cyber Capabilities," Association of the United States Army, November 28, 2018. As of August 12, 2019: https://www.ausa.org/articles/bear-problem-russian-special-forces-perfecting-their-cyber-capabilities

Brattberg, Erik, and Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, May 23, 2018. As of August 12, 2019: https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

"Breedlove's War: Emails Show Ex-NATO General Plotting U.S. Conflict with Russia," *RT*, July 1, 2016. As of August 12, 2019: https://www.rt.com/usa/349213-hacked-emails-breedlove-ukraine/

"British Officials Probe 2,800 Russian Bots That 'Spread Confusion' After Salisbury Nerve Agent Attack on Former Spy," *Daily Mail*, March 23, 2018. As of August 12, 2019: https://www.dailymail.co.uk/news/article-5538699/Officials-probe-2-800-Russian-bots-spread-confusion.html

Broderick, Ryan, "Here's Everything The Mueller Report Says About How Russian Trolls Used Social Media," *BuzzFeed News*, April 18, 2019. As of August 12, 2019: https://www.buzzfeednews.com/article/ryanhatesthis/mueller-report-internet-research-agency-detailed-2016

Bump, Philip, "Don't Blame the Seth Rich Conspiracy on Russians. Blame Americans," *Washington Post*, July 9, 2019.

Burenok, V. M., A. A. Ivlevl, and V. Yu. Korchak, *Development of Military Technologies of the XXI Century: Problems, Planning, Actualization [Развитие военных технологий XXI века: проблемы планирование, реализация]*, Tver, Russia: OOO "Kupol," 2009, cited in Makarenko, p. 224.

"Bushuev, a Russian Military Colonel (aka 'Dawn') Was Killed in the Donbass [На Донбассе погиб полковник ВС РФ Бушуев «Заря»]," Trust.ua, July 4, 2016. As of October 7, 2019:
https://uapress.info/ru/news/show/136593

Calabresi, Missimo, "Inside Russia's Social Media War on America," *Time*, Vol. 189, No. 20, May 18, 2017. As of August 9, 2019:
https://time.com/magazine/us/4783906/may-29th-2017-vol-189-no-20-u-s/

Carberry, Sean D., "CyberCom Seeks 16 Percent Budget Surge for 2018," *FCW*, May 23, 2017. As of August 12, 2019:
https://fcw.com/articles/2017/05/23/cybercom-rogers-budget-carberry.aspx

Cederberg, Gabriel, *Catching Swedish Phish: How Sweden Is Protecting Its 2018 Elections*, Defending Digital Democracy Project, August 2018.

Central Intelligence Agency, "Europe: Ukraine," World Factbook website, undated. As of August 12, 2019:
https://www.cia.gov/library/publications/the-world-factbook/geos/up.html

Charap, Samuel, and Timothy J. Colton, *Everyone Loses: The Ukraine Crisis and the Ruinous Contest for Post-Soviet Eurasia*, Milton Park, United Kingdom: Routledge, 2018.

Charap, Samuel, and Ivan Timofeev, "Can Washington and Moscow Agree to Limit Political Interference?" *War on the Rocks*, June 13, 2019. As of August 12, 2019:
https://warontherocks.com/2019/06/
can-washington-and-moscow-agree-to-limit-political-interference/

Chekinov, S. G. and S. A. Bogdanov, "Forecasting the Nature and Content of Wars of the Future [Прогнозирование характера и содержания войн будущего: проблемы и суждения]," *Military Thought [Военная мысль]*, No. 15, 2015, pp. 44–45.

"Chemical Weapons and Absurdity: The Disinformation Campaign Against the White Helmets," Bellingcat, December 18, 2018. As of August 12, 2019:
https://www.bellingcat.com/news/mena/2018/12/18/chemical-weapons-and-absurdity-the-disinformation-campaign-against-the-white-helmets/

Chen, Adrian, "The Agency," *New York Times*, June 2, 2015.

Cheshuin, S. A., "Features of Modern Information Confrontation and Taking Them into Account in Preparation of Specialists of Foreign Military Information in the Military University [Особенности современного информационного противоборства и их учёт при подготовке специалистов зарубежной военной информации в Военном университете]," Pandia.ru, undated. As of August 9, 2019:
https://pandia.ru/text/77/194/29043.php

Chesney, Robert, and Danielle K. Citron, *Disinformation on Steroids: The Threat of Deep Fakes*, New York: Council on Foreign Affairs, of October 16, 2018. As of August 12, 2019:
https://www.cfr.org/report/deep-fake-disinformation-steroids

———, "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics," *Foreign Affairs*, January/February 2019. As of August 12, 2019:
https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war

Chiacu, Doina, and Arshad Mohammed, "Leaked Audio Reveals Embarrassing U.S. Exchange on Ukraine, EU," Reuters, February 6, 2014. As of August 12, 2019:
https://www.reuters.com/article/us-usa-ukraine-tape/leaked-audio-reveals-embarrassing-u-s-exchange-on-ukraine-eu-idUSBREA1601G20140207

Churakova, Ol'ga, Elena Mukhametshina, Elizaveta Ser'gina, and Ekaterina Bryzgalova, "Channels on Telegram Have Become the New Market for Political Advertisement [Каналы в Telegram стали новым рынком политической рекламы]," *Vedomosti [Ведомости]*, September 27, 2017. As of August 12, 2019:
https://www.vedomosti.ru/politics/articles/2017/09/27/735467-telegram-kanali-politicheskoi-reklami

Cimpanu, Catalin, "Russia's Elite Hacking Unit Has Been Silent, but Busy," *Zero Day*, October 5, 2018. As of August 10, 2019:
https://www.zdnet.com/article/russias-elite-hacking-unit-has-been-silent-but-busy/

———, "US Wiped Hard Drives at Russia's 'Troll Factory' in Last Year's Hack," *Zero Day*, February 28, 2019. As of August 12, 2019:
https://www.zdnet.com/article/us-wiped-some-hard-drives-of-russias-troll-factory-in-last-years-hack/

Coats, Daniel R., *Worldwide Threat Assessment of the U.S. Intelligence Community*, Washington, D.C.: Office of the Director of National Intelligence, January 29, 2019. As of August 12, 2019:
https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Cohen, Michael, and Mathew Green, "Ukraine's Volunteer Battalions," *Infantry Magazine*, April–July, 2016. As of August 12, 2019:
https://www.benning.army.mil/infantry/magazine/issues/2016/APR-JUL/pdf/16)%20Cohen_UkraineVolunteers_TXT.pdf

Cohen, Raphael S., Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwille, Elina Treyger, and Nathan Vest, *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*, Santa Monica, Calif.: RAND Corporation, RR-4373/1-AF, 2021. As of July 19, 2021: https://www.rand.org/pubs/research_reports/RR4373z1.html

Cohen, Raphael S., Alyssa Demus, Michael Schwille, and Nathan Vest, *U.S. Efforts to Combat Foreign Disinformation on Social Media*, Santa Monica, Calif.: RAND Corporation, 2021, Not available to the general public.

Cohen, Raphael S., and Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat*, Santa Monica, Calif.: RAND Corporation, RR-1793-A, 2019. As of August 12, 2019: https://www.rand.org/pubs/research_reports/RR1793.html

Collins, Liam, "Russia Gives Lessons in Electronic Warfare," Association of the United States Army, July 26, 2018. As of August 12, 2019: https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare

"Commander of the RF Armed Forces Bushuev Perished in the Donbass: How This Came to Pass [На Донбассе погиб полковник ВС РФ Бушуев. Как это было] " Inshe.TV, July 4, 2016. As of September 30, 2019: https://inshe.tv/society/2016-07-04/138184/

Confessore, Nicholas, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," *New York Times*, April 4, 2018.

Cordy, Jane, *The Social Media Revolution: Political and Security Implications*, NATO Parliamentary Assembly Committee on the Civil Dimension of Security, October 7, 2017. As of August 12, 2019: https://www.nato-pa.int/download-file?filename=sites/default/files/2017-11/2017%20-%20158%20CDSDG%2017%20E%20bis%20-%20SOCIAL%20MEDIA%20REVOLUTION%20-%20CORDY%20REPORT.pdf

"Corruption in Russia's Military Quadrupled in 2018, Prosecutors Say," *Moscow Times*, March 21, 2019. As of August 12, 2019: https://www.themoscowtimes.com/2019/03/21/corruption-in-russias-military-quadrupled-in-2018-prosecutors-say-a64907

Costello, Katherine, *Russia's Use of Media and Information Operations in Turkey*, Santa Monica, Calif.: RAND Corporation, PE-278-A, 2018. As of August 9, 2019: https://www.rand.org/pubs/perspectives/PE278.html

Cotovio, Vasco, and Emanuella Grinberg, "Spain: 'Misinformation' on Catalonia Referendum Came from Russia," CNN, November 14, 2017. As of August 12, 2019: https://edition.cnn.com/2017/11/13/europe/catalonia-russia-connection-referendum/index.html

"Cyber-Forces Will Appear in the Army Before the End of the Year [Кибервойска появятся в армии до конца года]," *Moscow 24 [Москва 24]*, July 5, 2013. As of January 28, 2019:
https://www.m24.ru/articles/Minoborony/05072013/20906

Cyber Operations Tracker, "Turla," webpage, undated. As of August 10, 2019:
https://www.cfr.org/interactive/cyber-operations/turla

"Cybertroops Are Deployed on the Internet [В интернет ввели кибервойска]," *Kommersant [Коммерсантъ]*, No. 2, January 10, 2017. As of January 7, 2020:
https://www.kommersant.ru/doc/3187320

Dave, Paresh, and Christopher Bing, "Russian Disinformation on YouTube Draws Ads, Lacks Warning Labels: Researchers," Reuters, June 7, 2019. As of August 12, 2019:
https://www.reuters.com/article/
us-alphabet-google-youtube-russia-idUSKCN1T80JP

Davydov, D., "Information-Psychological War in Afghanistan [Информационно-психологическая война в Афганистане]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 8, August 2012.

Dawisha, Karen, *Putin's Kleptocracy: Who Owns Russia?* New York: Simon and Schuster, 2014.

de Carbonnel, Alissa, "Insight: Social Media Makes Anti-Putin Protests 'Snowball,'" Reuters, December 7, 2011. As of August 10, 2019:
https://www.reuters.com/article/us-russia-protests-socialmedia/insight-social-media-makes-anti-putin-protests-snowball-idUSTRE7B60R720111207

Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations*, Washington, D.C., 2017. As of August 10, 2019:
https://www.dia.mil/Portals/27/Documents/News/
Military%20Power%20Publications/Russia%20Military%20Power%20
Report%202017.pdf?ver=2017-06-28-144235-937

Dek, Anton, Kateryna Kononova, and Tetiana Marchenko, "The Effects of Banning the Social Network VK in Ukraine," in *Responding to Cognitive Security Challenges*, Riga, Latvia: NATO StratCom CoE, January 2019, pp. 39–59. As of August 12, 2019:
https://www.ceeol.com/search/chapter-detail?id=774833

Delk, Josh, "Pentagon Reports Increase in Russian Trolls Since Syria Strike," *The Hill*, April 14, 2018. As of August 12, 2019:
https://thehill.com/policy/
cybersecurity/383169-pentagon-reports-increase-in-russian-trolls-since-syria-strike

Department of External Intelligence of Estonia [Департамент внешней разведки Эстонии], *Estonia in International Security Environment 2018 [Эстония в Международной Среде Безопастности 2018]*, Tallinn, Estonia, 2018. As of August 9, 2019:
https://icds.ee/wp-content/uploads/2018/06/VLA-Raport-2018-venekeelne.pdf

Department of the Army, "Appendix D: Propaganda Assessment," *Tactical Psychological Operations Tactics, Techniques, and Procedures*, Field Manual 3-05.302 MCRP 3-40.6B, October 2005.

"Details on the 'Psychos' of Russia's Armed Forces Have Become Known [Стали известны данные о войсках «психов» России]," *Tribune [Трибун]*, February 6, 2018. As of January 31, 2019:
https://tribun.com.ua/47273

Deutsche Welle, "Russia's Information Warfare Targets German Soldiers in Lithuania," Atlantic Council, February 24, 2017. As of August 12, 2019:
https://www.atlanticcouncil.org/blogs/natosource/russia-s-information-warfare-targets-german-soldiers-in-lithuania

DFRLab—*See* Digital Forensics Lab.

Digital Forensics Lab, "Electronic Warfare by Drone and SMS: How Russia-Backed Separatists Use 'Pinpoint Propaganda' in the Donbas," *Medium*, May 18, 2017. As of August 10, 2019:
https://medium.com/dfrlab/electronic-warfare-by-drone-and-sms-7fec6aa7d696

———, "Russia's Full Spectrum Propaganda: A Case Study in How Russia's Propaganda Machine Works," *Medium*, January 23, 2018a. As of August 10, 2019:
https://medium.com/dfrlab/russias-full-spectrum-propaganda-9436a246e970

———, "#TrollTracker: How to Spot Russian Trolls," *Medium*, March 29, 2018b. As of August 12, 2019:
https://medium.com/dfrlab/trolltracker-how-to-spot-russian-trolls-2f6d3d287eaa

———, "#PutinAtWar: Social Media Surge on Skripal," *Medium*, April 5, 2018c. As of August 12, 2019:
https://medium.com/dfrlab/putinatwar-social-media-surge-on-skripal-b5132db6f439

———, "#TrollTracker: 2000% More Russian Trolls on Syria Strikes?" *Medium*, April 16, 2018d. As of August 12, 2019:
https://medium.com/dfrlab/trolltracker-2000-more-russian-trolls-on-syria-strikes-dbca2b4a76da

——— "#TrollTracker: Russia's Other Troll Team," *Medium*, August 2, 2018e. As of August 10, 2019:
https://medium.com/dfrlab/trolltracker-russias-other-troll-team-4efd2f73f9b5

———, "#BalticBrief: The Kremlin's Loudspeaker in Latvia," *Medium*, November 19, 2018d. As of August 12, 2019: https://medium.com/dfrlab/balticbrief-the-kremlins-loudspeaker-in-latvia-14c6398b2473

———, "Top Takes: Suspected Russian Intelligence Operation," *Medium*, June 22, 2019. As of August 12, 2019: https://medium.com/dfrlab/top-takes-suspected-russian-intelligence-operation-39212367d2f0

Diamond, Jeremy, "Intel Report: Putin Directly Ordered Effort to Influence Election," CNN, January 6, 2017. As of August 10, 2019: https://www.cnn.com/2017/01/06/politics/intelligence-report-putin-election/index.html

Dias, Nic, *The Big Question: How Will 'Deepfakes' and Emerging Technology Transform Disinformation?* Washington, D.C.: National Endowment for Democracy, 2018. As of August 12, 2019: https://www.ned.org/wp-content/uploads/2018/10/How-Will-Deepfakes-and-Emerging-Technology-Transform-Disinformation.pdf

DiResta, Renee, and Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, Stanford, Calif.: Internet Observatory, Cyber Policy Center, Stanford University, white paper, 2019.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson, *The Tactics & Tropes of the Internet Research Agency*, New Knowledge, December 17, 2018. As of August 10, 2019: https://www.newknowledge.com/articles/the-disinformation-report/

Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Interim Report*, London, United Kingdom: United Kingdom House of Commons, Fifth Report of Session 2017–19, July 29, 2018. As of August 12, 2019: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm

"Disinformation Operations in the Czech Republic," European Values Center for Security Policy, blog post, September 13, 2016. As of August 9, 2019: https://www.europeanvalues.net/vyzkum/disinformation-operations-in-the-czech-republic/

Dobbins, James, Raphael S. Cohen, Nathan Chandler, Bryan Frederick, Paul DeLuca, Edward Geist, Forrest E. Morgan, Howard J. Shatz, and Brent Williams, *Extending Russia: Competing from Advantageous Ground*, Santa Monica, Calif.: RAND Corporation, RR-3063-A, 2019. As of October 28, 2020: https://www.rand.org/pubs/research_reports/RR3063.html

"Documentary About Battle of Debaltseve to Be Aired on February 17," 112.International, February 16, 2016. As of August 12, 2019: https://112.international/culture/documentary-about-battle-of-debaltseve-to-be-aired-on-february-17-2682.html

DoD—*See* U.S. Department of Defense.

Doffman, Zak, "Russia's Secret Intelligence Agency Hacked: 'Largest Data Breach in Its History,'" *Forbes*, July 20, 2019. As of August 10, 2019: https://www.forbes.com/sites/zakdoffman/2019/07/20/russian-intelligence-has-been-hacked-with-social-media-and-tor-projects-exposed/#749cdf556b11

Donovan, Alice, "Does America Need Such Friends," *Veterans Today*, February 25, 2016. As of August 12, 2019: http://web.archive.org/web/20160226102433/https:/www.veteranstoday.com/2016/02/25/does-america-need-such-friends/

Dostoevsky, Fyodor, *The Idiot: A Novel in Four Parts [Идиот: Роман в четырех частях]*, Moscow: Sciences Publishing House [Издательный дом «НАУКА»], reprint 1988. As of August 9, 2019: https://ilibrary.ru/text/94/index.html

Duke Reporters' Lab, homepage, undated. As of August 8, 2019: https://reporterslab.org/fact-checking/

Dvornikov, Aleksandr, "Headquarters for New Wars [Штабы для новых войн]," *Military-Industrial Courier [Военно-промышленный курьер]*, No. 28, July 24, 2018, p. 1. As of August 8, 2019: https://vpk-news.ru/articles/43971

Dylevskii, I. N., V. O. Zapivakhin, S. A. Komov, S. V. Korotkov, and A. A. Krivchenko, "On the Dialectic of Deterrence and Prevention of Military Conflicts in the Information Age [О диалектике сдерживания и предотвращения военных конфликтов в информационную эру]," *Military Thought [Военная мысль]*, No. 7, 2016.

Dylevskii, I. N., V. O. Zapivakhin, S. A. Komov, S. V. Korotkov, and A. N. Petrunin, "An International Nonproliferation Regime for Information Weapons: Utopia or Reality? [Международный режим нераспространения информационного оружия: утопия или реальность?]," *Military Thought [Военная мысль]*, No. 10, October 2014, pp. 3–12.

Dzikavitskiy, Aleksey, and Yaroslav Shimov, "Knights of the 'Russian World' [Рыцари «русского мира»]," Radio Svoboda [Радио Свобода], March 2, 2017. As of August 9, 2019: https://www.svoboda.org/a/28340833.html

Earley, Pete, *Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War*, New York: Berkley, 2006.

"Editor-in-Chief of RT Commented on Power's Statement on the Budget of the Channel [Главный редактор RT прокомментировала слова Пауэр о бюджете телеканала]," *RIANovosti*, January 18, 2017. As of January 8, 2020: https://ria.ru/20170118/1485960869.html

Elder, Miriam, "Russians Fight Twitter and Facebook Battles over Putin Election," *The Guardian*, December 9, 2011. As of August 9, 2019: https://www.theguardian.com/world/2011/dec/09/russia-putin-twitter-facebook-battles

———, "Emails Give Insight into Kremlin Youth Group's Priorities, Means and Concerns," *The Guardian*, February 7, 2012a. As of August 10, 2019: https://www.theguardian.com/world/2012/feb/07/nashi-emails-insight-kremlin-groups-priorities

———, "Russian Protests: Thousands March in Support of Occupy Abay Camp," *The Guardian*, May 13, 2012b. As of August 9, 2019: https://www.theguardian.com/world/2012/may/13/russian-protests-march-occupy-abay

"EU Releases New Sanctions List," Radio Free Europe/Radio Liberty, July 30, 2014. As of August 10, 2019: https://www.rferl.org/a/russia-new-eu-sanctions-ukraine/25475813.html

European Commission, "A Europe That Protects: The EU Steps Up Action Against Disinformation," press release, December 5, 2018. As of August 12, 2019: https://europa.eu/rapid/press-release_IP-18-6647_en.htm

———, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the Implementation of the Action Plan Against Disinformation*, Brussels, June 14, 2019. As of August 12, 2019: https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf

European Parliament, resolution on EU strategic communication to counteract propaganda against it by third parties, November 23, 2016. As of August 12, 2019: http://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html?redirect

European Values Center for Security Policy, homepage, undated. As of August 12, 2019: https://www.europeanvalues.net/

Evdokimov, Andrey, "About Active Information Measures Along the Southern Strategic Direction [Об активных информационных мероприятиях на южном стратегическом направлении]," *Defense and Security [Защита и безопасность]*, No. 4, 2010.

"Ex-French Economy Minister Macron Could be 'US Agent' Lobbying Banks' Interests," Sputnik, February 4, 2017. As of August 12, 2019: https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq/

Falichev, Oleg, and Andrey Kartapolov, "The Right Goes to the First to Rise to the Attack [Право Первым Подняться в Атаку]," *Military Industrial Courier [Военно-промышленный курьер]*, No. 35, September 11, 2018. As of August 12, 2019:
https://www.vpk-news.ru/articles/44913

Fedchenko, Yevhen, "Kremlin Propaganda: Soviet Active Measures by Other Means," Stopfake.org, March 21, 2016. As of August 10, 2019:
https://www.stopfake.org/en/
kremlin-propaganda-soviet-active-measures-by-other-means/

Field, Matthew, and Mike Wright, "Russian Trolls Sent Thousands of Pro-Leave Messages on the Day of Brexit Referendum, Twitter Data Reveals," *The Telegraph*, October 17, 2018. As of August 12, 2019:
https://www.telegraph.co.uk/technology/2018/10/17/
russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/

"Figure of the Week: 1.3 billion," *EU vs. Disinfo*, October 1, 2019. As of December 15, 2019:
https://euvsdisinfo.eu/figure-of-the-week-1-3-billion/

Fokht, Elizaveta, "Russia and Putin: Is President's Popularity in Decline?" BBC, June 19, 2019.

"The Forces of Russia's Information Operations: What Should Ukraine's Response Be? [Силы информационных операций России каким должен быть ответ Украины?]," Sprotyv.info, April 10, 2014. As of August 9, 2019:
https://web.archive.org/web/20190202014139/
http://sprotyv.info/ru/news/5931-sily-informacionnyh-operaciy-rossii-kakim-dolzhen-byt-otvet-ukrainy

Franke, Ulrik, *War by Non-Military Means: Understanding Russian Information Warfare*, Kista, Sweden: Swedish Defense Research Agency, March 2015. As of August 8, 2019:
http://johnhelmer.net/wp-content/uploads/2015/09/
Sweden-FOI-Mar-2015-War-by-non-military-means.pdf

Friedman, Misha, "The High Price of Putin's Takeover of Crimea," Bloomberg, March 31, 2017.

"FSB Does Not See Violations of the Law in the Actions of the Tomsk Hackers Against the Site 'Caucus-Center' [ФСБ не видит нарушения закона в действиях томских хакеров против сайта «Кавказ-центр»]," Newsru.com, February 4, 2002. As of August 9, 2019:
https://www.newsru.com/russia/04feb2002/tomsk.html

Galeotti, Mark, "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?" *Small Wars & Insurgencies*, Vol. 27, No. 2, March 21, 2016, pp. 282–301. As of August 9, 2019: https://www.tandfonline.com/doi/pdf/10.1080/09592318.2015.1129170?needAccess=true

———, "Russian Intelligence Is at (Political) War," *NATO Review Magazine*, May 12, 2017a. As of August 10, 2019: https://www.nato.int/docu/review/2017/also-in-2017/russian-intelligence-political-war-security/EN/index.htm

———, "The 'Trump Dossier,' or How Russia Helped America Break Itself," *Tablet Magazine*, June 13, 2017b. As of August 10, 2019: https://www.tabletmag.com/jewish-news-and-politics/237266/trump-dossier-russia-putin

———, *Controlling Chaos: How Russia Manages Its Political War in Europe*, London, United Kingdom: European Council on Foreign Relations, September 2017c. As of August 10, 2019: https://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe

———, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" *Foreign Policy*, March 5, 2018. As of January 2, 2020: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Gallacher, John D., Vlad Barash, Philip N. Howard, and John Kelly, "Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns Against U.S. Military Personnel and Veterans," ComProp Data Memo 2017.9, October 9, 2017. As of August 12, 2019: http://blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2017/10/Junk-News-on-Military-Affairs-and-National-Security-1.pdf

Gallacher, John D., and Rolf E. Fredheim, *Division Abroad, Cohesion at Home: How the Russian Troll Factory Works to Divide Societies Overseas but Spread Pro-Regime Messages at Home*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2019.

Gallagher, Sean, "Candid Camera: Dutch Hacked Russians Hacking DNC, Including Security Cameras," Ars Technica, January 26, 2018. As of August 12, 2019: https://arstechnica.com/information-technology/2018/01/dutch-intelligence-hacked-video-cameras-in-office-of-russians-who-hacked-dnc/

Gearan, Anne "In Recording of U.S. Diplomat, Blunt Talk on Ukraine," *Washington Post*, February 6, 2014.

Gerasimov, Valeriy, "The Value of Science Is in Prediction [Ценность науки в предвидении]," *Military-Industrial Courier [Военно-промышленный курьер]*, No. 8, February 26, 2013, pp. 1–3. As of August 8, 2019: https://www.vpk-news.ru/articles/14632

———, "According to the Experience of Syria [По опыту Сирии]," *Military Industrial Courier [Военно-промышленный курьер]*, No. 9, March 9, 2016. As of August 8, 2019: https://vpk-news.ru/sites/default/files/pdf/VPK_09_624.pdf

Gerber, Theodore P., and Jane Zavisca, "Does Russian Propaganda Work?" *Washington Quarterly*, Vol. 39, No. 2, Summer 2016, pp. 79–98. As of August 9, 2019: https://www.tandfonline.com/doi/pdf/10.1080/0163660X.2016.1204398?needAccess=true

Gerden, Eugene, "Russia to Spend $250m Strengthening Cyber-Offensive Capabilities," *SC Media*, February 4, 2016. As of January 31, 2019: https://www.scmagazineuk.com/russia-spend-250m-strengthening-cyber-offensive-capabilities/article/1477698

"Germany Fines Facebook for Underreporting Hate Speech Complaints," *DW*, July 2, 2019. As of August 12, 2019: https://www.dw.com/en/germany-fines-facebook-for-underreporting-hate-speech-complaints/a-49447820

Gerth, Jeff, "Military's Information War Is Vast and Often Secretive," *New York Times*, December 11, 2005.

Ghitis, Frida, "Is Putin Losing the Trust of Russians?" *Politico Magazine*, June 20, 2019. As of August 12, 2019: https://www.politico.com/magazine/story/2019/06/20/vladimir-putin-russians-227198

Giles, Keir, *Handbook of Russian Information Warfare*, Rome, Italy: NATO Defense College, November 2016.

Gleicher, Nathaniel, "Removing Coordinated Inauthentic Behavior from Russia," Facebook Newsroom, January 17, 2019. As of August 9, 2019: https://newsroom.fb.com/news/2019/01/removing-cib-from-russia/

GLOBSEC Policy Institute, "Central Europe Under the Fire of Propaganda: Public Opinion Poll Analysis in the Czech Republic, Hungary and Slovakia," September 2016.

Goble, Paul, "2018 Spring Draft Highlights Russia's Demographic Decline," *Eurasia Daily Monitor*, Vol. 15, No. 54, April 10, 2018. As of August 12, 2019: https://jamestown.org/program/2018-spring-draft-highlights-russias-demographic-decline/

Gordon, Greg, and David Goldstein, "Russian Propaganda Targeted U.S. Vets And Service Members Via Social Media," *Task and Purpose*, October 9, 2017. As of August 12, 2019:
https://taskandpurpose.com/
russian-propaganda-targeted-us-vets-service-members-via-social-media

Gotkowska, Justyna, "The Cyber and Information Space: A New Formation in the Bundeswehr," *Fortuna's Corner*, April 12, 2017. As of August 12, 2019:
https://fortunascorner.com/2017/04/14/
the-cyber-and-information-space-a-new-formation-in-the-bundeswehr/

Green, J. J., "Tale of a Troll: Inside the 'Internet Research Agency' in Russia," WTOP, September 17, 2018. As of August 12, 2019:
https://wtop.com/j-j-green-national/2018/09/
tale-of-a-troll-inside-the-internet-research-agency-in-russia/

Greenberg, Andy, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 20, 2017. As of August 9, 2019:
https://www.wired.com/story/russian-hackers-attack-ukraine/

Greenberg, Andy, "Russian Hackers Go From Foothold to Full-On Breach in 19 Minutes," *Wired*, February 19, 2019a. As of August 12, 2019:
https://www.wired.com/story/russian-hackers-speed-intrusion-breach/

———, "Alphabet-Owned Jigsaw Bought a Russian Troll Campaign As an Experiment," *Wired*, June 12, 2019b. As of August 10, 2019:
https://www.wired.com/story/
jigsaw-russia-disinformation-social-media-stalin-alphabet/

Gricius, Gabriella, "How Russia's Disinformation Campaigns Are Succeeding in Europe," *Global Security Review*, May 11, 2019. As of August 12, 2019:
https://globalsecurityreview.com/
russia-disinformation-campaigns-succeeding-europe/

Grimmer, Justin, "Cyberwar: How Russian Hackers and Trolls Helped Elect a President—What We Don't, Can't, and Do Know," *Public Opinion Quarterly*, Vol. 83, No. 1, Spring 2019, pp. 159–163.

Grinyaev, S., "Views of U.S. Military Experts on the Conduct of Information Confrontation [Взгляды военных экспертов США на ведение информационного противоборства]," *Foreign Military Observer [Зарубежное военное обозрение]*, No. 8, August 1, 2001.

Grynko, Anastasiia, "Fake Narratives in Times of Presidential Elections: How Hybrid War Reshapes the Agenda of Ukrainian TV," StopFake, February 21, 2019. As of August 12, 2019:
https://www.stopfake.org/en/fake-narratives-in-times-of-presidential-elections-how-hybrid-war-reshapes-the-agenda-of-ukrainian-tv/

"Half of Russian Scientists Want to Emigrate," *UAWire*, June 30, 2018. As of August 12, 2019:
https://www.uawire.org/half-of-russian-scientists-want-to-emigrate

Hanlon, Bradley, "From Nord Stream to Novichok: Kremlin Propaganda on Google's Front Page," Alliance for Securing Democracy, June 14, 2018. As of August 12, 2019:
https://securingdemocracy.gmfus.org/from-nord-stream-to-novichok-kremlin-propaganda-on-googles-front-page/

Harding, Luke, "Russians 'Spread Fake Plot to Assassinate Boris Johnson' on Social Media," *The Guardian*, June 22, 2019. As of August 12, 2019:
https://www.theguardian.com/world/2019/jun/22/russians-spread-fake-plot-to-assassinate-boris-johnson

Harrington, David F., *Berlin on the Brink: The Blockade, the Airlift, and the Early Cold War*, Lexington, Ky.: University Press of Kentucky, 2012.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, RR-2237-OSD, 2018. As of October 22, 2020:
https://www.rand.org/pubs/research_reports/RR2237.html

Howard, Philip, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François, *The IRA, Social Media and Political Polarization in the United States, 2012–2018*, University of Oxford: Computational Research Project, December 2018. As of August 8, 2020:
https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf

Hulcoop, Adam, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, "Tainted Leaks: Disinformation and Phishing with a Russian Nexus," The Citizen Lab, University of Toronto, May 25, 2017. As of August 3, 2019:
https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

"Hungary Protests Ukrainian Military Moves, 'Death List' of Dual Citizens," Radio Free Europe/Radio Liberty, October 11, 2018. As of August 12, 2019:
https://www.rferl.org/a/hungarian-protests-ukrainian-military-moves-death-list-dual-citizens-ethnic-hungarian-minority/29537306.html

Hybrid CoE, "What Is Hybrid CoE?" webpage, undated. As of August 12, 2019:
https://www.hybridcoe.fi/what-is-hybridcoe/

Iasiello, Emilio J., "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters*, Vol. 47, No. 2, 2017, pp. 51–63.

Ignatius, David, "Russia's Radical New Strategy for Information Warfare," *Washington Post*, January 18, 2017.

———, "The U.S. Military Is Quietly Launching Efforts to Deter Russian Meddling," *Washington Post*, February 7, 2019.

Imeri, Dijedon, "Recent Twitter Activity Indicates Russian Plan to Destabilise Bosnia Ahead of General Election in October," *Jane's*, January 24, 2018. As of August 12, 2019:
https://janes.ihs.com/Janes/Display/FG_725892-IWR

"In Blagochavensk, They Say Goodbye to a Fallen Soldier [В Благовещенске Прощаются с Погибшим Военнослужащим]," Amurinfo, July 7, 2016. As of September 30, 2019:
https://www.amur.info/news/2016/07/07/113198

"In the Armed Forces They Are Creating a Force of Information Operations [В Вооруженных силах создают войска информационных операций]," *Independent Military Review [Независимое военное обозрение]*, May 16, 2014. As of January 28, 2019:
http://nvo.ng.ru/nvo/2014-05-16/2_red.html

"In the Footsteps of the GRU Officers. New Details in the 'Case of Russian Hackers' [По следам офицеров ГРУ. Новые детали в «деле русских хакеров»]," Radio Svoboda [Радио Свобода], July 17, 2018. As of August 9, 2019:
https://www.svoboda.org/a/29372280.html

"Information Confrontation Was Worked Out at 'Caucasus 2016' [Информационное противоборство отработали на «Кавказе-2016»]," *Izvestiya [Известия]*, September 14, 2016. As of January 28, 2019:
https://iz.ru/news/632393

"Information Wars [Информационные войны]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 5, 2015, pp. 100–112.

InformNapalm, "InformNapalm International Volunteer Community" webpage, undated. As of August 12, 2019:
http://informnapalm.rocks/

Innes, Martin, "Russian Influence and Interference Measures Following the 2017 UK Terrorist Attacks," Cardiff University, Crime and Security Research Institute, December 18, 2017. As of August 12, 2019:
https://www.cardiff.ac.uk/news/view/1037714-russian-influence-and-interference-measures-following-the-2017-uk-terrorist-attacks

Interfax-Ukraine, "Two Die in Rallies Outside Crimean Parliament, Says Ex-Head of Mejlis," *Kyiv Post*, February 26, 2014. As of August 12, 2019:
https://www.kyivpost.com/article/content/euromaidan/two-die-in-rallies-outside-crimean-parliament-says-ex-head-of-mejlis-337708.html

———, "Parubiy Signs Resolution on Sanctions Against 112 Ukraine, NewsOne Channels," *Kyiv Post*, October 20, 2018. As of August 12, 2019:
https://www.kyivpost.com/ukraine-politics/parubiy-signs-resolution-on-sanctions-against-112-ukraine-newsone-channels.html

International Strategic Action Network for Security, *Coercion to "Integration": Russia's Creeping Assault on the Sovereignty of Belarus*, Warsaw, Poland, February 2019.

Ioffe, Julia, "What Russia's Latest Protests Mean for Putin," *The Atlantic*, March 27, 2017. As of August 12, 2019:
https://www.theatlantic.com/international/archive/2017/03/navalny-protests-russia-putin/520878/

IREX, "Learn to Discern (L2D)—Media Literacy Training," webpage, undated. As of August 12, 2019:
https://www.irex.org/project/learn-discern-l2d-media-literacy-training

Isikoff, Michael, "Exclusive: The True Origins of the Seth Rich Conspiracy Theory," Yahoo News, July 9, 2019. As of August 10, 2019:
https://news.yahoo.com/exclusive-the-true-origins-of-the-seth-rich-conspiracy-a-yahoo-news-investigation-100000831.html

Ivannikov, Oleg Vladimirovich, *The Complex Character of Information Warfare in the Caucasus: A Social-Philosophical Perspective [Комплексный характер информационной войны на Кавказе: Социально-философские аспекты]*, dissertation, Rostov-on-Don, Russia: Southern Federal University [Южный Федеральный Университет], July 3, 2008. As of August 9, 2019:
https://dlib.rsl.ru/viewer/01003172912#?page=1

Jankowicz, Nina, "How the U.S. Can Fight Russian Disinformation for Real," Atlantic Council blog post, July 11, 2019. As of August 12, 2019:
https://www.atlanticcouncil.org/blogs/ukrainealert/how-the-us-can-fight-russian-disinformation-for-real

Jasper, Scott, "Russia's Ultimate Weapon Might Be Cyber," *The National Interest*, January 28, 2018. As of August 9, 2019:
https://nationalinterest.org/blog/the-buzz/russias-ultimate-weapon-might-be-cyber-24255

Jensen, Donald N., "Russia in the Middle East: A New Front in the Information War?" Jamestown Foundation, December 20, 2017. As of August 12, 2019:
https://jamestown.org/program/russia-middle-east-new-front-information/

"Jessikka Aro: How Pro-Russian Trolls Tried to Destroy Me," BBC, October 6, 2017. As of August 12, 2019:
https://www.bbc.com/news/blogs-trending-41499789

Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, Washington, D.C., November 27, 2012, incorporating change 1, November 20, 2014. As of August 8, 2019:
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Jones, Seth, *Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare*, Washington, D.C.: Center for Strategic and International Studies, CSIS Brief, October 1, 2018. As of August 12, 2019:
https://www.csis.org/analysis/
going-offensive-us-strategy-combat-russian-information-warfare

Jowett, Garth S., and Victoria O'Donnell, *Propaganda and Persuasion*, Thousand Oaks, Calif.: Sage Publications Inc., 2012.

Kamp, Karl-Heinz, *Russia's Myths About NATO: Moscow's Propaganda Ahead of the NATO Summit*, Berlin, Germany: Federal Academy for Security Policy, Working Paper No. 15/2016, 2016. As of August 12, 2019:
https://www.baks.bund.de/sites/baks010/files/working_paper_15_2016.pdf

Kapustin, Igor, "Gypsies in Pentagon's Employ, [Цыгане на службе Пентагона]," *Red Star [Красная Звезда]*, September 20, 2006. As of August 9, 2019:
http://old.redstar.ru/2006/09/20_09/3_03.html

Kartapolov, A. V., "Lessons of Military Conflicts and Prospects for the Development of Means and Methods of Conducting Them. Direct and Indirect Actions in Contemporary International Conflicts [Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах]," *Bulletin of the Academy of Military Science [Вестник Академии Военных Наук]*, No. 2, 2015.

Kartapolov, Andrey, and Oleg Falichev, "The Army Should Be Spiritual [Армия должна быть духовой]," *Defense and Security [Защита и безопасность]*, No. 4, 2018, pp. 26–28.

King, Esther, "Russian Hackers Targeting Germany: Intelligence Chief," Politico, November 29, 2016.

Kirk, Michael, "Andrei Soldatov, Co-Author of *The Red Web*," Frontline, July 25, 2017. As of August 12, 2019:
https://www.pbs.org/wgbh/frontline/interview/andrei-soldatov/

"KL Calculated the Average Cost of Custom DDoS-Attacks [ЛК подсчитала среднюю стоимость заказной DDoS-атаки]," SecurityLab, March 24, 2017. As of August 12, 2019:
https://www.securitylab.ru/news/485665.php

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Santa Monica, Calif.: RAND Corporation, RR-1498-A, 2017. As of October 12, 2019:
https://www.rand.org/pubs/research_reports/RR1498.html

Kolesnikov, A. I. "Vladimir Putin Was Not at a Loss for Words Regarding His Friend [Владимир Путин за другом в карман не полез]," *Kommersant [Коммерсантъ]*, Vol. 60, April 8, 2016, p. 3. As of October 12, 2019:
https://www.kommersant.ru/doc/2957597

Kolesov, P., "Georgia's Information War Against South Ossetia and Abkhazia [Информационная война Грузии против Южной Осетии и Абхазии]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 10, October 2008, pp. 18–21.

Kolpakidi, Alexander I., and Dmitry P. Prokhorov, "Military Intelligence and the Epoch of Détente [Военная разведка и эпоха разрядки]," Militera.lib.ru, undated. As of August 9, 2019:
http://militera.lib.ru/research/kolpakidi_prohorov1/11.html

Kondrashov, Vyacheslav Viktorovich, "Information Confrontation in the Cybernetic Space [Информационное противоборство в кибернетическом пространстве]," *Scientific-Research Center of Problems of National Security [Научно-исследовательский центр проблем национальной безопасности]*, August 22, 2016. As of August 9, 2019:
http://nic-pnb.ru/analytics/informatsionnoe-protivoborstvo-v-kiberneticheskom-prostranstve/

Kovacs, Eduard, "Russian Cyberspies Shift Focus from NATO Countries to Asia," *Security Week*, February 20, 2018. As of August 9, 2019:
https://www.securityweek.com/russian-cyberspies-shift-focus-nato-countries-asia

Kovalev, Alexey, and Matthew Bodner, "The Secrets of Russia's Propaganda War, Revealed," *Moscow Times*, March 1, 2017. As of August 8, 2019:
https://www.themoscowtimes.com/2017/03/01/welcome-to-russian-psychological-warfare-operations-101-a57301

Kramer, Andrew E., "How Russia Recruited Elite Hackers for Its Cyberwar," *New York Times*, December 29, 2016.

———, "Russia Deploys a Potent Weapon in Syria: The Profit Motive," *New York Times*, July 5, 2017.

———, "Russian General Pitches 'Information Operations as a Form of War," *New York Times*, March 2, 2019. As of August 12, 2019:
https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html

"The Kremlin Apologizes to the German Newspaper Süddeutsche Zeitung for Yesterday's Words of Vladimir's Putin [Кремль извиняется перед немецкой газетой 'Зюддойче цайтунг' за вчерашние слова президента Владимира Путина]," *Echo of Moscow [Эхо Москв]*, April 15, 2016. As of October 12, 2019:
https://echo.msk.ru/news/1748422-echo.html

Kremlin Watch Team, *2018 Ranking of Countermeasures by the EU28 to the Kremlin's Subversion Operations*, Prague, Czechoslovakia: European Values Center for Security Policy, June 13, 2018. As of August 12, 2019:
https://www.kremlinwatch.eu/userfiles/2018-ranking-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations.pdf

Krikunov, A., "Cyberspace of Leading States in the Context of Modern Challenges and Threats [Киберпространство ведущих государств в контексте современных вызовов и угроз]," *Naval Digest [Морской сборник]*, No. 11, 2011.

Krysko, Vladimir Gavrilovich, *The Secrets of Psychological War (Goals, Tasks, Methods, Forms, and Experience) [Секреты психологической войны (цели, задачи, методы, формы, опыт)]*, Minsk, Belarus: Main Intelligence Directorate [Главное разведывательное управление], 1999. As of August 8, 2019: https://royallib.com/book/krisko_vladimir/sekreti_psihologicheskoy_voyni_tseli_zadachi_metodi_formi_opit.html

Kudryashov, A., "Use Abroad of Internet Networks in the Interests of Conducting Information Wars [Исползование за Рубежом Сети Интернет в Интересах Ведения Информационных Войн]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 4, 2011.

Kulakov, V. F., "Moral-Psychological Support of the Counter-Terrorist Operation in the Republic of Dagestan [Морально-психологическое обеспечение контртеррористической операции в Республики Дагестан]," *Military Thought [Военная мысль]*, No. 1, January 1, 2000.

Kuzmin, V., "U.S. Role in Implementing 'Color Revolutions' in Foreign Countries [Роль США в осуществлении «цветных революций» в зарубежных странах]," *Foreign Military Review [Зарубежное военное обозрени]*, No. 9, September 2008, pp. 9–18.

Laity, Mark, "Chief Strategic Communications at SHAPE: 'Perception Becomes Reality,'" presentation, October 2014.

Lapowsky, Issie, "Facebook May Have More Russian Troll Farms to Worry About," *Wired*, September 8, 2017. As of August 10, 2019: https://www.wired.com/story/facebook-may-have-more-russian-troll-farms-to-worry-about/

———, "NATO Group Catfished Soldiers to Prove a Point About Privacy," *Wired*, February 18, 2019. As of August 12, 2019: https://www.wired.com/story/nato-stratcom-catfished-soldiers-social-media/

Latsinskaya, Maria, Aleksandr Braterskiy, and Ignat Kalinin, "Russia Introduced a Force to the Internet [Россия ввела войска в интернет]," Gazeta.ru, February 22, 2017. As of August 9, 2019: https://www.gazeta.ru/tech/2017/02/22_a_10539719.shtml

"Latvia Shuts Down Sputnik Propaganda Website," Latvian Public Broadcasting, March 29, 2016. As of November 6, 2018: https://eng.lsm.lv/article/Society/society/latvia-shuts-down-sputnik-propaganda-website.a175627/

Lesaca, Javier, "Why Did Russian Social Media Swarm the Digital Conversation About Catalan Independence?" *Washington Post*, November 22, 2017. As of August 12, 2019:
https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/

Lewandowsky, Stephan, Ullrich K. H. Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook, "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest*, Vol. 13, No. 3, 2012, pp. 106–131. As of August 12, 2019:
https://journals.sagepub.com/doi/full/10.1177/1529100612451018

Lin, Herb, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," *Lawfare,* blog post, September 6, 2018. As of August 12, 2019:
https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations

Linvill, Darren L., and Patrick Warren, "Russian Trolls Can Be Surprisingly Subtle, and Often Fun to Read," *Washington Post*, September 10, 2018.

Lister, Tim, and Clare Sebastian, "Stoking Islamophobia and Secession in Texas—from an Office in Russia," CNN, October 6, 2017. As of August 12, 2019:
https://www.cnn.com/2017/10/05/politics/heart-of-texas-russia-event/index.html

Litovkin, Nikolai, "Russia's Cyber Army Hacks a Spot in the Top 5," *Russia Beyond the Headlines*, January 12, 2017. As of August 10, 2019:
https://www.rbth.com/defence/2017/01/12/russias-cyber-army-hacks-a-spot-in-the-top-5_679221

Livingston, Steven, "Disinformation Campaigns Target Tech-Enabled Citizen Journalists," Brookings Institution, March 2, 2017. As of August 12, 2019:
https://www.brookings.edu/blog/techtank/2017/03/02/disinformation-campaigns-target-tech-enabled-citizen-journalists/

Loveluck, Louisa, "Russian Disinformation Campaign Targets Syria's Beleaguered Rescue Workers," *Washington Post*, December 18, 2018.

Lucas, Edward, and Peter Pomerantsev, *Winning the Information War: Techniques and Counter-Strategies to Russian Propaganda in Central and Eastern Europe*, Washington, D.C.: Center for European Policy Analysis, August 2016. As of August 12, 2019:
https://cepa.ecms.pl/files/?id_plik=2715

Luzin, Pavel, "How Successful Is Russia's Military Propaganda Media?" *Moscow Times*, July 10, 2019. As of August 10, 2019:
https://www.themoscowtimes.com/2019/07/10/how-successful-russias-military-propaganda-media-a66337

Lysenko, Yakov, "Terrorists Used Telegram [Террористы использовали Telegram]," Gazeta.Ru, April 27, 2018. As of August 12, 2019: https://www.gazeta.ru/social/2018/04/27/11732455.shtml

MacAskill, Ewen, "British Army Creates Team of Facebook Warriors," *The Guardian*, January 31, 2015. As of August 12, 2019: https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade

MacFarquhar, Neil, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, August 28, 2016.

———, "Inside the Russian Troll Factory: Zombies and a Breakneck Pace," *New York Times*, February 18, 2018.

———, "Reporter's Arrest Sets Off Widespread Protests in Russia," *New York Times*, June 10, 2019.

Mackintosh, Eliza, "Finland Is Winning the War on Fake News. What It's Learned May Be Crucial to Western Democracy," CNN, May 2019. As of August 12, 2019: https://www.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

Makarenko, S. I., *Information Confrontation and Electronic Warfare in Net-Centric Wars of the Beginning of the XXI Century, [Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века]*, St. Petersburg, Russia: Knowledge-Intensive Technology [Наукоемкие технологии], 2017.

Makarov, Dmitriy, " Information Wars. A Word, Placed Under the Gun [Информационные Войны. Слово, Поставленное под Ружье]," *Flag of the Motherland [Флаг Родины]*, No. 115, 2009.

Martineau, Paris, "How Instagram Became the Russian IRA's Go-To Social Network," *Wired*, December 17, 2018. As of August 10, 2019: https://www.wired.com/story/how-instagram-became-russian-iras-social-network/

Matthews, Miriam, Alyssa Demus, Elina Treyger, Marek N. Posard, Hilary Reininger, and Christopher Paul, *Understanding and Defending Against Russia's Malign and Subversive Information Efforts in Europe*, Santa Monica, Calif.: RAND Corporation, RR-3160-EUCOM, 2021. As of December 31, 2021: https://www.rand.org/pubs/research_reports/RR3160.html

McKirdy, Euan, "Putin: 'Patriotic Russian Hackers May Have Targeted U.S. Election," CNN, June 2, 2017. As of August 10, 2019: https://www.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html

"Medvedev Named the 'Export of Intellect' from Russia as Unacceptable [Медведев назвал недопустимым «экспорт интеллекта» из России]," *RBC [РБК]*, February 27, 2017. As of August 12, 2019: https://www.rbc.ru/rbcfreenews/58b41aec9a7947ea101ed916

Meister, Stefan, "The 'Lisa Case:' Germany as a Target of Russian Disinformation," *NATO Review Magazine*, 2016. As of August 12, 2019: https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm

Menn, Joseph, "Exclusive: Russia Used Facebook to Try to Spy on Macron Campaign—Sources," Reuters, July 27, 2017. As of August 12, 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

Mettsel, Mikhail, "An Accomplice to the Founder of Russia's 'Troll Factory' Says the Organization Was Created Without Kremlin Instructions," *Meduza*, November 8, 2018. As of August 10, 2019: https://meduza.io/en/feature/2018/11/09/an-accomplice-to-the-founder-of-the-troll-factory-comes-forward-and-says-russia-s-u-s-election-interference-wasn-t-a-kremlin-initiative

"MH17—Russian GRU Commander 'Orion' Identified as Oleg Ivannikov," Bellingcat, May 25, 2018. As of October 7, 2019: https://www.bellingcat.com/news/uk-and-europe/2018/05/25/mh17-russian-gru-commander-orion-identified-oleg-ivannikov/

Mikhaleva, Elena, " Georgiy Shakhnazarov: Russia and Her Army Should Be Ready for Computer, Information, and Ecological Wars . . . [Георгий Шахназаров: 'Россия и ее армия должны быть готовы к компьютерным, информационным, экологическим войнам . . .']," *At the Fighting Post [На боевом посту]*, No. 29, April 9, 1997.

Mikryukov, Vasiliy, "Victory in War Should Be Achieved Even Before the First Shot [Победа в войне должна быть достигнута еще до первого выстрела]," *Independent Military Review [Независимое военное обозрение]*, January 15, 2016. As of August 8, 2019: http://nvo.ng.ru/concepts/2016-01-15/10_infowar.html

"Military Sites at the Festival for Author's Song [Военные площадки на фестивалях авторской песни]," Desantura.Ru, undated. As of August 12, 2019: http://desantura.ru/forum/forum43/topic12205/

Miller, Carl, "Inside the British Army's Secret Information Warfare Machine," *Wired*, November 14, 2018. As of August 12, 2019: https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military

"Minister of Defense of the Russian Federation Created Troops for Information Operations [В Минобороны РФ создали войска информационных операций]," *Interfax [Интерфакс]*, February 22, 2017. As of August 9, 2019: https://www.interfax.ru/russia/551054

Ministry of Defense of the Russian Federation, "Information Warfare [Informatsionnoe protivoborstvo]," *Military-Encyclopedic Dictionary of the Ministry of Defense*, undated. As of December 17, 2019:
https://encyclopedia.mil.ru/encyclopedia/dictionary/list.htm

Ministry of Information Policy of Ukraine, "About Ministry," webpage, undated. As of August 12, 2019:
https://mip.gov.ua/en/content/pro-ministerstvo.html

Mironenko, Peter, and Anastasia Yakoreva, "Cryptographers from Military Units: What We Know About the Accused Russian Hackers," *The Bell*, July 14, 2018. As of August 12, 2019:
https://thebell.io/en/cryptographers-from-military-units-what-we-know-about-the-accused-russian-hackers/

Modderkolk, Huib, "Dutch Agencies Provide Crucial Intel About Russia's Interference in US-Elections," *de Volksrant*, January 25, 2018.

Modestov, Sergey, "The U.S. Is Ready for an Information War with Russia [США готовы к информационной войне с Россией]," *Independent Military Review [Независимое военное обозрение]*, No. 25, July 12, 1997.

Modestov, Sergey, and Sergey Sokut, "Bytes in Place of Bullets [Байты вместо пуль]," *Independent Military Review [Независимое военное обозрение]*, No. 13, April 9, 1999.

Moscow Project, "Russia's Three Intelligence Agencies, Explained," October 12, 2018. As of August 10, 2019:
https://themoscowproject.org/explainers/russias-three-intelligence-agencies-explained/

Moscow-Russia.ru, "Military University of the Ministry of Defense of the Russian Federation [Войнный университет министерсвта обороны Российской Федерации]," webpage, 2019. As of August 12, 2019:
http://moscow-russia.ru/voennyy-universitet-ministerstva-oborony/

Mueller, Robert S., III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Vol. I, Washington, D.C.: U.S. Department of Justice, March 2019. As of August 12, 2019:
https://www.cnn.com/2019/04/18/politics/full-mueller-report-pdf/index.html

Mukhin, Vladimir, "Bet on an Informational Spetsnaz [Ставка на информационный спецназ]," *Independent Newspaper [Независимая Газета]*, No. 14, April 17, 2015. As of August 12, 2019:
https://nvo.ng.ru/nvo/2015-04-17/1_specnaz.html

Municipal Information Library System of Volzhskiy [Муниципальная Информационная Библиотечная Система г. Волжский], "Kondrashov Vyacheslav Viktorovich [Кондрашов Вячеслав Викторович]," webpage, February 21, 2018. As of August 9, 2019: http://www.mibs-vlz.ru/volzhane-v-interere-strani/kondrashov-vyacheslav-viktorovich

Myers, Jolie, "Meet The Activist Who Uncovered the Russian Troll Factory Named in the Mueller Probe," NPR, March 15, 2018. As of August 10, 2019: https://www.npr.org/sections/parallels/2018/03/15/594062887/some-russians-see-u-s-investigation-into-russian-election-meddling-as-a-soap-ope

Nakashima, Ellen, "U.S. Identifies Russian Government Hackers Who Accessed DNC Computers," *Washington Post*, November 3, 2017a.

———, "Inside a Russian Disinformation Campaign in Ukraine in 2014," *Washington Post*, December 25, 2017b.

———, "U.S. Cyber Command operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019.

National Cyber Security Centre, "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed," October 3, 2018. As of August 10, 2019: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

NATO StratCom CoE—*See* NATO Strategic Communications Centre of Excellence.

NATO Strategic Communications Centre of Excellence, "About Strategic Communications," webpage, undated. As of August 12, 2019: https://www.stratcomcoe.org/about-strategic-communications

"Navalny Video Accusing Medvedev of Corruption Posted on Government Websites," Radio Free Europe/Radio Liberty, June 11, 2017. As of August 12, 2019: https://www.rferl.org/a/navalny-video-medvedev-corruption-posted-goverment-websites/28541102.html

Nechaev, Anton, "State Duma Proposed to Legislate Who Should be Responsible for the Moral and Political State of the Military [Госдуме предложили узаконить, кто должен отвечать за морально-политическое состояние военных]," *Infokam [Инфокам]*, March 5, 2019. As of August 12, 2019: https://infokam.su/n36277.html

Nesmeyanov, Vladimir, "Can We Defend the Great Victory? [Сумеем ли Защитить Великую Победу?]," *Flag of the Motherland [Флаг Родины]*, No. 60, 2013.

———, "This Quiet, Deadly War [Эта тихая смертельная война]," *Flag of the Motherland [Флаг Родины]*, No. 10, March 10, 2017.

Newman, Lily Hay, "Russia's Elite Hackers May Have New Phishing Tricks," Wired, November 20, 2018. As of August 12, 2019: https://www.wired.com/story/russia-fancy-bear-hackers-phishing/

Nimmo, Ben, "Putin Sets His Disinformation Trolls on the MH 17 Investigators," *Newsweek*, September 28, 2016. As of August 12, 2019: https://www.newsweek.com/putin-sets-his-disinformation-trolls-mh17-investigators-503578

———, "Russian Narratives on NATO's Deployment," StopFake, April 2, 2017. As of August 12, 2019: https://www.stopfake.org/en/russian-narratives-on-nato-s-deployment/

———, "How MH17 Gave Birth to the Modern Russian Spin Machine," *Foreign Policy*, September 29, 2018. As of August 12, 2019: https://foreignpolicy.com/2016/09/29/how-mh17-gave-birth-to-the-modern-russian-spin-machine-putin-ukraine/

North Atlantic Treaty Organization, "Allied Intelligence Chiefs Discuss Countering Cyber-Attacks, Disinformation," November 29, 2018. As of August 12, 2019: https://www.nato.int/cps/en/natohq/news_161119.htm?selectedLocale=en

———, "NATO-Russia, Setting the Record Straight," August 5, 2019. As of August 12, 2019: https://www.nato.int/cps/en/natohq/115204.htm

Nossiter, Adam, David E. Sanger, and Nicole Perlroth, "Hackers Came, but the French Were Prepared," *New York Times*, May 9, 2017.

Novik, Aleksandr, "Weapons of the Future, British Style [Оружие будущего по-британски]," *Baltic Guard [Страж Балтики]*, No. 2, January 18, 2019.

Novikov, Mikhail, and Vyacheslav Ovchinnikov, "Information Confrontation in Contemporary Geopolitics [Информационное Противоборство в Современной Геополитике]," *Defense and Security [Защита и Безопасность]*, No. 2, 2011.

Novorus, homepage, undated. As of October 12, 2019: https://novorus.info

novorossia.ru, homepage, undated (website no longer active).

O'Brien, Luke, "The Making of an American Nazi," *The Atlantic*, December 2017. As of August 12, 2019: https://www.theatlantic.com/magazine/archive/2017/12/the-making-of-an-american-nazi/544119/

ODNI—*See* Office of the Director of National Intelligence.

Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, Washington, D.C., January 6, 2017. As of October 12, 2020: https://www.dni.gov/files/documents/ICA_2017_01.pdf

Oliker, Olga, "Russia's New Military Doctrine: Same as the Old Doctrine, Mostly," *Washington Post*, January 15, 2015.

Oliker, Olga, Lynn E. Davis, Keith Crane, Andrew Radin, Celeste Gventer, Susanne Sondergaard, James T. Quinlivan, Stephan B. Seabrook, Jacopo Bellasio, Bryan Frederick, Andriy Bega, and Jakub P. Hlavka, *Security Sector Reform in Ukraine*, RR-1475-1-UIA, Santa Monica, Calif.: RAND Corporation, 2016. As of October 24, 2020: https://www.rand.org/pubs/research_reports/RR1475-1.html

Orlov, S., "The Role of Social Networks in the Organization of Protest Populations of the Population in the Course of the 'Arab Spring' [Роль социальных сетей в организации протестных выступленний населения в ходе «Арабской весны»]," *Foreign Military Review [Зарубежное военное обозреине]*, No. 12, December 2014, pp. 51–54.

Orttung, Robert, Elizabeth Nelson, and Anthony Livshen, "How Russia Today Is Using YouTube," *Washington Post*, March 23, 2015.

Osborne, Charlie, "Fancy Bear Exploits Brexit to Target Government Groups with Zebrocy Trojan," Zero Day, December 14, 2018. As of August 12, 2019: https://www.zdnet.com/article/fancy-bear-exploits-brexit-to-target-government-groups-with-zebrocy-trojan/

Ostrovsky, E. O., and A. S. Sizov, "The Approach to Modeling the Cognitive Sphere of Operational Intelligence Objects [Подход к моделированию когнитивной сферы объектов оперативной разведки]," *Military Thought [Военная мысль]*, No. 2, February 2016, pp. 48–57.

O'Sullivan, Donie, "When Seeing Is No Longer Believing: Inside the Pentagon's Race Against Deepfake Videos," CNN, January 28, 2019. As of August 12, 2019: https://www.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/

O'Sullivan, Donie, Drew Griffin, Curt Devine, and Atika Shubert, "Russia Is Backing a Viral Video Company Aimed at American Millennials," CNN Business, February 18, 2019. As of August 10, 2019: https://www.cnn.com/2019/02/15/tech/russia-facebook-viral-videos/index.html

Paganini, Pierluigi, *ISIS Cyber Capabilities*, Madison, Wisc.: Infosec Institute, May 9, 2016. As of September 30, 2019: https://resources.infosecinstitute.com/isis-cyber-capabilities/#gref

Panarin, Igor, "'Trojan Horse' of the 21st Century. Informational Arms: Realities and Possibilities ['Троянский конь' XXI века. Информационное оружие: реалии и возможности]," *Red Star [Красная звезда]*, No. 282, August 12, 1995.

Parkinson, Joe, and Georgi Kantchev, "Document: Russia Uses Rigged Polls, Fake News to Sway Foreign Elections," *Wall Street Journal*, March 23, 2017.

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 August 12, 2019: https://www.rand.org/pubs/perspectives/PE198.html

Peck, Michael, "The Russian Military's Worst Enemy (HINT: Not America)," *The National Interest*, April 27, 2019. As of August 12, 2019: https://nationalinterest.org/blog/buzz/russian-militarys-worst-enemy-hint-not-america-54307

Peisakhin, Leonid, and Arturas Rozenas, "Electoral Effects of Biased Media: Russian Television in Ukraine," *American Journal of Political Science*, Vol. 62, No. 3, 2018, pp. 535–550.

Pesonen, Ari "Russian Psychological Warfare Units Were Created in the Reform of the Armed Forces [Venäjän psykologisen sodankäynnin yksiköt luotiin puolustusvoimauudistuksessa]," *New Finland [Uusi Suomi]*, March 1, 2018. As of August 9, 2019: http://aripesonen1.puheenvuoro.uusisuomi.fi/251571-venajan-psykologisen-sodankaynnin-yksikot-luotiin-puolustusvoimauudistuksessa

Plackett, Benjamin, "Russian Spam Accounts Are Still a Big Problem for Reddit," Engadget, April 2, 2019. As of August 12, 2019: https://www.engadget.com/2019/02/04/russia-spam-account-problem-reddit-propaganda/

Podoprigora, Boris, "Third World [War]—Informational? [Третья мировая—информационная?]," *Navy Newspaper [Морская газета]*, No. 39–40, 2011.

"Police Open Criminal Case over Provocative Anti-Hungarian Billboards in Zakarpattia Region," *Unian*, October 22, 2018. As of August 12, 2019: https://www.unian.info/society/10306989-police-open-criminal-case-over-provocative-anti-hungarian-billboards-in-zakarpattia-region.html

Polskikh, A., " General Military Problems. On the Application of the Global Computing Network Internet in the Interest of Information Confrontation [Общие военные проблемы. О применении глобальной компьютерной сети интернет в интересах информационного противоборства]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 7, July 31, 2005.

Polyakova, Alina, and Spencer P. Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Washington, D.C.: Brookings Institution, March 2018. As of August 12, 2019: https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf

Pomerantsev, Peter, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*, New York: PublicAffairs, 2015.

Pomerantsev, Peter, and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money: A Special Report Presented by the Interpreter, a Project of the Institute of Modern Russia*, New York: Institute of Modern Russia, 2014. As of August 9, 2019: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf

Ponomaryova, Alya, "Humpty-Dumpty Under the 'Cover' of the FSB [Шалтай-Болтай под «крышей» ФСБ]," Radio Svoboda [Радио Свобода], January 26, 2017. As of August 12, 2019: https://www.svoboda.org/a/28260556.html

Popovych, Nataliia, and Oleksiy Makhuhin, "Countering Disinformation: Some Lessons Learnt by Ukraine Crisis Media Center," Ukraine Crisis Media Center, April 20, 2018. As of August 12, 2019: http://uacrisis.org/66275-countering-disinformation-lessons-learnt

Potapov, V., *The Activity of Joint Formations and Units of Ground Forces in Conducting Special Operations to Disarm Illegal Groups in 1994–96 in the Chechen Republic [Действия соединений, частей и подразделений СВ при проведении специальной операции по разоружению НВФ в 1994-96 гг. на территории Чеченской республики]*, report to the South-Caucasus Military District, undated. As of August 9, 2019: http://textarchive.ru/c-1943769-pall.html

Poulsen, Kevin, "This Hacker Party Is Ground Zero for Russia's Cyberspies," *Daily Beast*, August 4, 2018. As of August 12, 2019: https://www.thedailybeast.com/this-hacker-party-is-ground-zero-for-russias-cyberspies-3?ref=scroll

Priest, Dana, and Michael Birnbaum, "Europe Has Been Working to Expose Russian Meddling for Years," *Washington Post*, June 25, 2017.

"Proposal to Triple Financing of Mass Media [Финансирование СМИ из бюджета предложено увеличить на треть]," *Interfax*, September 26, 2019. As of January 8, 2020: https://www.interfax.ru/russia/678102

Pushkarev, Nikolay, "The Activities of Military Intelligence During the Fall of the Soviet Union [Деятельность военной разведки в период Распада СССР]," *GRU: Inventions and Reality [ГРУ: вымыслы и реальность]*,Moscow: Eksmo [Эксмо], 2004. As of January 28, 2019: https://public.wikireading.ru/75444

Putin, Vladimir, "'Soldier' Is an Honorable and Respected Rank [Солдат есть звание высокое и почетное]," excerpts from the annual address to the Federal Assembly of the Russian Federation, *Red Star [Красная звезда]*, May 11, 2006. As of August 8, 2019: http://old.redstar.ru/2006/05/11_05/1_01.html

"Putin-Linked Think Tank Drew up Plan to Sway 2016 U.S. Election—Documents," Reuters, April 19, 2017. As of August 9, 2019: https://www.reuters.com/article/us-usa-russia-election-exclusive/putin-linked-think-tank-drew-up-plan-to-sway-2016-us-election-documents-idUSKBN17L2N3

"Putin's Propagandists Filmed a New Fake in the Donbas: Details from Intelligence [Пропагандисты Путина отсняли на Донбассе новый фейк: подробности от разведки]," Online.ua, July 29, 2016. As of August 9, 2019: https://news.online.ua/748764/propagandisty-putina-otsnyali-na-donbasse-novyy-feyk-podrobnosti-ot-razvedki/

Reisinger, William M., Marina Zaloznaya, and Vicki L. Hesli Claypool, "Does Everyday Corruption Affect How Russians View Their Political Leadership?" *Post-Soviet Affairs*, Vol. 33, No. 4, 2017, pp. 255–275.

Reynolds, Anna, ed., *Social Media as a Tool of Hybrid Warfare*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, May 2016.

Riley, Michael, "Russian Hackers of DNC Said to Nab Secrets from NATO, Soros," Bloomberg, August 11, 2016.

Robinson, Linda, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, Santa Monica, Calif.: RAND Corporation, RR-1772-A, 2018. As of October 13, 2020: https://www.rand.org/pubs/research_reports/RR1772.html

Rogers, Michael S., testimony presented before the U.S. Senate Committee on Armed Services, Washington, D.C., March 19, 2015. As of August 12, 2019: https://fas.org/irp/congress/2015_hr/031915rogers.pdf

"Rogozin Urged to Stop the "Brain Drain" Abroad [Рогозин призвал остановить «вымывание мозгов» за рубеж]," *RBC [РБК]*, February 27, 2018. As of August 12, 2019: https://www.rbc.ru/rbcfreenews/5a9524119a794717e2d20506

Romashkina, N. P., and A. B. Koldobskiy, "New Methods of Confrontation in the XXI Century [Новые методы противоборства XXI века]," *Digest of the Academy of Military Sciences [Вестник Академии Военных Наук]*, No. 1, 2015, pp. 134–139.

Roonemaa, Holger, and Inga Springe, "This Is How Russian Propaganda Actually Works in the 21st Century," *BuzzFeed News*, August 31, 2018. As of August 9, 2019: https://www.buzzfeednews.com/article/holgerroonemaa/russia-propaganda-baltics-baltnews

Rosenberg, Matthew, Charlie Savage, and Michael Wines, "Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn," *New York Times*, February 13, 2018.

Rosenberger, Laura, "Foreign Influence Operations and Their Use of Social Media Platforms," Alliance for Securing Democracy, July 31, 2018. As of August 12, 2019: https://securingdemocracy.gmfus.org/foreign-influence-operations-and-their-use-of-social-media-platforms

"Roskomnadzor Will Create a Public Registry of Fake-News Sources [Роскомнадзор создаст публичный реестр источников фейк-ньюс]," TASS, May 15, 2019. As of October 7, 2019: https://tass.ru/obschestvo/6433718

Ross, Brian, Megan Christie, and James Gordon Meek, "Behind #SyriaHoax and the Russian Propaganda Onslaught," ABC News, April 13, 2017. As of August 10, 2019: https://abcnews.go.com/International/analysts-identify-syriahoax-russian-fueled-propaganda/story?id=46787674

RT, "About RT," webpage, undated. As of October 7, 2019: https://www.rt.com/about-us/

"Russia Bans Smartphones for Soldiers over Social Media Fears," BBC, February 20, 2019. As of August 12, 2019: https://www.bbc.com/news/world-europe-47302938

"Russia Is Creating a Cyber-Force [Россия создает кибервойска]," *Military Review [Военное обозрение]*, August 8, 2013. As of January 28, 2019: https://topwar.ru/31668-rossiya-sozdaet-kibervoyska-stdailycom-kitay.html

"Russia-Ukraine Tensions Rise After Kerch Strait Ship Capture," BBC, November 26, 2018. As of August 12, 2019: https://www.bbc.com/news/world-europe-46340283

Russian Defense Ministry [Минобороны России], @mod_russia, Twitter account, undated. As of August 12, 2019: https://twitter.com/mod_russia

Russian Federation, Russian National Security Strategy, full-text translation, December 31, 2015. As of August 12, 2019:
http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

"Russian Marine Kills Ukraine Navy Officer in Crimea, Says Ministry," Reuters, April 7, 2014. As of August 12, 2019:
https://www.reuters.com/article/us-ukraine-crisis-military-idUSBREA360GB20140407

"The Russian Ministry of Defense Is Working on the Option of Creating Humanitarian Scientific Companies [Минобороны России прорабатывает вариант создания гуманитарных научных рот]," TASS, July 10, 2013.

"Russian Nation-State Hacking Unit's Tools Get More Fancy," Oodaloop, May 24, 2019. As of August 12, 2019:
https://www.oodaloop.com/briefs/2019/05/24/russian-nation-state-hacking-units-tools-get-more-fancy/

"The Russian Offensive in Syria You Haven't Heard About," .coda, November 28, 2017. As of August 12, 2019:
https://codastory.com/disinformation/armed-conflict/the-russian-offensive-in-syria-you-haven-t-heard-about/

Rutenberg, Jim, "RT, Sputnik and Russia's New Theory of War," *New York Times*, September 13, 2017.

Salvo, David, and Bradley Hanlon, "Key Takeaways from the Kremlin's Recent Interference Offensive," Alliance for Securing Democracy, October 11, 2018. As of August 12, 2019:
https://securingdemocracy.gmfus.org/key-takeaways-from-the-kremlins-recent-interference-offensive/

Sarts, Janis, "Russian Interference in European Elections," testimony presented before the U.S. Senate Select Committee on Intelligence, June 28, 2017. As of August 12, 2019:
https://www.intelligence.senate.gov/sites/default/files/documents/sfr-jsarts-062817b.pdf

Satariano, Adam, "Facebook Identifies Russia-Linked Misinformation Campaign," *New York Times*, January 17, 2019.

Satter, Raphael, "Russian Hackers Who Posed as ISIS Militants Threatened Military Wives," Talking Points Memo, May 8, 2018. As of August 9, 2019:
https://talkingpointsmemo.com/news/russian-hackers-isis-militant-posers-military-wives-threat

Schafer, Bret, *View from the Digital Trenches—Lessons from Year One of Hamilton 68*, Washington, D.C.: The German Marshall Fund of the United States, November 19, 2018.

Schindler, John R., "False Flags: The Kremlin's Hidden Cyber Hand," *Observer*, June 18, 2016. As of August 10, 2019:
https://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/

Schmidt, Michael S., and Helene Cooper, "ISIS Urges Sympathizers to Kill U.S. Service Members It Identifies," *New York Times*, March 21, 2015.

Schreckinger, Ben, "How Russia Targets the U.S. Military," *Politico Magazine*, June 12, 2017. As of August 10, 2019:
https://www.politico.com/magazine/story/2017/06/12/how-russia-targets-the-us-military-215247

Schwirtz, Michael, "German Election Mystery: Why No Russian Meddling?" *New York Times*, September 21, 2017.

Schwirtz, Michael, and Sheera Frenkel, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering," *New York Times*, March 29, 2019.

Seldin, Jeff, "Russia Influence Operations Taking Aim at U.S. Military," *Voice of America*, November 2, 2018. As of August 12, 2019:
https://www.voanews.com/a/russia-influence-operations-taking-aim-at-us-military/4640751.html

Selhorst, Tony, "Russia's Perception Warfare: The Development of Gerasimov's Doctrine in Estonia and Georgia and Its Application in Ukraine," *Militaire Spectator*, Vol. 185, No. 4, 2016. As of August 8, 2019:
https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire%20Spectator%204-2016%20Selhorst.pdf

Semenov, D., "The Role of Disinformation in Information Confrontation of the Parties in the Syrian Conflict [Роль Дезинформации в информационном противостоянии сторон в сирийском конфликте]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 12, December 2014, pp. 38–42.

Sen, Ashish Kumar, "The Importance of Working Together in the Fight Against Disinformation," Atlantic Council, June 20, 2019. As of August 12, 2019:
https://www.atlanticcouncil.org/blogs/new-atlanticist/the-importance-of-working-together-in-the-fight-against-disinformation

Serov, A., "About the Role of Disinformation in Modern Conflicts and Wars [О роли дезинформации в современных конфликтах и войнах]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 8, 2011.

Sexhauer, Amy, Victor Mckenzie, Shari Smith, and Philip Kautz, "Optimizing Indirect MISO: MIST-Iraq and Advising at the Operational Level of War," *Special Warfare*, January–March 2018, pp. 28–32.

Shane, Scott, and Mark Mazzetti, "The Plot to Subvert an Election," *New York Times*, September 20, 2018.

Shultz, Richard H., and Roy Godson, *Dezinformatsiya: Active Measures in Soviet Strategy*, Washington, D.C.: Pergamon-Brassey, 1984.

Simpson, John, "Russia's Crimea Plan Detailed, Secret and Successful," BBC, March 19, 2014. As of July 16, 2019:
https://www.bbc.com/news/world-europe-26644082

Sindelar, Daisy, "The Kremlin's Troll Army: Moscow Is Financing Legions of Pro-Russia Internet Commenters. But How Much Do They Matter?" *The Atlantic*, August 12, 2014. As of August 10, 2019:
https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/

Sivkov, Konstantin, "The 'Wisdom' of Yanukovich [«Мудрость» Януковича]," *Military-Industrial Courier [Военно-промышленный курьер]*, No. 26, July 23, 2014.

Skorobutov, Dmitriy, "Confession of a Propagandist. Part I. How to Make News on Government TV [Исповедь пропагандиста. Часть I. Как делают новости на государственном ТВ]," *The Insider*, June 9, 2017. As of August 9, 2019:
https://theins.ru/confession/59757/

Smeets, Max, "Europe Slowly Starts to Talk Openly About Offensive Cyber Operations," Council on Foreign Relations blog post, November 6, 2017. As of August 12, 2019:
https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations

Smith, Rohan, "Columbia Chemical Hoax Tracked to 'Troll Farm' Dubbed the Internet Research Agency," News.com, June 4, 2015. As of August 9, 2019:
https://www.news.com.au/technology/online/social/columbia-chemical-hoax-tracked-to-troll-farm-dubbed-the-internet-research-agency/news-story/128af54a82b83888158f7430136bcdd1

Snegovaya, Maria, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Russia Report I, Washington, D.C.: Institute for the Study of War, September 2015. As of August 9, 2019:
http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf

Snyder, Glenn Herald, *Deterrence and Defense: Toward a Theory of National Security*, Princeton, N.J.: Princeton University Press, 1961.

Sokirko, Viktor, "Symmetrical Answer: With Which Weapons Can Russia Answer America [Симметричный ответ: Каким оружием Россия может ответит США]," *Flag of the Motherland [Флаг Родины]*, No. 87, November 13, 2015.

Soldatov, Andrei, and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, New York: PublicAffairs, 2015.

Somer, Iryna, "Lithuanians Create Artificial Intelligence with Ability to Identify Fake News in 2 Minutes," *Kyiv Post*, September 21, 2018. As of February 4, 2019: https://www.kyivpost.com/technology/lithuanian-creates-artificial-intelligence-with-ability-to-identify-fake-news-within-2-minutes.html

Soshnikov, Andrei, "Inside a Pro-Russia Propaganda Machine in Ukraine," BBC, November 13, 2017. As of March 12, 2019: https://www.bbc.com/news/blogs-trending-41915295

"Source in Ministry of Defense: The Armed Forces of the Russian Federation are Creation Troops for Information Operations [Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций]," TASS, May 12, 2014. As of August 9, 2019: https://tass.ru/politika/1179830

"Special Front [Особый фронт]," *Arguments of Time [Аргументы времени]*, October 1, 2018. As of January 28, 2019: http://svgbdvr.ru/voina/osobyi-front

Sputnik, "About Us," webpage, undated. As of October 7, 2019: https://sputniknews.com/docs/about/index/

"The St. Petersburg Troll Factory Targets Elections from Germany to the United States," *EU vs. Disinfo*, April 2, 2019. As of August 12, 2019: https://euvsdisinfo.eu/the-st-petersburg-troll-factory-targets-elections-from-germany-to-the-united-states/

Standish, Reid, "Russian Troops Are in Syria, and We Have the Selfies to Prove It," *Foreign Policy*, September 8, 2015. As of August 12, 2019: https://foreignpolicy.com/2015/09/08/russian-troops-are-in-syria-and-we-have-the-selfies-to-prove-it/

Stedman, Scott, "Kremlin Propagandist Boasted of His Hacking Efforts, Strongly Implied Colluding with Trump Team in Facebook Posts," *Medium*, November 21, 2017. As of August 12, 2019: https://medium.com/@ScottMStedman/kremlin-propagandist-boasted-of-his-hacking-efforts-strongly-implied-colluding-with-trump-team-in-a905104965a1

Steinzova, Lucie, and Kateryna Oliynyk, "The Sparks of Change: Ukraine's Euromaidan Protests," Radio Free Europe/Radio Liberty, November 21, 2018. As of August 12, 2019: https://www.rferl.org/a/ukraine-politics-euromaidan-protests/29608541.html

Stelzenmüller, Constanze, "The Impact of Russian Interference on Germany's 2017 Elections," testimony presented before the U.S. Senate Select Committee on Intelligence, June 28, 2017. As of August 10, 2019: https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/

StopFake, "About Us" webpage, undated. As of August 12, 2019: https://www.stopfake.org/ru/o-nas/

Streltsov, A. A., "The Main Tasks for Government Policy in Information Warfare [Основные задачи государственной политики в области информационного противоборство]," *Military Thought [Военная мысль]*, No. 5, 2011, pp. 18–25.

Stubbs, Jack, "#NoRussiaNoGames: Twitter 'Bots' Boost Russian Backlash Against Olympic Ban," Reuters, December 8, 2017. As of August 12, 2019: https://www.reuters.com/article/us-twitter-russia-olympics/norussianogames-twitter-bots-boost-russian-backlash-against-olympic-ban-idUSKBN1E223V

Sukhankin, Sergey, "Military Psychology—New Pivot of Russian Military Strategy," *RealClearDefense*, March 15, 2018. As of August 12, 2019: https://www.realcleardefense.com/articles/2018/03/15/military_psychologynew_pivot_of_russian_military_strategy_113200.html

"Surkov Declared Putinism the Ideology of the Future [Сурков объявил путинизм идеологией будущего]," Lenta.ru, February 11, 2019. As of August 9, 2019: https://lenta.ru/news/2019/02/11/surkov/

Swire, Briony, Ullrich K. H. Ecker, and Stephan Lewandowsky, "The Role of Familiarity in Correcting Inaccurate Information," *Journal of Experimental Psychology: Learning, Memory, and Cognition*, Vol. 43, No. 12, 2017, pp. 1948–1961. As of August 12, 2019: https://www.ncbi.nlm.nih.gov/pubmed/28504531

Syria Justice and Accountability Centre, "Russia's Twitter Campaign: Influencing Perceptions of the Syrian Conflict," December 12, 2018. As of August 12, 2019: https://syriaaccountability.org/updates/2018/12/12/russias-twitter-campaign-influencing-perceptions-of-the-syrian-conflict/

Szayna, Thomas S., *The Ethnic Factor in the Soviet Armed Forces*, Santa Monica, Calif.: RAND Corporation, R-4002-A, 1991. As of August 12, 2019: https://www.rand.org/pubs/reports/R4002.html

Taylor, Margaret L., "Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe," Brookings Institution, July 31, 2019. As of August 12, 2019: https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/

Teper, Yuri, and Daniel D. Course, "Contesting Putin's Nation-Building: The 'Muslim Other' and the Challenge of the Russian Ethno-Cultural Alternative." *Nations and Nationalism*, Vol. 20, No. 4, 2014, pp. 721–741. As of August 12, 2019: https://onlinelibrary.wiley.com/doi/full/10.1111/nana.12078

"Temnik—the Kremlin's Route to Media Control," *EU vs. Disinfo*, March 29, 2017. As of August 10, 2019: https://euvsdisinfo.eu/temnik-the-kremlins-route-to-media-control/

"TEXT: Full Mueller Indictment on Russian Election Case," Politico, February 16, 2018. As of August 12, 2019:
https://www.politico.com/story/2018/02/16/text-full-mueller-indictment-on-russian-election-case-415670

"Threat Group-4127 Targets Google Accounts," *Secureworks*, June 26, 2016. As of August 12, 2019:
https://www.secureworks.com/research/threat-group-4127-targets-google-accounts

Timberg, Craig, "Russian Propaganda Effort Helped Spread 'Fake News' During Election, Experts Say," *Washington Post*, November 24, 2016.

Timofeev, Vladimir, "On Informshablon [Про информшаблону]," *Red Star [Красная звезда]*, No. 6, January 19, 2005.

Tomlin, Gregory M., "#SocialMediaMatters: Lessons Learned from Exercise Trident Juncture," *Joint Force Quarterly*, No. 82, July 1, 2016. As of August 12, 2019:
https://ndupress.ndu.edu/Media/News/Article/793264/socialmediamatters-lessons-learned-from-exercise-trident-juncture/

"Transcript: Putin Says Russia Will Protect the Rights of Russians Abroad," *Washington Post*, March 18, 2014.

"Transcript: Vladimir Putin's April 17 Q&A," *Washington Post*, April 17, 2014.

Troianovski, Anton, and Ellen Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in PUTIN'S DUELS with the West," *Washington Post*, December 28, 2018.

Tsyganok, Anatoliy, "The First Casualties of New-Generation Weapons [Первые Жертвы Оружия Нового Поколения]," *Independent Military Review [Независимое военное обозрение]*, No. 44, 2018.

Turovsky, Daniil, "Our Time to Serve Russia Has Arrived [0 Пришло наше время послужить России]," *Meduza*, August 7, 2018a. As of August 9, 2019:
https://meduza.io/feature/2018/08/07/prishlo-nashe-vremya-posluzhit-rossii

———, "The GRU—What's to It? Whom Do They Recruit as Spies? And Why Are They So Often Revealed? [ГРУ— это вообще что? Кого берут в шпионы? И почему их так часто раскрывают?]," *Meduza*, October 15, 2018b. As of August 9, 2019:
https://meduza.io/feature/2018/10/15/gru-eto-voobsche-chto-kogo-berut-v-shpiony-i-pochemu-ih-tak-chasto-raskryvayut

———, *Invasion: A Short History of Russian Hackers [Вторжение: Краткая История Русских Хакеров]*, Moscow: Individuum Publishing [Индивидуум паблишинг], 2019.

Twitter, "Data Archive," webpage, undated. As of August 12, 2019:
https://about.twitter.com/en_us/values/elections-integrity.html#data

Ukraine Crisis Media Center, "Who We Are," webpage, undated. As of August 12, 2019:
http://uacrisis.org/about

"Ukraine Profile—Media," BBC, December 10, 2018. As of August 12, 2019:
https://www.bbc.com/news/world-europe-18006248

"Ukraine's 'Invisible' Volunteer Fighters," Hromadske International, November 18, 2018. As of August 12, 2019:
https://en.hromadske.ua/posts/ukraines-invisible-volunteer-fighters

*United States v. Internet Research Agency*, indictment, case 1:18-cr-00032-DLF, D.D.C., February 16, 2018. As of August 10, 2019:
https://www.justice.gov/file/1035477/download

*United States v. Khusyaynova*, criminal complaint, case 1:18-MJ-464, E.D. Va., September 28, 2018. As of August 12, 2019:
https://www.justice.gov/usao-edva/press-release/file/1102591/download

*United States of America v. Viktor Boris Netyksho, Boris Alekseyevich Antonov et al.*, case 1:18-cr-00215-ABJ, July 13, 2018. As of August 12, 2019:
https://www.justice.gov/file/1080281/download

U.S. Advisory Commission on Public Diplomacy, *2018 Comprehensive Annual Report on Public Diplomacy and International Broadcasting*, Washington, D.C.: U.S. Department of State, November 20, 2018. As of August 12, 2019:
https://www.state.gov/2018-comprehensive-annual-report-on-public-diplomacy-and-international-broadcasting/

U.S. Attorney's Office, Eastern District of Virginia, "Russian National Charged with Interfering in U.S. Political System," news release, October 19, 2018. As of August 12, 2019:
https://www.justice.gov/usao-edva/pr/
russian-national-charged-interfering-us-political-system

U.S. Department of Defense, "Cyber Mission Force Achieves Full Operational Capability," May 17, 2018. As of August 10, 2019:
https://dod.defense.gov/News/Article/Article/1524747/
cyber-mission-force-achieves-full-operational-capability/

U.S. Department of Justice, Office of Public Affairs, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," press release, October 4, 2018. As of August 10, 2019:
https://www.justice.gov/opa/pr/
us-charges-russian-gru-officers-international-hacking-and-related-influence-and

U.S. House of Representatives Permanent Select Committee on Intelligence, "Social Media Advertisements: 2017: Quarter 2, May: Ad ID 981," webpage, undated-a. As of July 30, 2018:
https://democrats-intelligence.house.gov/social-media-content/
social-media-advertisements.htm

———, "Social Media Advertisements: 2017: Quarter 2, May: Ad ID 1262," webpage, undated-b. As of July 30, 2018: https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm

———, "Social Media Advertisements: 2017: Quarter 2, May: Ad ID 3023," webpage, undated-c. As of July 30, 2018: https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm

U.S. Senate Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, Washington, D.C.: U.S. Government Publishing Office, January 10, 2018. As of August 12, 2019: https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

"U.S. Tried to Slow Down North Korea's Atomic Program [США пытались затормозить ядерную программу КНДР]," *Foreign Military Review [Зарубежное военное обозрение]*, No. 6, 2015, pp. 107–108.

Vasilev, Yuriy, and Dinara Setdikova, "The SVR: A Million Dollars—On Blogs [СВР: миллион долларов - на блоги]," Radio Svoboda [Радио Свобода], August 27, 2012. As of August 11, 2019: https://www.svoboda.org/a/24689413.html

Vilmer, Jean-Baptiste Jeangène, *The "Macron Leaks" Operation: A Post-Mortem*, Washington, D.C.: Atlantic Council, June 2019. As of August 8, 2019: https://www.atlanticcouncil.org/images/publications/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

Vilmer, Jean-Baptiste Jeangène, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera, *Information Manipulation: A Challenge for Our Democracies*, Paris: Policy Planning Staff of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research of the Ministry for the Armed Forces, August 2018. As of August 8, 2019: https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

Virtual Globetrotting, "MediaSintez LLC—Division of Internet Research Agency—Russian 'Troll Farm,'" webpage, undated. As of August 12, 2019: https://virtualglobetrotting.com/map/mediasintez-llc-division-of-internet-research-agency-russian-troll-farm/view/google/

Vladimirov, Yuriy, "The Chechen War (The Psychological Aspect) [Чеченская воина (психологический аспект)]," *On the Fighting Post [На боевом посту]*, No. 75, September 29, 2000.

Volchek, Dmitry, and Claire Bigg, "Ukrainian Bloggers Use Social Media to Track Russian Soldiers Fighting in East," *The Guardian*, June 3, 2015. As of August 12, 2019: https://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine

Way, Lucan Ahmad, and Adam Casey, *Is Russia a Threat to Western Democracy? Russian Intervention in Foreign Elections, 1991–2017*, Stanford, Calif.: Stanford University, November 3, 2017. As of August 9, 2019: https://pdfs.semanticscholar.org/c11b/3070391cf888f2decdbfe4691201ae46a35a.pdf

Weisburd, Andrew, Clint Watts, and J. M. Berger, "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy," *War on the Rocks*, November 6, 2016. As of August 12, 2019: https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/

"What's Known About Vladislav Surkov [Чем известен Владислав Сурков]," *Kommersant [Коммерсантъ]*, May 24, 2019. As of August 9, 2019: https://www.kommersant.ru/doc/1939610

Yang, Jenny, "Information: The Perfect Weapon in Today's Wired World, A Three-Part Series," NATO Association of Canada, August 8, 2015. As of August 10, 2019: http://natoassociation.ca/information-the-perfect-weapon-in-todays-wired-world-a-three-part-series-2/

"Year in Review: 1001 Messages of Pro-Kremlin Disinformation," *EU vs. Disinfo*, January 3, 2019. As of August 12, 2019: https://euvsdisinfo.eu/year-in-review-1001-messages-of-pro-kremlin-disinformation/

"Yle Kioski Traces the Origins of Russian Social Media Propaganda-Never-Before Seen Material from the Troll Factory," *Kioski*, February 20, 2015. As of August 10, 2019: http://kioski.yle.fi/omat/at-the-origins-of-russian-propaganda

Yovanovitch, Marie, "Remarks by Ambassador Yovanovitch on the Occasion of the 5th Anniversary of the Ukraine Crisis Media Center's Founding," U.S. Embassy in Ukraine, March 5, 2019. As of August 12, 2019: https://ua.usembassy.gov/remarks-by-ambassador-yovanovitch-on-the-occasion-of-the-5th-anniversary-of-the-ukraine-crisis-media-centers-founding/

Zelensky, Mikhail, "Russia Will Soon Require Digital Journalists to Delete 'Fake News' 'Instantly.' Here's What That Actually Means," *Meduza*, March 6, 2019. As of August 12, 2019: https://meduza.io/en/feature/2019/03/06/russia-will-soon-require-digital-journalists-to-delete-fake-news-instantly-here-s-what-that-actually-means

Zhilin, Gennadiy, "Information-Psychological Weapons: Yesterday and Today [Информационно-Психологическое Оружие: Вчера и Сегодня]," *Soldier of the Fatherland [Солдат Отечества]*, No. 57, 2004.

Zushin, Yevgeniy Georgievich, "Power Has No Equal in Strength [Власть, не имеющая равных по силе воздействия]," *Independent Military Review [Независимое военное обозрение]*, No. 16, April 30, 1999.


PROJECT AIR FORCE

Russia is waging wide-reaching information warfare with the West. A significant part of this war takes place on social media, which Russia employs to spread disinformation and to interfere with the internal politics of other countries. Drawing on a variety of primary and secondary sources, expert interviews, and fieldwork in Ukraine, the report describes Russia's information warfare in the social media sphere (as of 2019) and provides recommendations to better counter this evolving threat. Moscow views social media as a double-edged sword—anxious about its potential to undermine Russia's security but aware of its advantages as a weapon of asymmetric warfare. Russia's use of this weapon picked up most markedly in 2014, suggesting a reaction to the West's response to the Ukraine conflict. Although popular portrayals of the Russian disinformation machine at times imply an organized and well-resourced operation, evidence suggests that it is neither. However, even with relatively modest investments, Russian social media activity has been wide-reaching. The impacts of Russia's efforts on the West—and of Western countermeasures on Russia—are difficult to assess. However, this threat can cause a variety of harms and is likely to evolve. Thus, the authors recommend that the U.S. Air Force and the joint force improve defensive measures aimed at raising awareness and lowering the susceptibility of the military and their families to Russian disinformation and propaganda campaigns.

$34.50

ISBN-10 1-9774-0968-7
ISBN-13 978-1-9774-0968-3


www.rand.org

RR-4373/2-AF