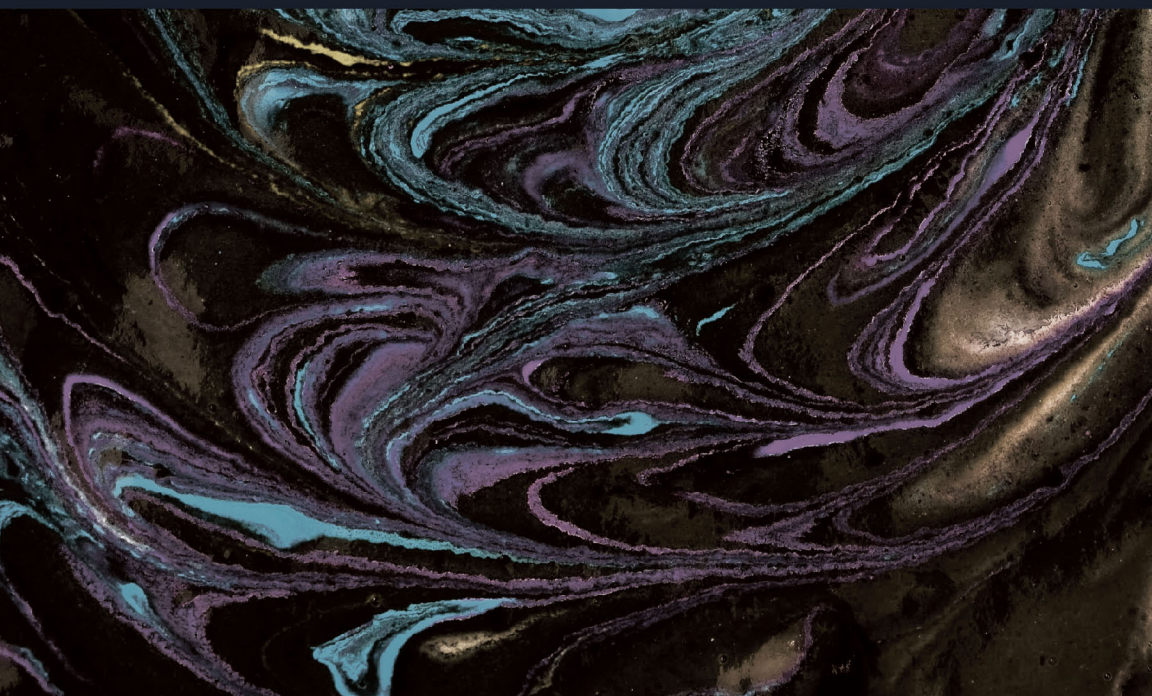


CREATING CHAOS ONLINE

Disinformation and
Subverted Post-Publics



Asta Zelenkauskaitė

Creating Chaos Online

Creating Chaos Online

Disinformation and Subverted Post-Publics

Asta Zelenkauskaitė

University of Michigan Press
Ann Arbor

Copyright © 2022 by Asta Zelenkauskaitė
Some rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. *Note to users:* A Creative Commons license is only valid when it is applied by the person or entity that holds rights to the licensed work. Works may contain components (e.g., photographs, illustrations, or quotations) to which the rightsholder in the work cannot apply the license. It is ultimately your responsibility to independently evaluate the copyright status of any work or component part of a work you use, in light of your intended use. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>

For questions or permissions, please contact um.press.perms@umich.edu

Published in the United States of America by the
University of Michigan Press
Manufactured in the United States of America
Printed on acid-free paper
First published September 2022

A CIP catalog record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication data has been applied for.

ISBN 978-0-472-07552-2 (hardcover : alk. paper)
ISBN 978-0-472-05552-4 (paper : alk. paper)
ISBN 978-0-472-90290-3 (OA)

DOI: <https://doi.org/10.3998/mpub.12237294>

Library of Congress Control Number: 2022939744

*To Živilė, Jūratė, and Danutė
With love*

Contents

Introduction. A Déjà Vu from the Silenced Generation	1
Disinformation	3
Soviet Propaganda in the Eyes of a Child	9
Vulnerabilities of Social Media	17
Trolling and Russian Trolling	23
Russian Trolling Circulation	30
Chapter 1. Propagandistic Masquerade	38
Text as a Mask	39
Paradoxes of a Mask	40
Subversiveness of a Mask	46
Performativity and Modus Operandi of a Propagandist Mask: self-sabotage	56
Multiple Faces for the Masks: Commenting User Typology	64
Discussion	75
Summary	79
Chapter 2. Divide and Conquer: Exploiting Political Polarization	81
Frameworks of Information Persuasion	84
Communication Persuasion Models	85
Mechanics of Propaganda	87
Communicative Tactics: Attack, Defense, and Whataboutism	99
Tactics Used in Online News Comments	102
Discussion	119
Summary	121

Chapter 3. Instilling Mistrust in Institutions	127
Living in Media	129
Comments as Forms of News Deliberations	136
News Portals Comments as Information Warfare Zones	139
Contexts That Situate Online Public Deliberation	143
Discrediting Media as an Institution	146
Attack on Government Institutions	154
Discussion	157
Summary	162
Chapter 4. Roots of Russia’s Victim’s Playing	171
New Media and Information Warfare in Authoritarian Regimes	173
Roots of Russia’s (Information) Warfare	177
Information Warfare in Action by Russia	186
Victim-Playing Russian Trolls in the News Comments	195
Delegitimization Rhetoric	202
Summary	218
Chapter 5. Deny and Conquer: Fears of Looking Like a “Pussy State”	220
Implications of the Denialism Discourse regarding Russian Trolling	221
Psychology of Denialism	227
Denial and Conspiracy Theories	231
Denial Normalization Traps to Avoid	234
Discussion	245
Summary	249
Epilogue: Now What?	255
Imperviousness to Chaos	255
What Solutions Are There for Russian Trolling?	260
Web as a Zero Institution	265
<i>Appendix</i>	267
<i>Bibliography</i>	271
<i>Index</i>	295

Digital materials related to this title can be found on the Fulcrum platform via the following citable URL: <https://doi.org/10.3998/mpub.12237294>

Introduction

A Déjà Vu from the Silenced Generation

“Denial, a psychological defense mechanism, is an unconscious mental maneuver that cancels out or obscures painful reality. . . . We do not need to confront or change things that do not exist”
(Milburn, 1998, p. 1)

Denial describes information operations that allow for the achieving of strategic goals. This book is set to expose efforts to justify Russian trolling. Specifically, this book documents patterns and frames of systematic denialism used to justify Russian trolling that circulated in two unrelated contexts and periods of time. This book not only uncovers justification arguments and the way they are constructed but also provides explanations of their origins and what led them to become so pervasive online. Furthermore, through the concept of post-publics, this book exemplifies how the public spheres are disrupted by employing discursive means of denialism, despite rational evidence grounded in facts.

I am compelled to examine the characteristics of Russian trolling across online platforms for a range of reasons. Russian trolling has been exposed as an ideological weapon employed to manipulate public opinion aided by disinformation (Berghel & Berleant, 2018). Manipulation was found to be adopting tactics typical for astroturfing trolling such as disruption and distrust (Berghel & Berleant, 2018), and deflection of attention to irrelevant issues (Zelenkauskaite & Niezgodna, 2017), thus creating chaos online.

This book is further driven by questions such as, What makes it so difficult to render Russian trolling visible despite unequivocal evidence? How does the justification of Russian trolling interference challenge democratic

beliefs and institutions? Such questions have become critical after the initial warnings about Russian trolling that received mainstream press coverage, as exemplified by Adrian Chen's story in the 2015 June 3 issue of the *New York Times Magazine*. The story exposed Russian trolling at work and its proliferation in online spaces to circulate propaganda on a global scale—how it sows the seeds of discord and blurs the lines between multiple constructions of reality. Chen's (2015) report on a Russian trolling factory was breaking news that catalyzed a global chain reaction.

Global news outlets, led by those in the United States of America, continued to generate stories about Russian trolling that gained a lot of traction. On 2014 May 4, *The Guardian* published a news report about organized, topic-based targeting in the news comments section, which had attracted pro-Putin propaganda posts that looked to be an orchestrated pro-Kremlin campaign (Elliot, 2014). Similarly, in 2015, Lithuanian news outlets released purported exposés about specific Russian trolling techniques, including the pushing of pro-Kremlin agendas embedded in divisive political comments across new media platforms (Delfi.lt, Kremliaus “trollių irštva,” 2015).

Russian trolling efforts reemerged in a new geopolitical context—the 2016 US presidential election—that will be remembered for the Russian trolling allegations that proliferated at the time. In 2017, the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the US National Security Agency (NSA) produced a report that detailed how Russia had spearheaded the disinformation campaign throughout the 2016 election. This campaign's objectives, the US agencies claimed, were social division and online chaos (Kennedy, 2017). Yet, the denial of Russian interference continued to circulate online.

In the broadest sense, this book details how the public sphere can be disrupted by exploiting online spaces, even if they are set to serve public deliberation (Bennett & Pfetsch, 2018). By specifically focusing on repeated Russian trolling justification arguments, this book contributes to the understanding of a phenomenon known as *coordinated inauthentic behaviors* (Keller et al., 2020). I first aim at introducing the main concepts used in this book: disinformation and how it differs from misinformation, its contextual meaning over time and my personal experience with it. Subsequently, I connect the concept of disinformation as used in the past to argue about the current social media landscape and its vulnerabilities, by then introducing the concept of trolling and Russian trolling. These concepts are set to contextualize Russian troll denialism frames which were identified in the systematic analysis of online portals comments and on Gab.com, a far-right social networking site.

While Russian trolling is central to exemplify denialism expressed through justification and deflection, denialism framework can be traced and extended to any contexts, especially during times of uncertainty. Russian trolling allegations keep resurfacing, but most importantly, the implications of denialism can be extended to any controversial topic or “cracks” in society that then are exploited to subvert the online public sphere (e.g., Ward, 2020). Furthermore, as worldwide news portals report, including in Lithuania, Russian trolling has become symptomatic of such vulnerabilities since it emerged as an online phenomenon in Europe (see, e.g., Vaišnys et al., 2017; Zelenkauskaitė & Niezgodą, 2017) and surged as a rhetorical trope for foreign interference in 2016 US presidential elections and computational propaganda has been witnessed around the globe (Woolley & Howard, 2017).

Disinformation

Creating Chaos Online specifies the arguments that are typically used to generate disinformation. Disinformation here is described as chaos creation efforts. Disinformation has been eloquently explicated by Starbird et al. (2019) as a subtype of strategic information operations—where strategic information surges from Habermasian theory of communicative rationality—yet, it is used subvert online discourse to influence opinions. In other words, disinformation involves “deliberate (often orchestrated) attempts to confuse or manipulate” (Ireton & Posetti, 2018, p. 7). And disinformation is designed to disrupt public communication processes.

Creating Chaos Online challenges the preconception that fake news and false information are the greatest threats in the current media landscape by arguing that a more subtle, doubt-instilling, affective stream of repeated ideas can eventually render publics vulnerable to disinformation (Allcott & Gentzkow, 2017). In this book the concept of disinformation goes beyond the false facts and rational arguments. Rather, disinformation is conceptualized as the deployment of propaganda that involves affective, deflective, and *misleading*, rather than false information, and propaganda is conceptualized as the intentional use of communication means to influence attitudes and behaviors in target populations (Faris et al., 2017).

The act of misleading does not necessarily involve the provision of false information. Rather, its objective is to generate doubt and uncertainty. Propaganda, unlike persuasion, distinguishes itself by its malign character, as argued by Jowett and O’Donnell (2018). The propagandist’s interests drive the communication that leads to persuasion. Then persuasion is employed

to serve such a malign intent and can deliberately introduce misinformation, even falsehood or deception. To achieve the goal of misinformation, communication is used to omit relevant information, not only distort it. Thus, while the mechanisms accompanying online misinformation and disinformation go hand in hand, they are distinct. Misinformation refers to the information that is factually inaccurate. In other words, it is “misleading information created or disseminated without manipulative or malicious intent” (Ireton & Posetti, 2018, p. 7). Such information is typically used from alternative sources that can be accessed and shared, especially online. Misinformation is often accompanied by disinformation—where individuals, groups, and organizations deliberately aim to create confusion and discord, as I argue in this book, by triggering an emotive response, that is, by employing affect.

This book also analyzes the role of affect in shaping disinformation by distinguishing disinformation from fake news. Instances of disinformation strategies that were found in online comments, and that this book analyzes, typically cannot be challenged on the grounds of the factuality of information—that is, apart from the instances where conspiracy theories are used to challenge the existence of Russian trolls. However, deflative counterarguments for the existence of Russian trolls contain scant contestable information. Such counterarguments remain compelling because disinformation can function without facts, depending instead on affect, or emotional persuasion. Disinformation circulated through affective strategies can create chaos because it operates on a more subtle, emotive level than fake news, which relies on factual accuracy that can be challenged on the rational grounds.

Therefore, this book discusses the affective public sphere that can be exploited for disinformation. While citing examples from established democracies, Papacharissi (2015) invoked affective publics to address how publics make sense of information in the public sphere. Even if it is driven by emotion, it does not disregard democratic premises of participation in public debate. However, affect has been found to be exploited in the current post-truth information age to harness hatred and division (Davis, 2020). Therefore, disinformation that appeals to the affect is an effective strategy for what some scholars, such as Bennett and Livingstone (2021), called forms of disruptive communication and in this book is interpreted as generating online chaos. Furthermore, scholars of the affective propaganda argued that such emotions serve as the greatest currency in the current media landscape (Boler & Davis, 2020).

While disinformation can take different shapes, this book argues that the affect, instilled through conspiracy theories, can inflame existing social and

political conflicts. It can manifest through attacks on scientific evidence and by the seeding of mistrust in institutions (see Bennett & Livingstone, 2021). Asmolov (2019), in addition, concluded that it is not too difficult to detect propaganda since it is produced to elicit emotions.

Why does it matter that the public sphere constitutes authentic people's comments? In established democracies, expectations about how debates should be conducted include rationality and affective ways of debating with civility. One can argue, however, that authentic audience comments, at times, depart from the expectations of the ideal Habermasian public sphere. For example, while the public sphere has been portrayed as an ideal space where debates generate some form of consensus, the internet provides online spaces where users speak but do not necessarily listen. Similarly, the tone of such debates can be, at times, crude or spontaneous—in either case, they are frequently emotional. As such, inflammatory comments can be crude, and direct, with little elaboration. Additionally, comments can include shouting, speaking over others, crude humor—direct, and at times, poorly structured arguments. Clearly, public sphere, especially online, can resemble an unpolished public sphere rather than an idealistic one, as argued by scholars like Bakardjieva (2008). Yet, the premise of such a public sphere, even if tainted by instances of incivility, is that it is constituted by authentic publics and not orchestrated inauthentic actors.

Affect, has been found to be successfully exploited in disinformation by inauthentic users. “Neutrollization” has been coined as a term to describe pro-Kremlin efforts to generate neutralizing efforts that absolve Russia from being viewed as a societal security threat (Kurowska & Reshetnikov, 2018). In this book such techniques are contextualized as discursive manifestations of a form of denialism or discursive efforts to merely dismiss or justify Russian trolling efforts. These efforts, which can be explained through the lens of disinformation, that Bennett and Livingstone (2021) explained as “as intentional falsehoods or distortions, often spread as news, to advance political goals such as discrediting opponents, disrupting policy debates, influencing voters, inflaming existing social conflicts, or creating a general backdrop of confusion and informational paralysis” (p. 33). In such way, information paralysis becomes another key aspect through which chaos is created in online contexts. Similar to information paralysis, Benkler et al. (2018) referred to a concept of disorientation defined as a condition through which propaganda seeks to induce where the targeted population can no longer to identify what is true and what is not.

In addition, one of the key aspects of disinformation is that it may undermine epistemological basis for truth validation; instead, emotions,

here referred to as *affect*, become the baseline for assessing the truthfulness of any information (Bjola & Papadakis, 2020). Disinformation, through affect and proliferation capacity, resembles rumors, which are particularly destabilizing and circulate most effectively in times of uncertainty—when public perception is most vulnerable to manipulation. Then, chaos spawns endless speculations, proving that the affective power of rumors exceeds that of merely factual information. In short, rumors become appealing when they are couched in the language of speculation (O’Leary, 2001). As O’Leary (2001) observed, rumors become dangerous when they enter mainstream discourses. When repeated sufficiently, rumors assume the guise of new realities. Attempts to debunk them by adopting a factual perspective do little to diminish their power to fascinate the public. Although rumors can originate in facts, they are ultimately difficult to verify. For instance, if the statement “Russian trolling could not have happened”—or claims during times of a pandemic that “vaccines are not safe”—are repeated multiple times in online spaces, its rapid proliferation is able to sow the seeds of doubt in the minds of some internet users and become “unspoken knowledge.” Thus, when disinformation functions as rumor, it can be deployed to generate online chaos.

This book contends that disinformation can proliferate easily in online spaces due to the sociotechnical structure of online platforms, including anonymity. Anonymity encourages users to assume masked or faceless identities to generate posts on news portals or social networking sites. Similarly, automation can foster the amplification and proliferation of the content, otherwise known as virality, where a certain idea or information can pave its way from the margins to the mainstream (Nahon & Hemsley, 2013). Moreover, such pseudonymous, or anonymous, messages can be easily replicated and reposted. Unlike fake news, disinformation does not purport to provide facts. Rather, it is a discursive tactic that strategically implants doubt in the minds of online news comment readers, or at least to some of them. Doubt is generated through the ambiguity of partial truths.

Like other traditional propaganda tactics, disinformation attempts to confuse online readers. Disinformation, as Geissler and Sprinkle (2019) noted, may combine prototypical and counterfactual elements. While prototypical elements refer to common techniques for propaganda dissemination, the term “counterfactual” is used to describe an approach that focuses on facts as evidence for propaganda. Unlike Geissler and Sprinkle (2019), who examined counterfactual propaganda to identify factual truth in conspiracy theories by focusing on factual sources, as in typical fake news studies, the objective here is to focus on the prototypical manifestation of chaos—that is, the techniques that are used to generate disinformation. The focus here

is on the prototypical parts of manifestation of disinformation that can be propagated by anyone.

Typically, disinformation is analyzed through three facets: content, reception, and intent (Woolley, 2020). This book analyzes the construction of the messaging, actors, and the context in which it takes place. Blatant denial of an event that has already occurred, acknowledgment of that event within a self-victimizing rhetorical context meant to appeal to readerly sympathy and deflecting from the immediate issue of debate (e.g., Russian trolling)—these are three major argumentative strategies for generating disinformation. Another strategy specifically related to Russian trolling was found to involve critiques and degradation of institutions that allegedly investigated the phenomenon. And yet another strategy included generating ambiguity and chaos—for instance, when a user claims to be a Russian troll or accuses other users of being one. Arguments that deployed these rhetorical strategies frequently adopt a dismissive, ridiculing, mocking, and delegitimizing tone to defend the phenomenon of Russian trolling. This tone invites chaos when repeated content across multiple news sources, leveling partisan lines. All in all, such tactics for generating ambiguity differ from those for deploying false information or misinformation, in that disinformation involves affect rather than the factuality of the information.

Moreover, I advance the argument that within shifting contexts, misinformation or false information can evolve into disinformation beyond the actor-based approaches, as very much thoroughly detailed by Benkler et al. (2018). Instead, this book asks how the arguments of disinformation are constructed and who they intend to target rather than investigating who is behind it. Similarly, the effectiveness of disinformation does not depend on the factual accuracy of information. Rather, that information must be partial and sufficiently unverifiable. In other words, the deployment of disinformation underscores the contextual and socially constructed nature of realities, as already argued by some scholars of disinformation, such as Karlova and Fisher (2013). Consequently, disinformation spawns the uncertainty that is at the root of chaos, since it originates in the malicious intent to obscure rather than to clarify.

While anonymity and automation of information in online spaces can activate the disinformation warfare of ideas, otherwise known as computational propaganda (as referred by Woolley & Howard, 2018), this book positions disinformation through its discursive lens rather than merely as a technology-driven phenomenon. Davis (2021) defined cyberwar as a type of warfare that is in the shadows that works in pursuit of power and national interest. This book builds on the argument about the social construction

of technology—where the responsibility lies within each of us who use and create and manage these systems, including online platforms that host online content, in addition, but not only the technological properties that surround this.

Furthermore, partisan politics in the United States reflected in media ecosystems and their vulnerability for influence, has been argumentatively critiqued by scholars like Benkler et al. (2018). Benkler and colleagues uncovered these social constructions through asymmetries in partisan perception of trust in media, tropes by partisan media content circulation, and institutional forces and actors involved in disinformation circulation. This book places more weight on the false sense of (new) media affordances in which comments and social media circulate specific tropes, here referred to as frames, while highlighting the need to understand the logics behind types of messaging that constitute disinformation.

While some might contend that Russian trolling justification lurking in news portals comments seem to be merely comments “in the margins,” scholarship attributes an increasing power of online user-generated content and the impact of social media in our lives. For example, Vaidhyanathan (2018) proposed a convincing argument that social media platforms like Facebook have penetrated in our lives not only as pleasure machines but more recently as politics machines. Thus, messages, exchanged through media that have been typically designed as interpersonal media, currently can be used to push agendas, with a range of mechanisms embedded in specific sociotechnical system—from targeted advertisement on social media to automated content dissemination and machine-learning techniques or other artificial intelligence tools to seed relevant content for contestation.

News comments, in particular, have been empirically found to have an effect on the credibility of a conveyed news story content (e.g., Naab et al., 2020). Furthermore, as in rumors, the distance from being in the underground to spreading virally into the mainstream can be unexpectedly short. For example, hatred after surging in the sporadic comments online starts to proliferate and circulate in a memetic way, as exposed through platforms such as 4chan (Zelenkauskaite et al., 2021). Thus, Russian troll justification in the news portals’ comments is not merely a matter of communication in the margins.

This book focuses on the sociotechnicality of disinformation and mechanisms used to create chaos through the proliferation and recirculation of arguments. This book presents evidence where Russian troll justification recirculation was found across media sources and geopolitical contexts. And the sociotechnicality of these media ecosystems, even if not designed for

these purposes, can be used not only for public deliberation but also for computational propaganda to be employed in various online spaces, including comments, associated with news stories. It might be that the comments are propagating with the help of automated tools, such as algorithms or bots that dispatch content based on specific rules or news portals; the comments can be exploited to spread disinformation. Throughout this book, disinformation is treated as a form of information warfare that involves not only social media but also news comments written by general public users. And both of these platforms of information become subjects of disinformation, where disinformation adds to existing challenges of misinformation.

Soviet Propaganda in the Eyes of a Child

Interpretation of Russian trolling as a form of disinformation, embedded in online news portal comments, reflects the kind of propaganda that has already been circulated during World War II and more recently in authoritarian and totalitarian contexts. Such propaganda had been used to create chaos rather than to persuade the public to rally toward a single ideology. Thus, disinformation resembles a form of *déjà vu* experienced in different times and spaces. It bridges past and present by bringing together mass media, such as television, newspapers, and radio; newer media forms that are enabled through online social networks; and user-generated content, such as social media posts and news portal comments.

My personal experience with disinformation is based on the dual reality that I had known in my formative years, when images of prosperity starkly contrasted with the lived realities of the Soviet era. Chaos had been fomenting by exposing the Soviet citizenry to this dual reality, even while it was being silenced through the prohibition of free speech or at least deterrence. Szulecki (2018) summarized this experience in these words “Communist ideology was, by the late 1970s, hollowed out, yet it performed a stabilizing and normalizing function in that peculiar system. It was, according to Havel, an asylum and an alibi—an alibi for not-thinking, not-acting, not-caring, and not-asking for the Truth. ‘Living a lie’ was to be the result of a more general, existentially and politically understood human condition—coupled with hollow, ritualized ideology” (p. 321).

Yet the current media landscape is unique in that chaos is created by shaping information, not necessarily to make false claims but to expose disputable ones. Current online spaces can be used strategically, where messages are crafted by state-aligned actors to manipulate public opinion. According

to Karga and Rauchfleisch (2019), “These extrajurisdictional practices turn harassment into a relatively low-cost weapon for targeting the opposition, limiting freedom of speech through intimidation and pursuing a ‘silencing’ strategy” (p. 2). Silencing, a typical practice of authoritarian regimes, ensures government-dictated consensus. Therefore, silencing can become a weapon—one that is opposed to the processes of democratic deliberations and that is also a hallmark of propaganda.

I reference Soviet propaganda as a form of silencing to explain why Russian trolling as a phenomenon matters today. While the concept of trolling, popularly defined as “trolls post deliberately incendiary content to a discussion forum or other online community . . . for no other reason than to stir up chaos and outrage” (Dibbell, 2009, para. 9), has existed online since the Web 2.0 era, when the World Wide Web started to acquire socially interactive features, it has since become urgent to understand how rhetorical influence operates in online news and social media contexts. By invoking a personal account of persuasion, my goal is to contextualize Russian trolling as a by-product of postmodernism, or the polarity of arguments, that enables chaos to proliferate. The question is how to uncover such polarizing narratives that create chaos have emerged in response to Russian trolling across multiple online platforms and how they have proliferated in the online public sphere—across news portal comment spaces.

Raised in the former Soviet Union, my generation can be called the *silenced generation*. Silence reflects the absence of open debate, the possibility of public opposition to the status quo, or the overt endorsement of unpopular beliefs. Even if media scholars such as Chakars (2010) have extensively traced historical developments of the journalism in the post-Soviet era in the Baltics, or propaganda construction in media by scholars like Mažeikis (2010), I provide a personal account of those times to exemplify the realities of navigating the post-truth waters. The silenced generation collectively embodies the dichotomy of everyday life, or two versions of living: The version they are told to believe; and the actual, or “lived,” one. My generation learned to inhabit this duality.

We learned to identify the discrepancy between reality and its distortions—a phenomenon that had been validated by the media. Specifically, the Soviet media projected “official broadcast” messages of standardized reality that starkly contrasted with the actualities that could not be discussed openly. Yet we perceived them in our everyday lives. Such a dichotomously experienced reality can simply be equated with the Orwellian perception of life as the dystopic by-product of totalitarianism. Masha Gessen (2017), author of “The Future Is History: How Totalitarianism Reclaimed Russia,”

acutely observed: “George Orwell’s (2009) book could not be published in a society that it described, so Soviet readers would not have access to it till 1989, when censorship constraints had loosened sufficiently” (p. 16).

As a child, I had been exposed to changes within contexts that Thomas Kuhn (2012) called “paradigms.” Kuhn (2012) claims that paradigms change very slowly, typically after the death of those who establish them. In other words, it is rare to see the paradigmatic change in one’s lifetime. Yet throughout my own lifetime, the major paradigmatic shift I had experienced was the move from disinformation to its absence. Paradigms are comparable to frameworks of thought—how one can make sense of “reality.” I lived through a uniquely radical paradigm change when I witnessed the collapse of the former Soviet Union’s communist regime—how the “right” ways of thinking changed overnight. That was also when reality itself had changed. Ideological changes did not eliminate the silenced generation, however, and after the dissolution of the Soviet Union, we were finally allowed to speak up. But we still did not know how to talk—how to break out of the silence that had been imposed upon us. Thus, we had to learn quickly how to identify the vestiges of Soviet ideology that were no longer embedded in mass media and in other print forms. Yet at the same time, voicing the sudden change in circumstances has remained a remarkable obstacle that characterized my generation. The concept of a silenced generation remains prevalent in many parts of the world. For example, China’s authoritarian regime continues to dictate the clear “red lines” of debate that cannot be crossed, and prohibited debate topics include the efficacy of communist rule or the possibility of endorsing an alternative political party (Van Dijk & Hacker, 2018).

Similarly, ideological persuasion and disinformation are no mere abstractions for me. Rather, they are lived experiences that urge me to try to make sense of new media landscapes. After all, I grew up in the Republic of Lithuania when it was part of the Soviet Union—a vast territory of culturally diverse countries whose center was Moscow. In fact, I grew up among multiple dualities that did not always make sense. The first of these derived from a dual-state affiliation that I experienced through language. The Soviet Republic of Lithuania was technically bilingual, its recognized national languages being Russian and Lithuanian. Although my birth certificate retains inscriptions in both languages, as a child, I was raised in a Lithuanian-speaking family. I did not know Russian; nor did I grow up with kids who spoke the language. I did not pick it up at playgrounds, as some of the other kids did, where the Russian-speaking population was larger. However, when I started my schooling, I already knew how to read and write in Lithuanian, a language that is transcribed in the Roman alphabet. Later on, in first grade,

I learned the Cyrillic alphabet together with Russian. Consequently, I lived in a de facto bilingual world—another curious duality that begged for sense.

Even so, being raised as a bilingual Lithuanian child was not the most defining aspect of my dual existence. What had been definitively unique, however, was that I had grown up amid the censorship that a totalitarian one-party regime exercised over the lives of its citizenry. Government censorship supplied my generation with a predefined sense of reality. Thus, we were told what reality *should be*. At the same time, we could not help witnessing actualities. Obviously, they differed radically from the projected realities we had been fed. Such idealized distortions of reality, oftentimes couched in the language of emotional appeal, had been presented to us primarily through radio and television, and they were validated by educational materials approved for school curricula. These distortions infiltrated our everyday lives through the textbooks that we read as kids and the summer-camp rituals that we performed. Our textbooks paid tribute to Vladimir Lenin's courage and detailed his challenging life's journey, starting with his boyhood. We consumed images of the economic prosperity and the bright future that would be ours someday. And so we became involved in the ritualistic structures of ideology from early on by becoming little Octobrists, pioneers, and young communists, called upon to pave the pathway to communist party enlistment. Everyone's social role was defined by these ideological structures—mine, my parents', my schoolmates', my teachers'—even if not all of us had enlisted in the Communist Party.

An additional duality that I encountered through my schooling was communism's ideological framing, omnipresent in all media forms and in the educational system. It replicated the same ideological projection of communist prosperity—an ongoing narrative that allegedly paralleled the quinquennial progress, communism's bright future, equality for all. Such propaganda was a staple of all officially circulating information to instill what Mažeikis (2010) described as normative ideology. School textbooks, cartoons, magazines, newspapers, and television news projected the world in two different ways. Propaganda was also infused in popular art forms. It was evident in statuary on bridges that depicted peasants and workers uniting toward a bright communist future. We read it in the poetry and in the other literary genres of those times. Although communist propaganda glorified a bright future for the working class and proclaimed the steady advancement of the quinquennial plan, it was clear that socioeconomic instability was the actual norm in our daily lives.

From the economic standpoint, the quinquennial plan did not achieve its professed goals with each five-year iteration. In fact, overall economic

progress was sustained by limiting public information about actual situations. We were further duped into contributing to that so-called progress through sustainability initiatives, such as school recycling programs. Specifically, we were encouraged to compete with other schools to recycle the greatest number of disposable materials. Thus, we would reroute recyclables, like stacks of paper, from our homes to our schools to gain an edge over our competitors. Yet so-called progress was actually regressive, and the compromised economy finally crashed—an occurrence that coincided with the dissolution of the entire Soviet Union. Thus, I saw the dramatic reconfiguration of overarching ideological paradigms.

More specifically, I witnessed Soviet propaganda at work, together with its formative influence on my own childhood experiences and on those of all the other kids of my generation. Our most direct exposure to Soviet propaganda was through social structures, of which the most remarkable was school—its ideological medium being its sanctioned textbooks that promoted Soviet dominance. We were not obliged to purchase these textbooks. They were, in fact, unavailable for purchase. Instead, they circulated freely among us from library collections, changing hands each year among ourselves. In other words, the schoolchildren who advanced to higher grades would indirectly bequeath them, through the circulating library's agency, to those who would succeed them and peruse them for one school year. I remember how we had to buy transparent plastic covers for each textbook at the trimester's start. These were available in specific sizes to facilitate the precise lamination of each book. The books appeared glossily new in their plastic encasements, ensuring their continued use by many other successive generations of schoolchildren. We were sternly prohibited from marking the books in any way. Instead, they were to remain undefaced and intact in all other ways for their yearly end-of-term inspection. If they passed the requisite inspection, they would be routed to the library.

Retrospectively, this transparent plastic covering seems more than a simple book preservation routine that we have practiced to cover spines of my school's textbooks. The covering actually enhanced the outward concealment of textbook contents—it literally glossed over them. These contents included more than their purported subject matter. Specifically, each of my textbooks, whether its primary subject matter was mathematics, literature, or geography, contained pages of encomiums to Lenin and the communist regime. These pages portrayed Lenin as an ordinary boy who was raised by a humble peasant family—just like the rest of us, the little Octobrists. According to these books, he was like a farm boy who herds geese, yet he was extraordinary—dedicated, bright, and hardworking. These were the very

qualities that we were asked to emulate in order to advance the prosperity of communism.

Consequently, textbooks, regardless of their purported subject matter, included sections that praised the communist regime as a political body with a bright future—one whose ever-increasing merits would bring prosperity to all the people. This passionately optimistic view of the future was characterized by equal opportunities for all—by a superabundance of newly manufactured products and recycled goods, and by dedicated workers who cheerfully contributed to collective labor on government-owned land.

Uniformity had a power to materialize the ideals of equality and solidarity: We wore school uniforms; during recess, we were asked to march in pairs—from one end of the school corridor to the other, repeatedly. The purpose of this seemingly militaristic practice was to make us into true believers of the system. As reflected in the shortness of the school corridor down which we dutifully marched, there was no space for questioning the status quo of communist ideology. Communism was embedded in numerous scripted history lessons, augmented by field trips to commemorate the nameless, fallen soldiers or to celebrate the special days for remembering the national contributions of the army, or of women.

Such propaganda contrasted starkly with the actualities that we inhabited. Even when I was a child, I knew that these two realities differed from each other. According to Gessen (2017), the subject who could distinguish between realities occupied a privileged social space—one that the elites of communism exclusively inhabited. Gessen cited a British scholar of Soviet society, Mervyn Matthews, who accurately assessed this privilege by stating: “The leadership of the Soviet Communist Party has, from its early days, been profoundly elitist in its attitudes. . . . In daily life, however, it has always ensured for itself and its close associates with privileges commensurate with these awesome demands” (p. 20).

I knew that those who endorsed the communist regime—in other words, those who joined the communist party, were “protected” by the regime. The government gave them access to material goods that included vehicles. These were considered luxury goods to which the common populace had no easy access. The vehicles of government employees bore three main types of distinctive insignia that indicated their rank within the communist hierarchy. These cars were manufactured in the Soviet Union and considered status symbols. Volga was the most prestigious of the three vehicle types, followed by Zhiguli, then Zaporozhets, a model that represented the working class (Гремин, 2006). While scholars like Siegelbaum (2011) argued that the Soviet car industry operated similarly to capitalism in the Western world,

such expressions of capitalism that emphasized the social class distinction through cars, is merely just one illustration of such contradiction.

Throughout my childhood, I knew that the world filtered through the lens of communist society did not offer equality for all. I could not help but notice the signs of hierarchy. For instance, I knew that in the *kolkhoz*, people were not happy to perform the collective labor they were assigned. My parents were deprived of their land—the property that they had legitimately owned until its privatization by the government. It would not be returned to them till the dissolution of the Soviet Union. I also knew that the general populace required special “tickets” to buy various goods that would become accessible only after years of waiting. I knew that these long Soviet wait lines were forming for basic appliances as well. And people placed at the end of the supply distribution chain of these goods, such as cashiers, had more advantage than the rest because they could function as gatekeepers.

How did everyone deal with the duality of communist ideal versus lived actuality in the Soviet era? For the repressed, silence can be a form of resistance. My generation’s countermovement that resisted propaganda was based on a tacit knowledge of possible alternatives. There are two elements involved here: awareness of two coexisting realities and the lived memory of the past. The former is rooted in the understanding that things were not as bright as depicted. Everyone was aware of lack of progress, yet nobody talked about it. Both versions of reality coexisted. Both were real for us, and yet both were equally surreal. The “silence” aspect of the entire experience marked my generation with at least one family member who had literally been “silenced” for endorsing certain beliefs. My generation lived with an active memory. They lived through our parents’ and grandparents’ experiences of having been silenced, not only metaphorically but also physically, at the hands of an oppressive totalitarian government. Some were killed, others were deported to Siberia, and others were forced to live in exile.

Thus, freedom of speech acquired a very special meaning for me—especially uncensored news reports that could empower future generations. In Lithuania, the oppositional movement targeting the Soviet regime had also been “silenced” before I was born. Thus, my generation became affiliated with the silent countermovement until Lithuania regained its independence—which was the beginning of the dissolution of the Soviet Union.

The disconnect between reality and its various distortions became even more pronounced when Lithuania seemingly achieved overnight independence. Lithuania played a major role in abolishing the Soviet Union as it sought and secured the restoration of its independence. In those times, criti-

cal thinking and the interpretation of reality beyond projected reality were crucial for one's safety, given that the mainstream media were objects of military attack and civilian defense at crisis moments during the independence movement. Lithuania's 1990 proclamation of independence from the Soviet Union had the same surreal quality as the lines of Russian tanks that crawled into Vilnius, the capital city where I lived. Lithuanian citizens, who silently rose up and stood before these tanks, were killed as they clashed with peaceful protesters in order to protect media broadcasting and the main government building from armed destruction by the Russians.

In 1991, the Russian tanks finally left Lithuania, and we returned to school. This overnight change prevented us from acquiring new textbooks immediately. These could not be produced to coincide with the start of a new school year during such times of economic turmoil. Thus, we were given yet another set of textbooks from the same libraries that previous generations had used—those same textbooks chock-full of accolades of Lenin and the continuous upgrade of the Soviet standard of living—even though Lithuania was technically no longer part of the Soviet Union. Although Lithuania was an independent nation—in fact, the first one to secede from the Soviet Union, its schools retained the textbooks written in Soviet times.

These outdated textbooks enabled me to read between the lines—to make sense of a reality that was no longer relevant and that was otherwise known as Soviet propaganda. Without any noticeable change of tone, our teachers told us to ignore propagandistic textbook sections that glorified communist prosperity and to focus on the book's main content instead. Although we were told to “skip” textbook parts that we had to discern as propaganda, we also needed to develop the acuity to recognize instances of propaganda whenever they appeared in the course of our reading. Thus, I had learned to think critically from an early age and to isolate facts from irrelevant effluvia through this textbook information-filtering process. While this entire critical-thinking experience distinguishes my generation from others, I remember that distinctive formative period when I had been explicitly taught how to recognize propaganda—and despite the normalized transition to a new school year in extraordinary circumstances.

During times of radical change, when it was impossible to switch paradigms so quickly, the vestiges of propaganda remained before my very eyes and impacted my life in very direct ways. My early experiences with propaganda also prepared me to understand the postmodernist perception of reality. I would learn that there can be more than one set of ideology. After all, I have lived through more than one. From an early age, I had been exposed to not only propaganda techniques but also strategies for identifying them

so that I would resist their influence in later years. I also retain in my experiential repertoire eyewitness accounts of the discrepancy between communist regime depictions of reality and the everyday actualities that surrounded me.

I am grateful for these experiences and the times I was born into because they have provided me with the lens for seeing the world in ways that I could not have possibly done otherwise. Postmodernism might seem a mere abstraction, but when I learned about paradigmatic inferences, all the dots within the frameworks in which I had been raised suddenly became connected. Today, I reflect on postmodernism by invoking the value of information literacy skills—which, in turn, leads me to ask how we can approach current digital propaganda or, in the words of Macnamara (2020), What are the consequences of post-communication?

Vulnerabilities of Social Media

My personal exposure to ideologically charged affect-soliciting messages and my learned resilience to their influence have encouraged me to value media literacy. In either case, my experiences were atypical ways for learning how to detect and make sense of the ideological thinking that infiltrated everyday life. Yet, thankfully, most people have not been raised in my circumstances. My readers might, in fact, wonder how any of those experiences were possible. Such skepticism is understandable, especially given the status quo of baseline expectations grounded in a democratic media ecosystem that itself is fundamentally situated in debate between politicians, ideas, points of view, and citizens. By contrast, the uninviting, dialogue-deprived environment in which I grew up revealed to me the discrepancy between the told and the lived versions of reality. This overall experience provided me with one of the most powerful life lessons—how to distinguish between multiple truths, and truths that pertain not only to facts but also to belief systems and modes of affect. I did not receive formal training for acquiring media literacy. Instead, I had to learn it on my own to survive in Soviet and post-Soviet societies.

Most people who live in democratic media ecosystems are not expecting to encounter ideologically charged messages pushed by a foreign government. And they can choose silence as a form of a democratic participation repertoire. As argued by Papacharissi (2021), silence is as important as voice. Moreover, it is hard to be prepared to interpret messages within new media ecosystems and a range of platforms that are founded upon the ethos of “anyone can post a comment.” Given that democracy invites multiple points

of view, it also attracts misinformation and disinformation. Democratic discourse online is not only produced by humans but also pushed by bots or automated machine-learning algorithms. Social media has emerged as spaces for personal interaction—initially, for people who already knew each other or who belonged to the same social circles (see, e.g., boyd & Ellison, 2007). Thus, social media was comparable to networks of trust. And even if that comparison can be questioned, it was paradoxically the very ethos that gave birth to social media. More recently, however, social media and new interactive media settings are no longer based on the premise of familiarity. In short, posting on social media can be anonymous, and such posts can be artificially constructed—that is, automated and reproduced.

Thus, we live in an era where social media has become yet another form of mass media that requires formal training for users to identify media-embedded paradigms. The media ecosystem we live in encourages interactions that take place through them. These interactions constitute a blend of mass media and interpersonal communications, or what has been called the *masspersonal* (O’Sullivan & Carr, 2018). What does this mean for persuasion? There are too many ways to interpret content, and in media literacy studies, too much emphasis is placed on individual responsibility (boyd, 2017). Individual responsibility requires every media user to acquire proficiency in evaluating media sources and to access various interpretations of information from multiple sources where policy-driven approaches and media literacy become critical (Balčytienė & Juraitė, 2017).

However, while challenging, media literacy is particularly critical to combat propaganda since propaganda has been defined as the “means to communicate ‘truth’ to the ignorant” (Pratkanis & Aronson, 1992, p. 255). It is also linked with the concept of information warfare—given that propaganda has been strategically deployed during times of war and can remain applicable to other times that are characterized by other forms of uncertainty (Choukas, 1965). Denial, as warfare tactic, here is conceptualized as a rhetorical tactic to justify the Russian trolling phenomenon, similar to a tactic found to be useful for cyberwar coercion, as argued by the cybersecurity scholars Borghard and Lonergan (2017).

In the current age, propaganda and cyberwar coercion have been codified and delineated by scholars in various domains. Propaganda today can be microtargeted in sophisticated automated ways. As such, propaganda no longer resembles early persuasive tactics that can be described like “shooting in the dark.” Consequently, persuasion techniques today are the fruits of years of labor and fine-tuning. Choukas (1965) wrote, “Today many of the techniques by Goebbel’s ministry are being employed even more effectively

by our subsequent adversary” (p. iv). He continued: “A first step in our efforts to neutralize their effectiveness is recognition of the fact” (p. iv). As he described, the ability to recognize underlying meanings of messages is crucial for interpreting disinformation.

This book exposes the ideological trolling techniques that go beyond fact-based persuasion. These new types of persuasion are based on the sociotechnicality of new spaces that allow for new actors to thrive. These decentralized spaces are forums where anyone can contribute, and they are designed to foster democratic debates. Since messaging operates in such decentralized online spaces, it can be used as yet another computational propaganda tool.

Throughout this book, propaganda is treated as the antithesis of the democratic process. Debate is central to the democratic process as the rhetoric that clarifies actions within societies, the template for which is ancient Greece; it advocates for the meaningfulness of debate (see Pratkanis & Aronson, 1992). Thus, this book argues that the current media landscape subverts debate as a democratic rhetorical process that clarifies meaning. Instead, debate is used to push agendas and to obfuscate meaning—the major catalyst for such unconstructive debate being the Russian trolling phenomenon.

This book treats the online spaces designated for news portal comments as the information warfare battlegrounds based on democratic paradigms. The rise of Web 2.0 and user-generated content does not necessarily provide new spaces for online interaction. In fact, Web 2.0 also creates new contexts for the information distortion intended for subversive purposes. When considering online influence and current propaganda models, today’s propaganda exemplifies what I call Propaganda 2.0. By this phrase I mean the interactive spaces where all users can participate, including those who attempt to destabilize the focus of online discussions. Propaganda 2.0 is digital, ephemeral, and yet far-reaching. Thus, it is much more sophisticated than previous propaganda models. Entrenched in the newest communicative platforms, it circulates within spaces designated for today’s most informed citizens, such as those who belong to technology-savvy circles.

This book focuses on information tactics through the lens of a phenomenon of Russian trolling to discuss information warfare due to the recent proliferation of Russian troll farms in the European (in particular, Lithuanian) media landscape and how they resonated in the 2016 US presidential election. To successfully analyze disinformation, cross-platform analyses are viewed as a gold standard (Bennett & Livingston, 2018). I employ cross-platform and cross-case analyses to draw parallels of how Russian troll justification across a range of media sources. Analyzed media sources draw empirical analysis of the comments from the US news portals labeled as

liberal (*New York Times*) (e.g., Benkler et al., 2018) and *Breitbart* that has been categorized as an extreme news site, treated as a news portal that aims to radicalize their audiences or is known as a “Republican-aligned” source (Peck, 2019). For a cross-platform comparison far-right social networking site Gab.com (later referred as Gab) was analyzed. To compare these findings, US news portals were compared to a Lithuanian Delfi.lt news comments, thus allowing to cross-validate and compare findings between two diverse sociopolitical contexts.

This book, furthermore, demonstrates that the Russian trolling was justified in the Lithuanian media with the similar rhetorical arguments used in the US news comments. At the core of it is the victim-playing frames by Russian trolls found across analyzed sources that resonate with the alleged “Russophobia” frames—i.e., where Russians are allegedly blamed for everything and hated by the “West.” These Russophobia frames have been found to be prolifically used inside of Russia as a narrative to the Russian people before the Russian-Crimean conflict as Darczewska and Żochowski (2015) argued, to justify the annexation of Crimea.

The Lithuanian Delfi.lt case is critical to illustrate the information warfare and disinformation campaigns. First of all, the use of Russian trolling in the Lithuanian news portals emerged at the onset of the Russian interference allegations in the 2016 US presidential election. Additionally, Lithuania serves as a significant case study, because its former Soviet satellite status could render visible any Russian influence in its news portal comment spaces. As Orenstein (2019) put, experiences of Eastern European countries, are valuable early-warning systems. Examples in this book from the Lithuanian news portals showcase how Russian trolling justification was presented to potentially stir chaos in the Lithuanian readers’ minds as then, the same arguments were used to justify Russian trolling after the 2016 US presidential election.

The information warfare through trolling can be attested through a recent study of the Lithuanian news portals comments (Zelenkauskaitė & Niezgodą, 2017). According to a review of the pervasiveness of Russian trolling, in 2016 alone, 2,284 (0.57%) of 400,633 comments on the Lithuanian news portal Delfi.lt included the word “troll” (Zelenkauskaitė & Niezgodą, 2017). Out of 5,358 Delfi.lt stories posted in one month, 706 (13.2%) drew user comments containing the word “troll.” Interestingly, trolling was not mentioned in any of these story headlines or in the actual text of the stories. Rather, the comments were frequently posted to call out Russian trolls in the news portals. There were 1,120 unique users who posted comments related to Russian trolls. The number of times these user comments mentioned the

word “troll” ranged from 1 to 117. Moreover, 304 users (27%) posted more than one comment containing the word. Of 2,284 comments, 463 featured “troll” within heading spaces; 1,888 included the word within main body sections; and 67 included it within both heading and main body spaces. Of the total number of comments containing the word “troll,” 46.1% were replies to prior postings. In the sample where the word was never mentioned, 35.2% of comments were replies (Zelenkauskaite & Niezgodna, 2017).

While this descriptive statistical overview indicates that Russian trolling has been a public concern, it remains unclear how it is conducted and how to make sense of the phenomenon. Ever since Russian trolling had been exposed, news portals have provided various guidelines for recognizing Russian troll comments, as the following excerpt indicates:

It is important to see how Kremlin’s strategists take advantage of social networking sites to achieve a desired scope. . . . Visible “trolling” examples are seen about the discussion on forest rarefaction is presented as a news spread as if they are rarefied to create space for NATO [military] exercises are in need in larger polygons; when discussing children’s rights, ‘trolls’ provoke the society about so called “Western tradition” when children are taken away from their parents and are given to gay couples, and it is only Eastern countries that maintain traditional family values. Propaganda is an art to find certain hooks themes, and subthemes, that allow to escalate division in the society. (Delfi.lt, “Rinkimai—palanki terpė,” 2018, para. 15)

Clearly, the focus on Russian trolls emerged from the escalation of Russian interference in the 2016 US presidential election. More specifically, it was discovered that Russia had mobilized the support of compatriot communities in the Baltic states by exercising “soft influence” (Simons, 2015). Country-specific perspectives become particularly compelling when information warfare escalates—when nations assert their own opinions, positions, and sometimes even propaganda (Thornton, 2015). User-generated content, in particular, provides a *terra franca* in those contexts: loosely codified practices allow for various types of behaviors, some of which are deliberative, while others are perpetuated by governments, despite their resemblance to grassroots initiatives. If Russian trolling is a phenomenon that is based on mere conjecture, then, it represents one of the multiple voices that characterize the democratic process. However, if Russian trolling is orchestrated by the Russian government to influence elections, then it is no longer a grassroots activity.

News portals comments sections offer unique platforms for deliberative and foreign government influence because they allow all internet users to comment. Online platforms enable two-way communication where any user can post his or her own interpretations of given phenomena and others can respond, ensuring a debate. At first glance, comments in democratic contexts seem to open up spaces where meaningful debate is an illusory concept rather than a reality. After all, some may argue that news story comments or social media posts represent the margins—or at the very least, the periphery of a media ecosystem whose core is professional journalistic content. Within that discursive context, news story comments are positioned as secondary relative to the news stories that are typically produced by media professionals, or journalists.

The secondary or “in the margins” positioning of news comments and social media posts provides a false sense of security that they do not matter or influence anyone’s perception, contrary to evidence found by various researchers described in this book. This false sense of security derives not only from the professionally uncoded nature of their content but also from that content’s online spatial placement and from the user who generates it. Specifically, comments appear only after the main text of news stories, as internet users scroll down on computer screens to access them. Moreover, comments target the general news portal reader public—not experts or journalists—as primary contributors. Yet, in the context of ideological function, it is not the content substantiality or their seriousness that is questionable in the comments. The chief concern is that comments offer perfect spaces for ideological influence. Since comments are not in the spotlight, they are vulnerable to influence. Thus, they become online spaces that morph into ideological battlegrounds. While there is much debate about social media spaces as potential battlegrounds, online commenting remains somewhat overlooked from this standpoint, notwithstanding the emergent paradigms such as dark participation referenced in this book (Frischlich et al., 2019; Quandt, 2018).

Creating Chaos Online exposes the resurgence and subsequent amplification of disinformation that infiltrates such media ecosystems at their margins—comments as a form of user-generated content. This book also exposes the striking resemblance of this infiltrated content and the similarity of the recurrence of justification frames to the former Soviet regime’s disinformation propaganda tactics. Yet these examples have been found in the current democratic media landscapes, where disinformation is circulated through the information communication technologies that are comparable to the former Soviet Union’s totalitarian media influence techniques.

To sum up, the resurgence of propaganda in the democratic media ecosystem through decentralized user-generated content spaces, such as social media, can be quite paradoxical for various reasons. First, social media is considered mundane. It is typically used for interpersonal purposes such as feeding into a range of subcultures, be it selfies or sharing food pictures online. Yet social media can be powerful when users appropriate it as a medium for persuading the masses. Second, arguments are taking place in democratic countries that have historically employed rhetorical techniques to persuade others. However, one fact is clear: Social media, as a decentralized networked mass medium, can be weaponized and used for information warfare. Such weaponization is possible through the infiltration of foreign propaganda and by simply using social media to expose users repeatedly to affective content.

Trolling and Russian Trolling

While the treatment of Russian trolling throughout *Creating Chaos Online* intends to uncover the online discursive tactics as means of disinformation, it is imperative to discuss how Russian trolling taps into the broader notion of internet trolling. Trolling has become inseparable from online social media, as argued by, for example, Sun and Fichman (2019), or even as a type of online sub-culture that reached the mainstream (Phillips, 2015). While typologies of trolling are extensive, such as provocation, social engineering, grooming, partisan, firehose, ad hominem, sport, snag, jam, nuisance, diversion, false flag, huckster, amplification or relay, and rehearsal, as summarized by Berghel and Berleant (2018), all share deviant, malicious repetitive behavior and are based on individual motivations such as boredom or disruption. Trolls have also been found to be motivated by an ideological agenda (Bulut & Yörük, 2017; Sanfilippo, Yang, & Fichman, 2017). For example, Fichman and Sanfilippo (2016) defined trolling as “a repetitive, disruptive online deviant behavior by an individual toward other individuals or groups” (p. 6); political trolls with a specific ideological agenda have emerged to exemplify a specific type of trolling.

In a case of Russian trolling, ideological positioning has been further accompanied by allegations of foreign government-sponsored activities aimed at compromising the democratic premise and create chaos online (e.g., Bessi & Ferrara, 2016; Jamieson, 2018; Shane, 2017; Zannettou et al., 2018). Russian trolling has been analyzed through various lenses; however, its relationship to disinformation techniques as potential means

of political influence continues to linger not only in the aftermath of the 2016 US presidential election but also in various parts of the world (e.g., Woolley & Howard, 2018).

Trolling is also considered a volatile, contextually grounded phenomenon. This volatility and context dependency renders it hard to grasp. Furthermore, it captures perceptual realm in addition to its manifestations, as argued by Rosamond (2019). This book works to uncover treatments of Russian trolling by particularly focusing on its tangibly accessible manifestations. In the news stories comment sample, the analysis starts with the stories that covered Russian trolling, and comments left on those stories. Comments were analyzed to identify how Russian trolling was interpreted. In addition, on a social networking site Gab, a public search of the term “Russian troll” was used to gather instances. Considering the prevalence of Russian trolling coverage, this book asks how affective themes and trolling are exploited further to discuss Russian trolling as a phenomenon, especially to justify it or absolve it.

This book asks not only about the themes that justify Russian trolling but also the nature in which they are presented. It can be expected that online justification can use some of the common techniques, for example, by internet trolls. Typical techniques used by online trolls include triggering to raise emotional response (Fichman & Sanfilippo, 2016) and mocking (Clarke, 2018). Baiting online to engage in perpetual meaningless responses, thus shifting attention from the main topic, is yet another manifestation of trolling (Herring et al., 2002). Early research on trolling suggests that trolling exploits existing tensions in the group. Herring et al. (2002) argued that trolls typically exploit the freedom-of-expression norms of a group, making it more difficult for a group to take an action against such behaviors. Finally, three types of “masks” were found to be used by trolls in their messaging: appearing outwardly sincere, engaging in messages that predictably attract a response, and wasting the respondent’s time in futile arguments (Herring et al., 2002). In this book, trolling techniques were similarly found and applied to justify Russian trolling.

Here I document repetitive justification frames legitimizing or excusing Russian trolling behavior, found and circulated in spaces of user comments across social media, despite the release of former US special counsel Robert Mueller’s compelling evidence by asking how what types of arguments were circulated. Mueller’s report addresses Russian trolling accordingly:

Instagram accounts had hundreds of thousands of US participants.
IRA [Internet Research Agency]-controlled Twitter accounts sepa-

rately had tens of thousands of followers, including multiple US political ones who retweeted IRA-created content. In November 2017, a Facebook representative testified that Facebook had identified 470 IRA-controlled Facebook accounts that collectively made 80,000 posts between January 2015 and August 2017. Facebook estimated the IRA reached as many as 126 million persons through its Facebook accounts. In January 2018, Twitter announced that it had identified 3,814 IRA-controlled Twitter accounts and notified approximately 1.4 million people Twitter believed may have been in contact with an IRA-controlled account. (Mueller, 2019, p. 23)

The report concluded:

Social Media Influence in the 2016 US. Election, Hearing Before the Senate Select Committee on Intelligence, 115th Cong. 13 (11/1/17) (testimony of Colin Stretch, General Counsel of Facebook) estimate that roughly 29 million people were served content in their News Feeds directly from the 80,000 posts over the two years. Posts from these Pages were also shared, liked, and followed by people on Facebook, and, as a result, three times more people may have been exposed to a story that originated from the Russian operation. Our best estimate is that approximately 126 million people may have been served content from a Page associated with the IRA at some point during the two-year period). The Facebook representative also testified that Facebook had identified 170 Instagram accounts that posted approximately 120,000 pieces of content during that time. Facebook did not offer an estimate of the audience reached via Instagram. (Mueller, 2019, p. 118)

This statement clarifies the extent to which social media users have been publicly exposed to messages that they believed were from other verified users. Yet those posted messages were intended to create or reinforce ambiguity about the communication of critical issues during the US presidential election. Similar approaches to trolling have been identified in the Lithuanian media following the publication of stories about operations of Russia's government-sponsored Internet Research Agency. But in this book, Russian trolls are treated as operatives who are directed and paid by government agencies to promote ideas through the commenting process.

Understanding how Russian trolling is reflected in user comments is particularly pertinent given the alleged skepticism about Russian trolling

that circulated online in 2018 in some mainstream media sources and in comments, even after Russia was identified as one of the most aggressive cyberspace actors, creating and amplifying propaganda efforts against the governments of a given targeted state (Valeriano et al., 2018). In response to the doubts seeded by the denial of Russian trolling, much effort has been expended to provide evidence for its existence, extensively reviewed in this book and proposed in Mueller's report, or the effects of social media regarding political influence, as argued by Vaidhyanathan (2018). This book does not ask these questions. Instead, it questions how a perception of Russian trolling can be shaped by using divisive rhetoric that leads to more obscurity than clarity. This rhetorical device construction to justify Russian trolling has been analyzed in online comments in the aftermath of the 2016 US presidential election (for US sources), when both scholarly articles and journalistic pundits started to question sources of evidence to identify the originators of influence.

These rhetorical Russian troll justification frames are treated as a type of influence and it is detailed here through the various lenses, including astroturfing. To capture this complex and multifaceted phenomenon, this book approaches the Russian trolling justification rhetoric by contextualizing it through an array of fields and grounding it in scholarly literature. This book applies a range of theoretical and conceptual lenses to map and capture a multifaceted picture of what Russian trolling as a phenomenon entails by baring evidence from various disciplines.

This book foregrounds assumptions regarding typologies of online influence by departing from a recent account on Russian trolling provided by the scholarly community. One of the assumptions is the role of information warfare in the current media and political systems. Jamieson (2018), in her account of Russian trolling, specified the role of information warfare in the 2016 US presidential election. Her observations were based on the public information of US intelligence documents proving that trolling substantially influenced the election. This book provides parallels to what Jamieson exposes as information diffusion practices of the former Soviet Union's propaganda factory. Such propagandistic information diffusion are derived from the efforts to determine seeding spaces that could serve as credible evidence of widespread Russian trolling. However, we continue to ask the same question: What is Russian trolling if it retains the potential to influence future presidential elections worldwide?

This book asks what other actions are required apart from publicizing a factual exposé of Russian trolling? *Creating Chaos Online* offers a systematic analysis of the discourses that either justified Russian trolling or that

generated skepticism about its existence. After all, the subliminal quality of Russian trolls begs for clarification. Thus, this book adopts a definitional perspective for the term “Russian trolling.” This is the term to which internet users resort when posting online and to which journalists refer when producing news stories. While there has been much discussion about what constitutes trolling in the US media, especially in the aftermath of the 2016 US presidential election, Russian trolls, in general, have been treated as paid operatives. Mueller (2019) offered his own definition in his report, according to which trolls are “internet users—in this context, paid operatives—who post inflammatory or otherwise disruptive content on social media or other websites” (p. 23).

Another assumption is that of their visibility. The goal here is to render the Russian trolling phenomenon visible by approaching it from various angles. These angles become entry points—the doors that enable access to the rather ephemeral phenomenon of Russian trolling. Thus, Russian trolling in this book is mapped out by considering its wide-ranging contexts. These contexts allow us to engage in a broader discussion about the origin of the Russian trolling phenomenon and strategies for approaching it. The visibility of Russian trolling is enabled through the lens of information warfare, a concept that is closely related to ideological trolling and to a confluence of other phenomena.

This book addresses the mechanisms for creating the online chaos that shifts attention from crucial issues to trivial or irrelevant ones and that manipulates perception through information overload. And silencing of the new era can take new shapes: it shifts from the censoring or exclusion of certain information to an abundance of information that serves to deflect—through concepts of *infoglut* (Andrejevic, 2013) and *information flooding* (Roberts, 2018), discussed in subsequent chapters. *Creating Chaos Online* details the effects and on-the-ground evidence of online information warfare by focusing on denial as a discursive tactic. This book particularly focuses on chaos construction as a form of disruption through the efforts of degradation resonated in the news portals comments. These include astroturfing, a phenomenon that is related to the political influence that trolling enables.

Together with propaganda and ideological formations, astroturfing could escalate into what Jamieson (2018) has called cyberwar. Cyberwar identifies *where* attacks take place. It also implies the *what*—that is, the types of activities that take place, such as hacking, posting, impersonating, strategic information management—in other words, the tactical release of information. Moreover, Jamieson claimed that cyberwar “invites us to see perpetrators as enemies, casts hackers and trolls as soldiers, saboteurs, and spies, sees

how the US president as commander-in-chief; creates the expectations that attacked country will retaliate; and implies the value of inviting its public to arm itself” (p. 9).

The observations of others, like Benkler et al. (2018), went beyond online digital spaces to refer to the mass media network’s influence, calling this phenomenon network propaganda. Woolley and Howard (2019) referred to digital cyberspace as computational propaganda. While traditional propaganda frames have aimed for a specific agenda or target population, they have proved comparatively inefficient in the current sea of online information. In other words, it is hard to break through the cacophony of voices. And that is because information warfare seems to adopt a model that is antithetical to the one on which traditional propaganda is based: chaos. Thus, where Russian trolling is concerned, information warfare is the framing lens for understanding chaos as a militaristic tactic.

Within the contexts of foreign and domestic government influence, the current media landscape has been treated as the backdrop for computational propaganda (see, e.g., Woolley & Howard, 2018). Throughout this book, the term “computational propaganda,” is used in reference to any online spaces, including not only social networking sites but also news portal comment spaces. By claiming that information warfare is assuming various forms in online spaces, I depart from mainstream approaches to digital influence in social networking sites. Influence can take place across platforms, such as WhatsApp or Reddit, depending on the use of those spaces in a specific sociocultural context. However, scholars such as Woolley and Howard (2018) have focused on social networks as the most immediate spaces for computational propaganda.

Online comments provide a fertile terrain for analyzing the information battlefield. And, it has been observed that the commenting behaviors of Russian trolls differed in structure and content from those of regular internet users (e.g., Zannettou et al., 2018). While there have been multiple studies that have analyzed US social media in terms of political influence (e.g., Bessi & Ferrara, 2016; Shane, 2017; Zannettou et al., 2018), *Creating Chaos Online* offers an analysis of partisan extremes together with a comparison of local and national news commenting spaces. Thus, the book’s objective is to explicate the ways in which influence can be used in online spaces, and the ways in which information, discourses, and online actors variously contribute to its proliferation.

Since this book continues to emphasize the significance of news organizations as sources of public information, the question arises: How can news organizations operate in the challenging situation they inhabit? On the

one hand, they are expected to engage with audiences by encouraging news assessment. On the other hand, they are obliged to negotiate public interactions that could be sponsored by foreign governments. Thus, while filtering comments, news organizations must distinguish between posting users: those who are authentic news readers, and those who are government affiliated (e.g., Russian trolls). And even as these news organizations have been nurturing civility for their reader comments, today they need to address challenges of dark participation as battlegrounds of information warfare that inadvertently take place in the news comments.

This book uses astroturfing as a framework—the deliberate posting of users, usually paid to infiltrate grassroots movements by impersonating activists. Thus, astroturfing is a propagandistic technique that Russian trolls use not only to shape public opinion but also to provoke more uncertainty. In fact, Russian trolls generate uncertainty through quasi-authentic self-presentation in online spaces on behalf of other parties, such as foreign governments, here discussed through a lens of a mask. This treatment of the public sphere goes beyond mere “uncivil” discourse. And this book showcases how news organizations have become victims of Russian trolling operating in their comment sections, which are accessible to their nurtured readership segments.

Creating Chaos Online highlights a paradoxical problem concerning news portal comments. On the one hand, they provide deliberative potential according to the democratic tradition. On the other hand, online deliberative spaces become targets for foreign government interference. In other words, how are authentic practices of self-expression subverted by what can be perceived as foreign mercenary interference? How do online discourses acquire the vestige of information warfare? While this book addresses these questions, it also focuses on comments and their discursive significance. Another player in this equation is the rise of new communication technologies that highlight the ubiquitous nature of platformed media. New communication technologies renew the promise of freedom of speech, but those same technologies create new constraints and generate new doubts about the authenticity of online public deliberation.

Similarly, this book scrutinizes the relationship between Russian trolling and online incivility and online trolling. Yet this book demonstrates how Russian troll justification arguments have capitalized on tactics typically found by online trolls, thus seeding ambiguity between incivility and foreign interference. It is less disconcerting that online incivility is rampant in newer democracies—that crudeness of expression is prevalent in the online comment spaces that they offer. Rather, it is more troubling that news portals are

becoming information warfare arenas where international politics are also staged. In other words, online deliberations take place in an active information battleground. In so doing, they contribute to the ongoing information warfare that has been defined as the use and management of information, and of communication technology, to achieve a competitive advantage over an opponent (Thornton, 2015). In the case of Russian trolling, it is the foreign actors who engage in creating influence.

This book aims to expose news portal comments and far-right social networking sites such as Gab as online media spaces that typically are treated as the marginalia compared to professionally produced mainstream media. However, this book argues that news portal comments and social media posts can serve as important early-warning systems of public sentiment—which at times is not only highly shaped by democratic voices but also tainted by rumor-based propaganda or disinformation to achieve specific agendas. Such online marginalia can significantly impact the paradigmatic warfare between democratic and nondemocratic constituents. Nondemocratic paradigms are driven by populism, post-truth, and chaos.

This book also moves beyond two major attributes of online (social) media: anonymity and automation, as already postulated by Woolley and Howard (2018). However, anonymity and automation are sociotechnical affordances integral to online platforms' fabric. Since we cannot entirely eliminate the potentially challenging ways in which they are used online, we must constantly update awareness of their changing contexts and effects.

To address this question, this book focuses on several objectives, including highlighting discourse-based mechanisms, providing an interpretative paradigm-based key for reading them, and exposing the contexts from which messages emerge. Central to the formation of these contexts is the increasing ubiquity of media in daily life, given that increased information circulation and access provide more instances allowing various types of influence to occur. Social media and news portal commenting can be positioned as parallel to traditional modes of mass media influence—television, newspapers, and radio. Social media represents new means of networked message distribution, produced by regular people and potentially by any other forces of influence.

Russian Trolling Circulation

This book is based on an empirical analysis of comments responding to Russian trolling stories published in four platforms: the sources *Breitbart*

and the *New York Times*, US news portals known for endorsing mutually oppositional ideological perspectives; the Lithuanian news portal comments at Delfi.lt; and Gab.com, a far-right social networking site. Data were collected during the investigation of the Russian trolling interference in the 2016 US presidential elections were still ongoing and ended with the stories collected: The time frame of data collection for this project included the stories that emerged after the Department of Justice (DOJ) announced the indictment of Russian trolls on 2018 February 16, and ended before Mueller's report was publicly released by the DOJ on 2019 April 18, for the US news portals *Breitbart* and the *New York Times*. From Gab, publicly available posts and data were collected retroactively: going back to February 2019 to capture instances of public postings through the keywords "Russian troll." Lithuanian comments were based on stories covering Russian trolling from the Lithuanian news portal Delfi.lt (e.g., Meidutė, 2018) that generated 818 comments. News story sources and types are summarized in the Appendix.

Throughout this book frames are conceptualized based on media Framing theory—where introduced frames “function to suggest how audiences can interpret an issue or event” (Tewksbury & Scheufele, 2019, p. 17). Media framing practices consider news a means of promoting the ideals of democratic deliberation.

Approaches of the systematic analysis of online comments included a combination of qualitative and quantitative approaches: Quantitative duplicate analysis was conducted to analyze content circulation repetition, quantitative content analysis measured the proportion of comments that used justification frames of Russian trolling, qualitative thematic analysis uncovered a list of Russian troll justification type frames, and the qualitative nature of the top users posting patterns. Users were also categorized regarding masking practices, i.e., between those who chose to register to post or remained anonymous (analyzed for *Breitbart* and Delfi.lt).

This research asked to what degree Russian trolling took place, how it was framed, and how the frequent users promoted or did not promote Russian troll justification. This book starts with the premise that if there is a common list of Russian justification theme frames, they belong to the same playbook. Metrics were combined with several approaches to produce these three outcomes for Russian trolling analysis: First, the creation of a reliable data set to isolate news stories that covered issues concerning Russian trolls (i.e., through keywords related to Russian interference in the US presidential election and the news story on Russian trolls in Lithuania); second, the analysis of user news comments of specific stories for news portals and comments mentioning Russian trolling on Gab; and third, the identification of

conversation entry points to reconstruct specific message threads in which users referred to themselves as “trolls.” This third process generates a sense of user perception of (Russian) trolling in online news portals and was coupled with content circulation analysis through duplicates by anonymous or registered users.

My analysis begins with the emergence of the Russian troll narrative in news portals and includes not only stories but also comments that were prevalent in 2015 in Lithuanian news portals (see Zelenkauskaitė & Niezgodą, 2017), even if data for this book are drawn from 2018. I provide large-scale quantitative and fine-grained qualitative analyses of the treatment of Russian trolling in news comments. My analyzed sample covers the year 2018 and examines 13 news stories from *Breitbart* with 37,137 related comments and 17 *New York Times* news stories with 3,431 related comments (10 had no comments). In addition, the publicly accessible far-right social networking site Gab was analyzed, where posts containing the keyword “Russian troll” were aggregated in February 2019 before the social networking site was shut down for federal investigation into the Pittsburgh synagogue shooting (Matsakis, 2018). Finally, given that Russian trolling circulated before it escalated in the US media, Lithuanian news portal comments on Russian trolling were sampled from 2018 (see Meidutė, 2018), and contextualized with the findings by Zelenkauskaitė and Niezgodą (2017) on the topic.

Which types of Russian troll justification were used? How were they related to the Russophobia frames or to other propaganda techniques? To address these questions, two topics are discussed throughout this book: the forms of justification for Russian trolling across news portals and the Russian trolling denial frames that exemplify information warfare. Analytical procedures of this study included the following: Quantification of automatic practices was conducted by the analysis of repeated and anonymous posting for the entire *Breitbart* sample. Theme analysis to identify disinformation techniques was conducted for the subsamples of each media outlet: *Breitbart*, Gab.com, Delfi.lt., and the *New York Times*. Given that theme analysis revealed a dichotomy in the treatment of Russian trolling—on the one hand, it was argued that Russian trolling existed, and on the other hand, that it did not—these positionings have been further quantified.

Breitbart and the *New York Times* (due to their contrasting political ideology), were compared how news stories about Russian trolls have been treated in the comments. “Trolls do not exist” was found in 40% of comments on *Breitbart* news stories, compared to 18% of *New York Times* comments.

Theme analysis and its quantification was done by manually coding messages and categorizing the techniques associated with them. The *New York Times* subsample included 1,796 comments across seven news stories on Russian trolls (other stories had no comments). The *Breitbart* analysis included a subsample of 2,061 comments from 15 news stories on Russian trolls (other stories had no comments). News stories had prolific comments that ranged in number from 18 to 1,635.

Justification typology and context analysis has become the core of this book, in light of the finding that justification of this online phenomenon comprised 18% and 40% of all related news story comments for the *New York Times* and *Breitbart*, respectively, as noted above, while the rest of the comments were neutral, unrelated, or acknowledging and discussing effects of Russian trolling. In addition, prominence of the mentions the word “troll” were analyzed showing that 16% of the comments contained it (15% in the *New York Times* and 17% in *Breitbart*), as detailed in Tables 2 and 3. What do these percentages imply? Consider that comments frequently refer to Russian trolling issues and that many promote pro-Russian narratives that justify trolling in response to stories about interference in the US presidential election process. While this study did not aim to analyze who is behind these messages, the mere prevalence of these narratives supporting Russian trolls is a significant finding.

To address the prevalence of Russian trolling denial frames across media sources, this book identifies tactics that have been used to legitimize Russian trolling in news story comments. The prevalence of comments that justified Russian trolling led to a fine-grained analysis of themes associated with them. The dominant discursive tactics used throughout the news portal comments were Russian troll denialism, accompanied by various types of justification frames and arguments. This analysis shows that in 2018, two years after the 2016 US presidential election, when the online phenomenon of Russian trolling had been exposed, comments defending Russian trolls as innocent were embedded in news portal spaces across all analyzed sources—the *New York Times*, *Breitbart*, Gab, and Delfi.lt—thus indicating the need for a unified framing of this phenomenon pushed across interpersonal user-generated content social media networks.

Chapter 1, “Propagandistic Masquerade,” is the first piece of the mosaic: In it, the mask is set to uncover efforts to deny the existence of Russian trolling. Overall, Chapter 1 summarizes Russian trolling tactics and positions them as online propagandistic masquerades by using the notion of a performative presentation of self (Goffman, 1967) and Danet’s (1998) online

construction of masks through text. In the broadest sense, this chapter asks how invisibility online and masking is projected and how in Russian trolling mask is a staging element used in propaganda in the past and how it is translated into online spaces.

Masks represent online personas for users who are bent on creating chaos. Some of these personas are identifiable as authentic users who amplify ongoing arguments or who initiate new ones. Lithuanian news portals reveal the efforts of such users to conceal their internet protocol (or IP) addresses while posting comments. But why resort to this subterfuge? Similarly, anonymous posting analysis has exposed *Breitbart* message masking, together with evidence of automation of numerous comments that have been duplicated across news stories. Mask as impersonation is further exemplified by recent computational propaganda tactics that include IP address concealment and user anonymity.

This chapter approaches online comments spaces as sites for staging propagandistic masquerades, thus connecting the propaganda of the past with its current forms of disinformation through masks. Such masquerades involve the creation of characters that dismiss Russian trolling by users who impersonate Russian trolls. These characters adopt conflicting voices. While some of them claim “I am a Russian troll,” others call out Russian trolls by saying, “You are a Russian troll.” These two user positionings illustrate the process whereby chaos seeds distrust and uncertainty. Thus, instead of generating certainty about what is happening, these contrasting approaches to Russian trolling exemplify the propensity for chaos while also instilling distrust and weakening the ability to identify the presence of Russian trolls. Consequently, the ultimate outcome of chaos is unresolvable uncertainty.

Chapter 2, “Divide and Conquer,” further addresses the techniques of Russian troll justification in a form of the exploitation of political polarization in news comments. Chaos is rendered visible by comparing the arguments that justify Russian trolling with those embedded in traditional propaganda models. The propaganda of then and now is further connected by linking the construction of disinformation arguments. Such arguments are based on not only deliberate distortion of information but also conspiracy theories and the discursive maneuver of blaming political opponents. More specifically, such arguments incite partisan division through statements such as “It was Hillary Clinton’s trolls.” They focus on the same objective to create division by invoking other digressive issues, such as voting rights for illegal immigrants. Thus, they falsely equate, through juxtaposition, two issues that are unrelated, or at best only remotely comparable. This rhetorical strategy deflects attention from the topic of Russian troll interference to other issues.

Deflection in news portal comments creates chaos by inciting political polarization—by attacking political opponents and by invoking controversial issues, such as fear-instilling and hate-provoking topics such as immigration or voting rights. These types of techniques are explained through the lens of what Davis (2020) calls antipublics. The antipublic sphere is distinguished by disregarding the ethical principles of the democratic public sphere: that is, deliberation, mutuality, reciprocity, and so on. In contrast, these groups promote visions of racism, misogyny, science denial, and social division. Discourses typically attributed to antipublics or the far right have been found to be utilized to justify Russian trolling. In Lithuania, such divisive topics include emigration, topics related to Soviet nostalgia, and internal politics, such as political parties and politicians who are vocal Russia's critics.

Deployment of conspiracy theories is another item covered through the propaganda of then and now. Conspiracies can become discursive weaponry for targeting what commenters on “both sides” call “the gullible.” In this, the efficacy of conspiracy is based on third-person rhetoric whereby “it is not I” but the “others” who are susceptible to influence. Chapter 2 discusses how conspiracy theories have been used to enforce propaganda. Russian trolling comments reveal two opposing narratives: On the one hand, such comments claim that “Russian trolling could not have happened,” while on the other hand, they insist that “Russian trolling has occurred because people are ‘gullible.’” The gullible people, in such instances, are the victims of Russian trolling. According to information science experts, conspiracy theories are particularly compelling coping mechanisms during times that threaten to disempower users (Lewandowsky & Cook, 2020). On the *New York Times* and *Breitbart*, blaming the “opposite” side was a major argumentative strategy. Such strategies that involve othering, by blaming those constructed and invoked “others,” can incite discord—the online chaos that lurks at the margins of comment spaces.

Chapter 3, “Instilling Mistrust in Institutions,” further addresses how government and media institutions were attacked by instilling mistrust in them and at the same time justifying Russian trolling. This chapter discusses how news organizations were blamed in the comments that they provide for the users with the intention of public deliberation. This chapter discusses dilemmas related to the public sphere that news organization have to address to balance between public sphere and dark participation. The chapter begins with the vulnerabilities of online news comments as spaces for “dark participation,” which refers to foreign influence in online news commenting. The chapter also specifies examples of how online news comments about Russian trolling stories are used to discredit media institutions and to undermine

their efforts to report on Russian trolling. It concludes by providing examples of how news organizations in European Union countries have combated Russian trolls, not only through the legislative front, extensively described by Barrinha (2018), but also through grassroots initiatives. One such case is the volunteer-run elves in the Lithuanian news initiative.

Chapter 4, “Roots of Russia’s Victim Playing,” provides another piece of the overall mosaic of the Russian trolling phenomenon—that is, the socio-political projection of techniques originating in and used in Russia. This chapter traces critical points that played an important role since 2000 in the ways Russia perceives information infrastructure and information warfare to illuminate why Russian trolling earned this name and reputation. This chapter covers a sociopolitical positioning of Russia that enables us to make sense of Russian trolling and chaos projection. The chapter provides historical examples of how chaos was used to instill doubt in Russia—that is, through the face-value denial based on irrational assumption (“it could not have happened”) and by evoking Russophobia. Such comments resemble arguments that justified Russia’s annexation of Ukraine and that proliferated throughout the former Soviet Union.

Chapter 4 shows how Russian trolls are justified by being presented in online comments not as perpetrators within those spaces but as victims. Russophobia-based arguments position Russians as victims of the rest of the world. In such a view, Russian trolls have been justified as being allegedly victimized or blamed for many things—frequently and unfairly. This chapter shows how such rhetorical strategies of self-victimization that originated in Russian propaganda campaigns, such as those deployed during the war with Ukraine, when prevalent Russophobic discourses incited Russians to represent themselves as victims who were xenophobically stigmatized, used “then” are reutilized and found in justifying Russian trolling “now” as well.

Such self-victimization that justifies Russian trolling was found in the American and Lithuanian media comments that this book analyzes. Self-victimization was further intensified by users hiding behind the freedom-of-speech arguments, trying to imply that they simply present a different opinion and should not be labeled as Russian trolls. Illustrations of this sentiment can be paraphrased as follows: “We are unjustly treated as Russian trolls [although we are not Russian trolls].” Yet others can be paraphrased as: “We are merely an authentic opposition,” and “Russian trolls are treated unfairly because they are denied freedom of speech,” and “Because they are denied the privileges of democracy, and are subjected to censorship instead,” and “Because they are locked into a zero-sum argument with the opposition (for example, elves in Lithuania).” While such efforts to justify Russian

trolling are already persuasive for those who already endorse Russian trolling justification, other more subtle narrative strategies have been identified in news comments.

Chapter 5, addresses the lingering question: Why would denial of Russian trolling even emerge in the American public sphere, represented in its news portal comment spaces? “Deny and Conquer: Fears of Looking Like a ‘Pussy State,’” discusses the ethos embraced by deny, deny, and deny tactic—with the ultimate goal of creating chaos by denying reality. The need for robust evidence to justify Russian trolls in US and Lithuanian news comments is discussed through the lens of a psychology of denial and by evoking the reconceptualized notion of publics by proposing its new facet, post-publics. In the era of invisible, possibly automated nonhuman actors, creating contradictory messaging leads to chaos. As a result, chaos online thus challenges the concept of publics who have to interpret deliberately confusing content. Continuous doubts regarding the ambiguity of interpretations of online messages make the social media and online public sphere as the “new mundane” are required from post-publics. The notion of post-publics furthermore goes beyond the democratic perceptions of publics with the assumptions of the underlying democratic principles, as well as counterpublics that operate in parallel to the established democratic discourse (as in e.g., Bjola & Papadakis (2020) and antipublics that operate against the established democratic values (Davis, 2020). There are two sides to the issue of Russian trolling beyond the democratic debate. A large proportion of users have acknowledged the phenomenon of Russian trolling and the consequences of chaos through the statement, “We are duped.” This hopelessness has been expressed as a state of anxiety that signaled the unpreparedness to cope with Russian trolling now and the inability to deal with it during the 2020 US presidential election. This concept of post-publics is also discussed through the lens of the current challenges of freedom of online speech.

The epilogue, “Now What?,” concludes with a reflection about the tensions that allowed for Russian troll justifications to become so prevalent online. *Creating Chaos Online* concludes with the comparison of online spaces with vessels that we fill up with content.

Propagandistic Masquerade

Breitbart Story 15, Example 1

No collusion, no impact. Just a bunch of Russians dressed up like liberal trolls hacking unsecured Democrat servers.

Dressing up with a mask conceals one's identity. And a mask can create chaos by instilling uncertainty about who does what on whose behalf, as illustrated in the example above. Online masks are constructs that are mediated by, or shaped through, technology. Thus, an internet user who opts to wear an online mask can choose how to shape it—for example, by choosing to be a troll or not, or to be a specific kind of troll. In online spaces, masks are worn by using elements that constitute one's online presence—mostly through text. A mask in online spaces can also be represented through a visual element or a GIF (Fichman & Dainas, 2019). In fact, masks can be signified by other online identity markers, and as such, they can reflect the self-determined option of identity disclosure or concealment—for example, by registering online with an actual legal name or opting for an anonymous online identity. Thus, masks are mediated by the online spaces in which they thrive or come to life. The life of a given mask is partially defined through the media infrastructures in which that mask operates. In some news portals, masks are constructed through anonymous posting, while in others, registration is required to sustain them.

Online identity is also mediated by text-based linguistic expressions—the argument strategies one uses and the sides one takes on an issue. Identity can be projected through various text-based faces, and authentic or nonauthentic narratives, such as those projected by the Internet Research Agency's

instructions that are established in a propaganda playbook. While masks enable the performance of Russian trolling, figuratively this phenomenon can be treated as a “worn” mask. Furthermore, the user narratives behind online performance scripts live their own lives. For instance, reactions surrounding Russian trolling messages mirror, amplify, and make Russian trolling come to life. While Russian trolls are operating online, they do not necessarily want to be called out, since calling them out would expose the fact that Russian trolls are lurking beneath masks. Yet at the same time, the act of calling out Russian trolls and “catching” them exposes an emblematic mask of its own. The wearing of a mask, reflected through text-based practices, exemplifies an orchestrated performativity.

This chapter delves into a construction of Russian trolling online as a form of performativity by analyzing sociotechnical contexts in which Russian trolling is taking place. This process of performativity, when captured as a still shot, illustrates disinformation that projects doubt and leads to chaos. This uncertainty is evident in representations of Russian trolls—and these representations, in turn, have been theorized and examined in several ways. This chapter is theoretically grounded in the analysis Goffman’s (1959) presentation of self. It also uses Brenda Danet’s (1998) notion of online mask as identify marker.

To situate manipulation of the propagandistic mask, the first approach to analyze automation in this book was by counting comment duplicates; the second was to assess anonymity by comparing private and public posts. Such comparison yields the conclusion that private posting is a standard means of hiding and repurposing a mask. The third method analyzes individual user activity as a proxy for one’s online masquerade: Individual users can choose to perform Russian trolling by calling themselves Russian trolls, while others can elect to call out Russian trolls. This chapter is based on news portal comments across media platforms that justify Russian trolling where users can make sense of Russian trolling and call it out. Yet such unmasking does not authenticate one’s identity. Even if the focus in this book is not on identity verification, masks online may instill uncertainty and chaos.

Text as a Mask

Prior to the emergence of the Russian trolling phenomenon, online trolls projected themselves through a set of imaginary masks. Trolls in different spaces have materialized in various guises. If one visits Seattle, Washington, and walks down Troll Street, the street eventually leads to a bridge. A colossal

statue of a lurking troll has been planted beneath it. Clearly, the statue represents a grumpy unpleasant creature that lives under the bridge in enigmatic secrecy. This grotesque caricature of a troll has been reified in online spaces through text-based means. The image has, in fact, accumulated a plethora of textual descriptors that appear vividly in online news story comments. Russian troll masks are unique, even if, as argued throughout this book, they are, by definition, invisible. These invisible masks, paradoxically, obscure the visibility of Russian trolls and invite us to ask: What types of masks are worn by Russian trolls?

The text as a mask can provide the critical lens through which self-presentation online is expressed. The mask performed through the text allows for simulation, or what scholars like Danet (1998) called textual masquerade. In contrast to masquerade that allows for further exploration of one's identity, as argued by Danet (1998), masks can also serve to perform a task of persuasion or at least dissemination of information with the goal of propagating it as a new fact.

Masks can be viewed as face management. The concept of face is used here as defined by Goffman (1967)—as an image of self-delineated, approved social attributes: “Face is a positive social value a person effectively claims for themselves by the line others assume he has taken during a particular contact” (p. 5). Goffman argued that face maintenance is a condition of interaction, not an objective. People engage in “facework,” where for example, face-saving strategies allow for neutralizing a given threat (Goffman, 1967). This chapter describes how face saving can be used to sustain Russian trolling justification over time.

This chapter showcases masks as creating an alternative reality through elements traceable through sociotechnical materiality, that is, locations, timing, and types of actors involved. These three approaches—locations, timing, and actors—and numerous instances, show how chaos is created by the emergence of the alternative realities mediated by what Starbird et al. (2019) called crisis actors. In this chapter the mechanics of the wearing of the masks are described as frames to spread and justify Russian trolling, e.g., by framing it as hoaxes (it didn't happen) or false-flag narratives (i.e., it happened but not like the media portrayed).

Paradoxes of a Mask

Why is it hard to uncover a mask? The mask entails obscuring, or covering, the face, whereby the face denotes the self and online identity. In the per-

formative process, the mask can be put on, changed, or taken off. Such gestures are enacted in online spaces through sociotechnical means—the online technological affordances, such as modalities of the text, online profile, and self-presentation—for example, by creating an online account or making posts anonymous. In either case, there is always the assumption that beyond the mask, there is a real or different or authentic self. Several paradoxes are involved when approaching Russian trolling as performative self-masking. Thus, this specific discursive phenomenon is discussed in this sequence: the paradox of invisibility, the paradox of tricks of invisibility, and the modus operandi of the propagandist mask.

Invisibility

Just as faces can be hidden behind masks, online influence can be invisible—and paradoxically, invisibility guarantees its effectiveness. The sociotechnical online infrastructure renders online trolls invisible, as they operate in the back end of the online environment they inhabit—be it through algorithms or programmed spaces. Additionally, the availability of tools, such as application programming interfaces (known as APIs), along with machine learning or, synthetic data-driven artificial intelligence, for online developers, make some online spaces more accessible for automation than others (see discussion in Zelenkauskaite & Bucy, 2016). As discussed earlier, these online spaces can be exploited to enable invisible acting, or the infiltration in online communities.

Invisible forces in the current media landscape can be unleashed not only by human users but also by automated bots that run according to algorithmic programs. As nonhuman actors, bots are invisible while operating in the background system through programming commands that run the surface content. The system is algorithmic because information can be driven by bots or algorithms that push, promote, or circulate content. Russian trolls can use to their advantage algorithmic tools that involve automated responses or frequent posting. The encoding and circulation of algorithmic information further enable Russian trolls to hide, and these can be customized to generate influence.

From the perspective of information structure, online spaces are invisible because of the inaccessible identities of actors that populate and promote them. For example, it is difficult to pinpoint who is posting and to determine whether that user is an actual person or a bot, even if tools have been developed for some platforms, such as Botometer for Twitter (Botometer,

n.d.). Moreover, bot detection is currently unavailable for users accessing online news comments. Because general public users lack both knowledge about bot technologies and the ability to recognize disinformation and their actors, hiding in online spaces is guaranteed. Furthermore, leading scholars of the digital divide might argue that such invisibility is problematic not merely as an outcome of lack of technology access but of the requisite skills and online tools for understanding how online influence takes place (Van Dijk, 2013).

To fully understand how information systems work, general readers in online spaces need to move beyond individual posting levels to access contexts in which messages are posted. Such contexts involve access to a bird's-eye view of big data of all posting flows to observe the circulation of information to start making sense of the patterns of influence, besides uncovering techniques that enable their proliferation which we currently lack. Technologically speaking, online users typically do not have access to or the capability of viewing patterns of information circulation, as critical accounts of remediation and big data uphold (Zelenkauskaite, 2017). However, it is worth mentioning that news portals have implemented user's activity access, especially if they register.

Similar arguments hold for fighting disinformation where an understanding of digital tools used becomes instrumental. While these lists of tools are compiled publicly (e.g., Rand's tool list is thorough and comprehensive) for bot and spam detection, credibility scoring, disinformation tracking, education and training, verification, whitelisting, and establishing codes and standards ("Rand," n.d.), their use in everyday life is still limited given that these lists appear post hoc and are not implemented as preemptive measures.

Given that users in online spaces typically cannot focus on how systems process the information surrounding them, invisibility becomes a key element that facilitates Russian trolling. Such invisibility can be enabled by the masks that mediated environments create. Thus, technological affordances of system-based seamlessness can be exploited to hide the influence of Russian trolling. Yet it remains crucial to uncover the mechanisms through which influence can take place and to enable users to recognize them.

Masks at Play

Trolling as a masquerade has been contextualized by Bakardjieva's (2008) analysis of the news comments within a larger national popular culture by describing online news comments as carnivalesque. As carnivalesque dis-

course, comments can be grotesque, humorous, or loud. Thus, Bakardjieva (2008) has emphasized the loose and informal aspects of online commenting. How can masks be interpreted through text? And how can masks instill chaos? How do these informal practices are translatable into contexts where not all actors involved are genuine?

Since the carnivalesque nature of online comments allows discursive participants to wear masks, such masks depend on the wearer's targeted audience. Moreover, given that any user can participate with any type of mask, and with any form of commenting, carnivalesque masks can also include ideological influence and disinformation. In such instances, trolling is rendered visible by approaching discourse as a mask—especially when Russian trolling is defended or called out. These discursive practices expose Russian trolling's subverted masks. The purpose here is to outline how subversion through online news comments takes place and which tactics are used to persuade. Specific masks that are examined here show how Russian trolling appears in comment spaces.

Propagandistic trolls are characterized by the intention to subvert authentic participation in the Habermasian public sphere, where everyone is invited to discuss news story issues. This subversion can take place in several ways. To be effective, ideological or propagandistic trolls need to blend into a conversation that is already taking place by presenting topics that would be approved by the group they join. Rather than employing a classical trolling strategy of aimlessly opposing ideas that have already been presented by group members, such trolls infiltrate conversations by amplifying, introducing new interpretations, or contesting a given issue at a specific moment (see, e.g., Herring et al., 2002). Such discursive tactics allow for a propagandistic mask to be perceived as one of the voices that constitutes online public debate. Thus, because online incivility attracts user scrutiny, the Russian troll, who intends to engage in disinformation, tries to hide in the crowd of other users to become one of the alternative or amplifying voices.

In short, such Russian trolls, to be effective, deliberately aim for online invisibility through discursive assimilation. Such deliberate efforts are sustained through the creation of masks and their continuous use. The true (authentic self) is hidden behind a customized mask, as is the case, for example, with Internet Research Agency's employees who pretend to be someone else when posting online, as further detailed in Chapter 4. The mask is based on a predefined ideological framework that is created for a specific case of influence. And the invisibility of trolls can be directly linked to the presence of a mask. Rather than the usual physical mask that may come to mind, the mask, in these online instances, is a nebulous abstraction that is based on

text, video, and internet links—and most importantly, an abstraction that projects a specific ideology used to craft messages for disinformation.

Within the parameters of this discussion, Russian troll masks need to be distinguished from the masks that other kinds of internet trolls wear in the online social sphere. Typically, online masks have been associated with internet trolls to explain uncivil behaviors. However, the behavior of an internet troll as disruptor is geared toward visibility because the objective is to monopolize attention or to stand out from the user crowd. Thus, internet trolls are represented as users who wear masks or who crave attention. While they may be masked by their social media name or handle, they still want their online comments to attract notice.

Although their masks assume numerous forms, they are invariably represented as grotesque. Yet Russian trolls can be distinguished from other internet trolls because they take advantage of user crowds to conceal themselves while advancing disinformation agendas. Furthermore, because Russian trolls endorse such agendas, they prefer denial and obfuscation to adopting a series of standardized troll masks to engage in uncivil behaviors in online spaces. For instance, they will deny the existence of Russian trolling in order to defend its operations while obscuring its effects. Thus, numerous questions arise: What types of masks can hide online identities or be replaced? How are masks worn? Who is behind the masks? How can Russian troll voices be amplified? And, why are masks convenient for engaging in information warfare? However, rather than confirm the presence of Russian trolls behind masks, the goal is to authenticate their discursive practices and their effects—in other words, to explain how troll masks can be created if they do not originate in authentic user behaviors.

Location as a Mask

Is a troll a mask, or is a troll the one who wears the mask? Or, when anyone can wear a mask, who is behind the troll mask? These questions permeate the problematic issue of Russian trolling in the current media landscape. Geographical location online can become a mask since it is marked through multiple sociotechnical affordances online—automatic ones (e.g., Internet Protocol (or IP) address where the content is produced); user-created such as geotagging where users can tag their own location or the location of the post, or providing location in the text. Location has been prolifically analyzed to draw insights on war and conflict to map physical spaces and online spaces (see e.g., Siapera et al., 2015).

Analyzing tweets associated with Internet Research Agency–based accounts confirms, so far, that users adopt a mask to present themselves as authentic (Xia et al., 2019). Therefore, the question is not about the existence of Russian trolling as self-masking performance. Rather, we might ask *how* that masquerade is performed. In her book on cyberwar, Jamieson (2018) observed that Russian trolls wore masks by harnessing the power of impersonation: “Because the geographic location of the communicator is not evident to those viewing posts and tweets, in a single sitting, a troll in St. Petersburg could masquerade as a housewife in Harrisburg, Pennsylvania; a black nationalist in Atlanta, Georgia; and a disaffected Democrat in Ripon, Wisconsin. Accordingly, @TEN_GOP was not in Tennessee, as its inhabitants alleged, but continents away. Likewise, there were no longhorns named Bevo or Boris anywhere near the Heart of Texas account’s authors” (p. 12).

This excerpt specifies how trolls can masquerade by impersonating various prototypes embedded in the American public consciousness. The key to understanding such impersonations is the intentionality of the acting—its specific goal to influence or at the very least “muddy the waters” or create chaos. Jamieson’s (2018) examples reveal location-based, deceptive self-representations, or masks designed to generate a perception of authentic participation in various online spaces, such as social media, and hypertext.

Manipulating one’s IP address is a practice that has been attributed to generating fraudulent accounts online, which constituted around 3% of Twitter and 1.5% of Facebook accounts (Thomas et al., 2013). However, in news portal contexts, IP-based, location-based evidence of foreign activity in Lithuania’s online spaces has also been exposed.

User IP address concealment is treated in IP analysis as the blueprint mask in online spaces. Typically, IP is automatically assigned to a message (or any content) on the basis of a device’s parameters, through which the message is transmitted. To mask these parameters, IP requires intentional alteration. Analysis of news portal content in the Russian-language version of Delfi.lt in previous research has shown how IP concealment is prevalent online (Zelenkauskaitė & Balduccini, 2017). To trace such intentionality about altering locations, Zelenkauskaitė and Balduccini (2017) analyzed 1,304 stories published between 2015 February 15 and 2015 March 15 on the Delfi.lt news portal, together with all related comments. This sample consisted of 4,940 users who contributed portal with 34,038 comments, with 6.9 comments per user on average. The sample contained 14 content categories, as defined by the news portal. Geolocation analysis of the data showed the following distribution of the countries from which comments have originated: the highest percentage of comments was traced back to

Lithuania (53.3%), followed by Russia (16.8%), then by cases whereby locations could not be identified (7.9%). These statistics further confirm the “mask” enacted through IP concealment.

It was also discovered that a location’s specificity was yet another indicator of Russian trolling. When scholars analyzed Twitter accounts associated with the IRA’s activities, they identified certain markers that revealed differences between typical Twitter users and IRA-orchestrated tweets (Zannettou et al., 2019). One difference identified was that IRA users included generic locations in their self-descriptions, while other types of users included specific ones (Zannettou et al., 2019). Other attributes of atypical posting in the news portals were found to involve users who post quickly—that is, by simulating the automated behaviors known as bot-based behaviors in social media (Zelenkauskaite & Balduccini, 2017). Indeed, there is a noticeable proportion of users who post very quickly when a news story is released and in response to multiple stories about similar topics synchronously. These behavioral traits indicate an orchestrated effort behind the accounts. Thus, accounts can function as masks.

Subversiveness of a Mask

A specific type of Russian trolling mask relates to propagandistic manipulation, according to which ill intentions must be successfully concealed, or rendered invisible to message recipients. At the heart of propagandistic manipulation is the continuous reality-testing (Lasswell, 1950). Choukas (1965) wrote: “It is the chief characteristic of propaganda to be elusive; characteristically, propagandists are secretive in their work, avoid the limelight as much as possible and seek the shelter of the shadow” (p. 10). However, both the propagandist and the Russian troll aim at influencing internet users through the messages that they promote, as Choukas (1965) has stated: “The function of propaganda agency is not to inform but to persuade” (p. 11). In other words, there is intentionality behind the persuasion process. Or, the persuader intends to craft messages that are “deliberately designed to influence opinions or actions of other individuals or groups with reference to predetermined ends” (Choukas, 1965, p. 13). Other definitions of propaganda as influence that were prevalent during World War II state that “the control of opinion” was exercised through “significant symbols, or, to speak more concretely and less accurately, by stories, rumors, reports, pictures and other forms of social communication” (Choukas, 1965, p. 14).

Yet another type of Russian trolling mask involves self-positioning as a

disruptive actor who engages in a communicative process based on a counteraction. This counteraction in online commenting is observable when expectations for communicative norms are not fulfilled. Typically, people engage in communicative strategies to achieve a successful communication exchange. One of these strategies is impression management.

When describing impression management, Goffman (1959) emphasized the need to prevent of what he called the occurrence of incidents. The occurrence of incidents violates impression management in a communicative exchange by something that does not conform to a given expectation. Occurrence of incidents, when handling incidents, to diminish the “damage” can outsource to face-saving strategies. Face saving indicates the need for redress in situations that are potentially uncomfortable—for example, when they occur unexpectedly, as with incidents. In such scenarios, the ideal interaction is one where interlocutors typically collaborate to foster a civil dialogue. Face-saving strategies minimize the possibilities for conflict or confrontation. Thus, it can be argued that in democratic contexts, confrontation is expected, as each party presents and defends ideas in ways that are both civil and face saving.

Goffman (1959) further postulated that both participants and nonparticipants are included in interactions for the purpose of avoiding embarrassing incidents that originate in miscommunication. To avoid such incidents, three sets of strategies are employed: “a) the defensive measures that performers use to save their own shows; b) the protective measures that an audience, or other non-performers, use to assist performers to save their show; and c) the measures the performers must take to enable the audience, and other non-performers, to employ protective measures on the performers’ behalf” (Goffman, 1959, p. 212). These behavioral strategies are applicable to Russian trolling in online news comments. The presence of these strategies indicates the artificiality involved in the creation of Russian trolling masks. After all, masks represent constructed personas, or what Goffman (1959) described as dramaturgical characters that serve to disseminate disinformation.

Sabotage: Calling Out Russian Trolls

Russian troll call out sabotage examples can be considered as a form of defensive measure where face saving is subverted by the audiences who do not comply with script promoted by Russian trolling. Goffman (1959) identified performative face saving as a defensive measure enabling performers to

save their own show. Defensive attributes and practices include dramaturgic loyalty (teammates must act as if they have accepted certain moral obligations), dramaturgic discipline (teammates must be on top of the performativity), and dramaturgic circumspection (constant awareness of performance).

Since these codified attributes can also apply to Russian trolling, the performance of Russian trolls can be sabotaged when an audience calls them out, as evidenced by multiple forms of such sabotage exemplified in the subsequent section. In other words, the sabotage can result from a violation of this tacit code. Violation occurs when expectations of audience cooperation remain unfulfilled. More specifically, an audience sabotages a Russian troll's masquerade by acting in ways that are contrary to typical audience behavior expectations in specific online spaces. According to the ideal scenarios for Russian trolls' success, such behavioral expectations include unconditional acceptance of Russian troll participation in online discussions. Such user acceptance can be demonstrated by playing along with trolls or cooperating with them by allowing them to propagate information.

Masks also represent tactics of self-presentation that are verified by audiences, who are presented with two choices: to accept masks at their face value by treating Russian trolls as legitimate participants of a given media ecosystem, or to call them out by sabotaging their performance and exposing them. An exposé of Russian trolling illustrates performance sabotage. Sabotage can counteract disinformation through user activities that do not conform to standardized communicative rituals—thus, breaking with the preestablished norms for avoiding embarrassing incidents. Consequently, disinformation can be nullified through the knowledge that a propagandistic act is taking place. It is when the act's occurrence has become a known fact that one can choose to expose or ignore it.

Comments calling out Russian trolls found in analyzed platforms' comments functioned as exposés. Many of these exposé frames allude to Russian trolls being paid by the government to comment online. Russian trolls, in these instances, were treated as mercenaries, paid by the Russian government—specifically, the Internet Research Agency, as exemplified below.

Breitbart Story 15, Example 2

I believe you are one of the Russian Internet Research trolls not yet pick-up. Nemesis will catch up with you soon. Take cover Dodger-even if there are 300 of you!

In some cases, Russian trolls were called out on the basis of linguistic features that provoked the suspicion that they were nonnative speakers of English:

Breitbart Story 15, Example 3

Hey Vlad, do yourself a favor and tell your handler you need some more English lessons before you can do a decent job of trolling. And lay off that WODKA!

Some exposé frames used a sarcastic tone:

Breitbart Story 15, Example 4

Give your handlers their money back, you're not good enough to troll.

Yet others called out Russian trolls by demanding their permanent departure from the *Breitbart* comments section.

Breitbart Story 15, Example 5

For any trolls checking in here, it's time to pull up your big boy pants and find a new hobby.

Others called them out through specific reference to typical Russian troll attributes, such as being paid and their intent to influence.

Breitbart Story 15, Example 6

[S]aid the troll being paid to influence the public narrative.

Similarly, another user posted:

Breitbart Story 6, Example 1

It is pretty clear the Russians trained you well. You ignore patriots who are trying to wake you up and you believe trolls and bots who tell you what you want to hear. And trump reinforces it. That is the problem. YOU ARE PART OF THAT PROBLEM.

Some comments included a variation of the line “I am not a Russian troll, like you are,” by generating opposition or through distancing.

Breitbart Story 4, Example 1

Little bit. but I am not fluent in Russian like you.!!!

Another user insinuated that Russian trolls are trained by an “apparatus.”

Breitbart Story 4, Example 2

I am not trained by the Russian troll apparatus.

Similarly, claims that Russian trolls not only exist but indeed exist here to sow discord are expressed by this user:

Breitbart Story 4, Example 3

Like, no duh! 90% of the trolls here alone are just here to sow discord -- Russian style.

Others called out the opposition by stating that there are also “Soros trolls.”

Breitbart Story 7, Example 1

Kinda ironic considering you can't spell “you're”. But keep trying Soros-troll!

Some referred specifically to foreign interference.

Breitbart Story 12, Example 1

Comment: Don't bet against Donald Trump.

Response: Why do you foreign troll care?

In this exchange, the second comment calls out the user who posted pro-Trump post referring to them as “foreign troll.” Similarly, other users pointed out that in *Breitbart* there are Russian trolls and bots who act like regular citizens:

Breitbart Story 15, Example 7

Russian trolls and bots prefer *Breitbart*.

Similarly, another user perceives that in *Breitbart* comments there are a lot of posts by Russian trolls:

Breitbart Story 15, Example 8

Jesus, seems like there is a lot of russian trolls here now. By the way, how is the weather in St. Petersburg?

Some users stated that Russian trolls exist and were “here” on *Breitbart*.

Breitbart Story 15, Example 9

Yep, *Breitbart* is indeed a Russian asset. I come here to keep up on the latest Russian troll talking points. I am deadly serious about this. You have undoubtedly noticed how so many of them keep repeating the same tired stuff over and over. Variations on a theme—but it always comes down to Hillary, Obama, Soros and the DNC—even when Trump is crashing and burning.

The statement “Russian trolls are here” is repeated in the following comment.

Breitbart Story 15, Example 10

The Russian trolls are busy today trying to discredit the indictment. They get the ignorant and stupid so lathered up all they can say is STFU or call someone a commie.

Similarly, some users refer to Russian trolls by calling them “comrades” and referring to “rubles” in reference to Russian trolls being paid by their government:

Breitbart Story 15, Example 11

Only somebody with a name and avatar like yours could be a troll. Sorry comrade, hope you earn a few rubles posting on here. Tough life

In the *New York Times* sample, a user flagged a comment as a Russian troll post based on its content.

New York Times Story 4, Example 1



CaliforniaNov. 7

@trump basher-Me thinks this reads a lot like a Russian troll post. Sigh.;->

Some users were hesitant to publicize Russian troll exposés. Others argued that certain posts “might have been written” by Russian trolls, as the following comment exemplifies.

New York Times Story 5, Example 1

██████████

Faywood, NM September 20, 2018

Your comment reminds me that Russian trolls frequently post in NYT opinion section.

One user sarcastically called out another user’s posts as those authored by Russian trolls.

New York Times Story 6, Example 1

██████████

Bozeman Montana Nov. 15

How’s the winter in Russia this year? Pretty nice here in the US

Some users offered media literacy lessons on how trolling works.

Breitbart Story 8, Example 1

So many people don’t realize the Russians troll both sides. I doubt they even cared who won. The whole point is to divide and sow discord and ultimately diminish the American people’s faith in our own nation. Everyone who joins in with the us vs. them mentality is being played. Our own politicians do it too.

Yet others explicitly praised the *New York Times* for exposing Russian trolling. For example, the following post received 185 “Recommend” hits.

New York Times, Story 5, Example 2

██████████

London September 20, 2018

This is indeed a remarkable article, detailed and containing very specific information I did not realise was actually out in the public domain. Cudos for the research. However, only in the last part does it address the shift in Republicans favourable views of Russia. Has there been any research into how or how much the russians have succeeded in influencing republican

representatives in congress and the senate? It also does not address the NRA in any depth. Are these stories for a future date, I hope?

Some users provide not only media literacy frameworks, but also, broader explanations for why Russia and conservatives are compelling.

New York Times Story 5, Example 3



Burley Idaho September 20, 2018

In the eyes of Americans conservatives, and this includes Evangelical Christians, Putin's Russia is seen as the last bastion of white Christian power. Putin has been cultivating this base for some time. Anti-gay laws, and promotion of the Russian Orthodox Church by Putin's government, has endeared him to American religious conservatives. Franklin Graham has had nothing but effusive praise for Putin. And he is not alone. I would suggest that you read Malcolm Nance's *the Plot to Destroy Democracy*, or David Korn's book *Russian Roulette*. Additionally, this information is not new, as Chris Hedges exposed the Christian right's fascist leanings and their hero worship of Putin in his book of *American Fascists* published in 2007. I don't know whether we're seeing the culmination of these efforts, but I certainly hope that enough of this information has been exposed to cause us to take a long skeptical look at American conservatives and where their movement come to.

Some users called out Russian trolling by commenting on the behavioral traits and language of Russian trolls.

New York Times Story 3, Example 1



New Hampshire March 9, 2018

Why would someone take the time to read NYT, then take more time to write a comment calling out NYT as "the corporate media" and "creating fake news to promote it's own agenda?" If you dislike the corporate media and consider NYT as part of the corporate media, and say they create self serving fake news, then why on earth would you read something you dislike so much? This seems suspicious. Trolls come to mind. He goes on to state, "There is a good principle of American Law and of Law in most countries; that principle is innocent until proven guilty." That statement is interesting because the commenter identifies himself as coming from Ankara, the capital

of Turkey. Interesting because Turkey doesn't buy into that principle. Over 110,000 have been locked up after the coup attempt with only about 41,000 charged. That leaves over 60,000 detained without charges. So much for innocent until proven guilty.

These examples illustrate how Russian trolls embedded in news portal comment spaces have been caught and called out wearing propagandistic masks. Yet even if exposés occur in online spaces, they do not necessarily sabotage the performances of Russian trolls. Instead, such exposés illustrate that, due to the prevalence of Russian trolls in a given online forum, information posted there is generally unreliable. Such projections of impending online chaos can suppress democratic debate by inciting users to leave spaces permanently, to request websites shut down user commenting due to challenges of comment moderation, or to merely ridicule the seriousness of Russian trolling.

It is possible to interpret such sabotage through the lens of Goffman's theory of performativity. According to Goffman (1959), however, the disloyalty of online community, exemplified here through callouts of Russian trolls, threatens potential backfire. In short, callouts can strengthen the opposition's in-group solidarity. Even if some audience members were to expose Russian trolls, those who endorse other perspectives (e.g., the conviction that Russian trolling is unproblematic) could form an opposing coalition. The opponents could then amplify the disinformation originating from Russian trolls and realize what Goffman called the "dramaturgical discipline" ideal. From the perspective of teammates, dramaturgical discipline involves the cooperation that enables them to follow along with the scripted performance. Thus, as a concept, dramaturgical discipline permits Russian trolls to play the role of trolls consistently. Sustaining such role-playing over time is possible because they can always attract complicit supporters, despite the presence of online community members who expose them and thus sabotage their masquerades.

Yet for Russian trolls to be successful, they need to find the right topics to attract followers. Thus, dramaturgical circumspection is required—a quality defined as a constant (self-)awareness or prudence in communicative acts. Goffman (1959) stated that "the prudence is needed while staging the event, exploiting contingencies that are presented with them and opportunities that remain" (p. 218). He also specified requirements for the successful enactment of prudence, such as selection of loyal and disciplined team members and awareness of how much loyalty can be expected from the team. In other words, Russian trolling needs support from loyal follow-

ers, or collaborators, who succumb to the lure of disinformation messaging and treat it as an authentic discursive form. These loyal followers can also be mere believers of disinformation messaging overall, if parts of the messaging appeal to their values. Consequently, they become enablers of Russian trolling success. As Jamieson (2018) observed, such followers can also be paid operatives who create a critical mass, or the general public who enables the proliferation of ideas held by Russian trolls.

To target enablers, there is another tactic that can be utilized for the performative masking of Russian trolling that involves what Goffman (1959) called the *circumspect performer*. More specifically, this tactic requires “selecting the kinds of audiences that will give a minimum of trouble in terms of the show the performer wants to put on” (Goffman, 1959, p. 219). Thus, theoretically speaking, before casting a wide messaging net, Russian trolls should test out online spaces where contestation of ideas is minimal. Then, they can deploy tactics for persuading audiences to take sides on issues that have already been endorsed for online debate. Such tactics expose potential alternatives that appeal to that specific segment of the audience. In other words, by providing various justifications for Russian trolling, the ones that become amplified or the ones that audiences find most appealing become increasingly evident. After such testing, messages can be seeded through repetition across multiple platforms.

Another technique that supports the *circumspect performer* is ensuring that information remains closely related to the facts and that these facts remain minimal for the production of simple and succinct scripts. In other words, the shorter and simpler the script, the less risky (as in the case of alibis) and the more likely the performance is prone to withstand sabotage. While this technique allows for less error, Goffman (1959) cautioned that it could decrease audience interest and engagement. Thus, short and simple, persistently repeated messages have the greatest likelihood of success as tactics of persuasion and influence. For Russian trolling specifically, such messages need to address topics that appeal to public affect and should be duplicated.

Another aspect of visibility that performers must consider is the amount of information sources available to the audience during the interaction process. This concern is important because it allows the performers (i.e., masked Russian trolls) to adapt to situations depending on the audience type they face—examples are shown in the subsequent chapters referring to cracks in the society pertinent to each sociocultural context. In other words, different news portals will draw specific audiences—whether that portal is *Breitbart*, the *New York Times*, Gab, or Delfi.lt. Thus, issues need to be customized for each of these audiences.

News portals that waive user registration requirements for posting comments also enable successful online masquerades. In such cases, invisibility can be more readily negotiated by performers, whereas automation further facilitates such masquerades. More specifically, the creation of myriad bots that act autonomously and promote certain messages becomes possible. If the human team behind the bots has an orchestrated agenda, it can render Russian trolling effective due to its ability to dispatch messages on a global scale.

Protective Measures

Protective measures can also be variations of the Russian trolling mask. While such measures have been described as modes of impression management, they are usually implemented according to voluntary discretion—that is, of interlocutors who ask individuals to refrain from entering spaces to which they have not been invited. Once they are invited to a performance, they still need to maintain what Goffman (1959) called tactful inattention.

Where Russian trolls and news portals are concerned, the uninvited aspect of online audiences is rendered irrelevant by the general assumption that democratic deliberation invites all users to participate and that such discursive participants self-select. Consequently, performances in online spaces can be deliberately sabotaged by any actor. While some participants are more active than others, the nature of participation varies, depending on news story categories and participant (inter)activity levels, for which an indicator is the number of messages posted.

Performativity and Modus Operandi of a Propagandist Mask: Self-Sabotage

As previously mentioned, Russian trolling as online masquerade can be examined through the critical lens of performativity. If influence is considered crucial for the perception of Russian trolling, the performativity of anonymous and automated Russian trolls in online spaces must also be considered. Yet questions linger: How do online masks shift, and how are they adopted for discursive performance? How can the masked self be presented according to Goffman's performance theory? After all, Russian trolls must present themselves within consistent frames that maintain the front through text, since message posting takes place online.

An example of performativity can be observed in examples where, users sarcastically called themselves Russian trolls to downplay the seriousness of Russian trolling. In such cases, self-sabotage was found to be another unmasking strategy, even if it is geared to obscure rather than uncover. An example of this strategy is confessing that one is a Russian troll (regardless of whether such confession is true). Self-sabotage geared to cause confusion regarding Russian trolling was expressed through some variation of the statement “I am a Russian troll.” This statement can exemplify deployment of the covert propaganda because such commenters establish their affiliation with the so-called opposition, or Russian trolls. At times, their comments exceed mere sarcasm, which indicates that they had adopted the “I am a Russian troll” narrative to demonstrate solidarity with Russian trolls in some instances. The manner in which this statement emerged showcases the push for the viral memetic circulation of the statement in a presumably ironic tone. The following statements exemplify such rhetorical maneuvers.

Breitbart Story 9, Example 1

That’s it, I am changing my screen name to “Russian Troll.”

Users resorted to sarcastic “I am a Russian troll” remarks when mocking the Russian trolling investigation.

Breitbart Story 15, Example 12

Seems like there are more Russian trolls here.

I am a russian bot. not troll  

The “I am a Russian troll” comment was used as a technique to discredit the face value of the investigation. In this case, users presented themselves as trolls.

Gab Example 1

#intelligence Report talks of #Russian paid #trolls on social media before the election to discredit #HRC & her campaign.

1. **Where is my paycheck for hours of trolling?**
2. **HRC/Podesta did a much better job of discrediting themselves than any troll could!**
3. **I am a proud troll!**

[image of seven trolls with colored hair]

This example illustrates how the user projects themselves as Russian troll, arguing that they are “proud trolls” and they deserve to be paid for their work and that Russian trolling is just a mere subcultural activity of which they are proud, thereby still downplaying Russian trolling.

On Delfi.lt, some users sarcastically called themselves Russian trolls. In so doing, they mocked the phenomenon of Russian trolling.

Delfi.lt Example by Anonymous Users 1

Headline: I am putin

Comment: I have been and I will be a troll. They will put me in the jail, I will troll from the jail, no problem :D

In this example, the user, who chose to be called “Putin,” insinuates that it is impossible to put an end to trolling.

“I am a Russian troll” evokes similarities with the #IAM movement whose hashtag was translated from the French *Je suis Charlie*. In her *Slate* article, Hess (2015) describes #IAM as the default mode of showing solidarity in the hashtag era. The movement originated in 2015, when gunmen targeted and killed staff members at the headquarters in Paris of the weekly satirical newspaper *Charlie Hebdo*. Since then, the movement’s hashtag was translated into multiple languages and began to include the names of the victims. For example, according to Hess (2015), the hashtag fractured into countless iterations, such as #JeSuisAhmed, in support of the Muslim police officer Ahmed Merabet. Then, it was used to show support in general when it was translated into multiple languages: #JeSuis, #IchBin, #IAM. As Hess (2015) observed, “This is now the standard opener for expressions of social media support” (para. 2).

In news portals, however, hashtags are not the typical sociotechnical means of content tagging or signaling. Thus, they do not exist within those contexts. Nevertheless, the “I am a Russian troll” line has been repeated across multiple news portals and contexts. Yet while the #JeSuis movement acquired momentum through both traditional and social media platforms, analyzed examples from news portals show how users have adopted it to emphasize their solidarity with allegedly falsely accused Russian trolls. Because “I am a Russian troll” insinuates that Russian trolls are victims, the statement is readable as a rallying call for support and solidarity. It also shows how frames that are popular in other contexts have been appropriated and reutilized to create new masks. Thus, the *Je suis Charlie* movement allows for the “I am a Russian troll” cross-referentiality, which, in turn,

invites sympathy toward Russian trolls. Later in the book, in Chapter 4, similarly, through Russophobia frame, Russian trolls were found to position themselves as alleged victims to evoke sympathy.

Modus Operandi I: The Troll Mask as Camouflage and Alter Ego

Constantly changing message flows in online spaces permits users to camouflage themselves within message clusters while enabling them to assume various roles. Russian trolls, in particular, if employing classical propaganda techniques, can assume at least two forms: the overt propaganda and covert propaganda. Choukas (1965) traced these propaganda techniques to World War II. Overt propaganda involves the propagandist's infiltration of an audience to simulate agreement with the majority of members. The goal is infiltration, followed by further polarization. By contrast, covert propaganda techniques require the propagandist to side with the opposition.

Such treatment of propagandistic masks is useful where Russian trolls can join movements and present themselves as members of a generally informed citizenry or as merely opinionated online forum participants. Consequently, group membership enables Russian trolls to operate as masked users who infiltrate spaces to sway opinions. Russian troll infiltration case was recently identified in the conflict among groups within the Black Lives Matter movement (CNN video, Russian trolls exploit, 2018; Stewart et al., 2018; Zannettou et al., 2019). In such cases, infiltrating trolls can feign participation in social movements through the tactics of overt or covert propaganda. Assimilation into the general online population further enables them to deploy these propaganda tactics. For example, they can assimilate by impersonating activists and by pretending to endorse their values. Infiltrating trolls can also impersonate members of oppositional teams. Thus, by assuming both activist and oppositional team member roles, disinformation is enabled through the consolidation of control over messaging, as in examples of "I am a Russian troll."

Furthermore, when referring to propaganda as a mask, Choukas (1965) stated that the mask represents the covert position of propagandists. He also claimed that unlike overt propaganda scenarios, whereby opponents are openly exposed or attacked, the covert propagandist assumes the role of the friend of an opponent, or—better yet—that type of propagandist assumes the roles of opponents. Thus, covert propaganda is understood to be fully orchestrated with complete objectivity, while no personal elements are included in its agenda. Moreover, covert propaganda involves using lies

to create objective facts. Yet when such facts became verifiable, such “covert” propagandistic messages become evident lies. Then, the propagandist is compelled to change strategies. But before that need arises, the propagandist can freely circulate pushed agendas as objective truths, due to debate distortion or sabotage in the online public sphere.

Modus Operandi 2: “Fake It Till You Make It”

Through the symbology of masks, online trolling can be viewed as a staged performance, especially if it is orchestrated by external forces of influence. Yet its performative element implies that to be perceived as “real,” one must engage in a persistent performance. This persistent performance can be encapsulated in the dictum “fake it till you make it.” Goffman (1959) described the sustained performance accordingly: “Performers may even attempt to give the impression that their present poise and proficiency are something they have always had and that they have never had to fumble their way through a learning period” (p. 47).

While Goffman noted that performers are better off if they enter a performance site without doubts, faking can be a useful technique for persuading an audience that the performance they are about to witness is actually authentic. Goffman, then, specified examples of high-executive jobs and how applicants for them are hired on the basis of the qualities that they appear to embody rather than the skills that they actually possess. In the case of executive positions, job applicants land them because of these “quasi-inherent” or performed (in advance) qualities.

So, how does all this apply to Russian trolling? First, Russian trolling in the comments has been positioned through specific frames. These frames are conveniently packaged for the reader as lenses through which Russian trolling should be interpreted. For example, Russian trolls exist and Russian trolls do not exist are two major oppositional frames through which Russian trolling was treated online. Russian trolling, thus, requires a great deal of effort with “fake it till you make it.” The need of sustained positioning of a given idea suggests that there is no agreement on a given topic, such as Russian trolling existence.

Sustained performances in professional settings were found to involve degrees of signaling. Goffman (1959) observed that “fake it till you make it” in service occupations is accompanied by tangible signs such as the appearance of “cleanliness, competence, [and] integrity” (p. 26). Such signs, he argued, are related to the self-presentation. Thus, in online performance

contexts, Russian trolls have to take stances by crafting targeted messages toward the groups and online spaces they intend to influence.

Additionally, the “fake it” aspect of trolling requires the adaptive selection of a presentation for maximizing approval of an issue related to disinformation. Such issues typically refer to sensitive topics that are relevant to a given group or are customized according to context. Then, to sustain that performance of authenticity, frames need to be repeated till audiences validate or accept them. Thus, performers encounter risks when adopting “fake it till you make it” strategies. However, performers can underperform or overperform when using given masks. Thus, a successful Russian troll needs to calibrate performance capacities. According to Goffman (1959), one calibration method involves setting the scenic parts of the expressive equipment. Thus, for disinformation to be effective, masks require constant adjustment as new topics emerge.

Goffman (1959) also claimed that there were preestablished fronts, or modes of self-presentation, that require particular performance acts for various roles. Users can fake authenticity by repeatedly employing such predesigned frames, or aforementioned fronts. Thus, specific positioning of Russian trolls through repeated frames can relate to fronts or the sustained presentation over time of a given idea as an authentic façade pertaining to a given matter. While typically sustained performance requires extensive effort, the current media landscape allows for automation. When the concept of preestablished fronts is applied to Russian trolling, a range of activities of self-presentation on the web can be automated.

Automation can be achieved through programming. Typically programming online is associated with bots. Gorwa and Guilbeault (2020) categorized bots based on structure (systems that are algorithmically or human-based), function (what bot’s task in the specific online space: e.g., to emulate accounts or communicate with others), and uses (how bots are employed). Based on programmed parameters, bots (short for “robots”) were originally designed to automate tediously repetitive online tasks. In such instances bots were launched in the early days of the web to perform tasks such as the systematic cleanup of Wikipedia entries to ensure their conformity to formatting requirements (Geiger, 2017). Bots are not unique in this way: Bots can exploit advantages that online environments provide for communication, described by Van Dijck and Poell (2013), such as programmability, popularity, connectivity, and datafication in social media.

While it is true that not all bots are malicious, Twitter, for example, outlined what constitutes prohibited activity by citing the following: “Malicious use of automation to undermine and disrupt the public conversation, like

trying to get something to trend; Artificial amplification of conversations on Twitter, including through creating multiple or overlapping accounts; Generating, soliciting, or purchasing fake engagements; Engaging in bulk or aggressive tweeting, engaging, or following; Using hashtags in a spammy way, including using unrelated hashtags in a tweet (a.k.a. ‘hashtag cramming’)” (Roth, 2020, para. 9).

Automated actors such as bots in current online media systems can be programmed to accomplish lists of tasks: search users by keyword, account, or ID; follow and classify users based on predefined parameters such as user types, trends, and keywords; “like” content, based on predefined parameters, such as user types, trends, and keywords; tweet and mention users and keywords based on AI-generated content, fixed-template content, or cloned content from other users; retweet users and trending content, and mass tweet based on specific parameters; chat to (reply) or with other users; use pauses to mimic API or human expectations; and store information for later use (Daniel & Millimaggi, 2020).

These automated tasks enable Russian trolls that are programmed through bots, as argued by Im et al. (2020) to express themselves with simulated authenticity. Specific type of bots, sockpuppet bots, are known to be designed with the goal to fake identities; and are deployed to interact with other users online. These bot accounts are controlled manually; however, automatic control has been also detected (Gorwa & Guilbeault, 2020). To sustain a sense of authenticity, the bot programmer simply needs to scan constantly posted user-generated content and, in so doing, extract relevant aspects—be it from social media posts or news portal comments. Based on these extractions, the programmer can simulate “authentic” content for dispatch. Through machine-learning techniques, typically used for artificial intelligence applications and deep-learning, these texts can assume any types of masks. Such prepackaged messages are just as easy to dispatch online by automated means. In such instances, “fronts” can function as online platform properties. These fronts can represent, while also enable, different behavior types. At the same time, the signaling system of messaging can be simulated through location identifiers or the kind of self-representation that involves impersonating someone else.

However, through the concept of automation, bots can also contribute toward the rhetorical contouring of propaganda. In the specific context of Russian trolling, the discussion concerns bots that are designed to deliver specific messages. According to Ferrara et al. (2016), these are “social bots” that “automatically produce content, and interact with humans on social media” (p. 96). Thus, these bots simulate human online behaviors. Specify-

ing bot typologies—for example, for advancing political agendas—becomes crucial for exposing and disambiguating the misconceptions about online information and communication ecosystems, where various actors coexist, as shown by Golovchenko et al. (2018). Such political bots were found to drive discussion about the shooting down of Malaysian Airlines Flight 17 in the Ukrainian war zone in 2014, even if it looked like a general public of “curators” or “involved” citizens, who tweeted about the incident (Golovchenko et al., 2018). However, a closer analysis of this tweet sample performed to detect bots revealed that a large number tweets were posted by bots acting on behalf of “citizens” and adopting impostor masks with a goal of a targeted circulation of centralized disinformation about the airplane shooting (Stukal et al., 2019).

Thus, the purported human users in this case had actually been masked automated bots that simulated active human engagement in information propagation, exemplifying the difficulty of unmasking online behaviors. Thus, automation through nonhuman means can be implemented through the use of automated bots, as an available option in the current media landscape.

Modus Operandi 3: Dramatic Self-Realization

Dramatic self-realization is another technique that enables Russian trolls to simulate the authenticity of self-presentation. This technique enables performers to appear spontaneous or authentic. For example, to facilitate discussions about the practice of dramatic self-realization, Hilton (1953) coined the term “calculated spontaneity.” This term refers to the need to achieve a conversational or spontaneous tone when reading a script. While this competence is crucial for professions, such as those involving presenters in TV or radio broadcasting, it is also applicable to online scenarios. Thus, dramatic self-presentation is acceptable or even desirable in certain situations, such as those involving TV, radio, or the internet. In fact, calculated spontaneity is a professional expectation for some occupations, especially those related to public speaking. For Russian trolling, however, strategic spontaneity is a tactic of influence.

Russian trolling as performance entails another strategic principle—what Goffman (1959) called expressive coherence, whereby “performers tend to foster an impression that their current performance of their routine and their relationship with their current audience have something special and unique about them” (p. 4). Consequently, once the mask is on, the expecta-

tions of that mask must be fulfilled. On a similar note, Enli (2015) spoke of a concept of mediated authenticity and the craft of the construction of the authentic self. And even if that authenticity is highly constructed, what matters is how the general public perceives these self-presentations. In other words, if spectators perceive interactions as authentic, they become authentic.

In the social media world, a similar concept of strategic authenticity has been proposed as an instrumental logic wherein the value of authenticity is based on ensuring a loyal base of followers (Gaden & Dumitrica, 2015). Thus, the calculated spontaneity, or what Gaden and Dumitrica (2015) referred to as a strategic authenticity, dominant in the current social media world, allows for the self to act differently in various settings. In these settings, or what Marwick and boyd (2011) called context collapse, expectations of different audiences encourage the compartmentalization of behaviors. For example, in an academic setting, a professor could opt for a dramatic classroom entry, while in daily life, that same professor could behave with extreme modesty. In the case of Russian trolling, however, constructed authenticity allows trolls to perform in masks based on the specific expectations of authenticity within political spectra they want to target.

Multiple Faces for the Masks: Commenting User Typology

Multiple masks and different faces constantly appear in online news portal spaces. While this book's objective is not the identification of real faces behind masks, it does explain how masks create online chaos regardless of the users who adopt them. To advance studies on online social influence, online user performance can be categorized by three types of behavioral data points, according to commenting user typology (CUT): content level (topic of the story category), user level (frequency of posting), and timing and location of postings (Zelenkauskaite & Balduccini, 2017). Additionally, online participation has been differentiated based on frequency—that is, through the identification of specific online behaviors, such as the hyperactive posting behavior known as “superposting” (Graham & Wright, 2014). Thus, CUT categories can be used to assign online participants to spaces where they repeatedly contribute and where Russian trolling callouts take place. In fact, active participation online was found to lead to a paradox where engagement in more of the political talk led to larger amounts of information spread, as shown by empirical evidence from private messaging (Rossini et al., 2020).

To uncover Russian trolling justification as a manifest phenomenon online, this book furthermore traced how Russian troll justification circulated across platforms. Although masks can be associated with individual users, they primarily represent prototypes of the Russian troll. Prototypical masks are considered in order to shed light on users' commenting behavior, as viewed through the critical lens of Goffman's performance theory. These prototypes are presented here as aggregates—in a form of frequently repeated comments that exemplify user commenting hyperactivity. Such online hyperactivity requires consideration of posting frequency, sustained over a specified time period. Frequency of posting was traced by taking into consideration the range and number of commented stories; and the content, style, language, and tone of posted comments.

Based on the premises of CUT framework introduced earlier, where commenting behaviors in online news portals are concerned, a typical user is expected to post several comments per story. For example, the *Breitbart* sample for all stories analyzed in this book totals 4,049 users, all of whom contributed by using public accounts. While an average posting comprised 4.2 comments per user, some users posted significantly more frequently than others. Of the 4,049 total users, 25 posted more than 50 times, generating a maximum total of 152 posts per user. Users are expected to be active in response to a wide range of news stories or to target specific ones. By reviewing all 13 news stories on Russian trolling published throughout 2018, variations in user posting have been identified. For example, while several users posted in response to one news story on Russian trolling, a noticeable percentage of users seemed to claim specialization in that topic. Specifically, such users were found to return to comment after the release of Russian trolling stories—even if that release had occurred several months earlier. Some of those users appear to be particularly dedicated toward Russian trolling stories; in some cases, the same users were found to comment on five separate Russian trolling stories.

This section specifies several techniques for unmasking trolls. The first asks whether news comments left to stories covering Russian trolls are public or private. This allows us to identify the degree to which users are “covering themselves” when discussing Russian trolling as a phenomenon. The second deals with automation. To assess whether users were striving to circulate repeated comments, the amount of duplicate comments were assessed. Such repetition can indicate an intent to circulate specific content, be it manually or via automation means. These two unmasking techniques are used by comparing news stories that covered Russian trolling alongside those that are unrelated to the Russian trolling, such as those on *Breitbart* specifically

focusing on sports stories. Following this procedure, prototypes of frequent posters are analyzed and presented.

Finally, the masks exposed in the news portal comments are presented through text-based means. As discussed earlier, these masks are accompanied by tactics, such as calling out Russian trolls or impersonating them. These analyses highlight the dichotomy involved in the positioning of Russian trolls within a single news portal or across multiple ones. In some instances, users acknowledge the existence of Russian trolls and the fact that their primary objective is persuasion. In other instances, users comment aggressively to justify or to deny the existence of such trolls. Although these arguments are widely divergent, they are invariably expressed with noticeable frequency across news portals.

Visibility of the Masks Through Private Versus Public Posting

Users who posted on Russian trolling stories were analyzed according to automation and anonymity, the main tools of computational propaganda. Automation of posting and self-presentation through anonymity can provide masks for Russian trolling to masquerade online by merely adjusting user privacy settings that allow one's comments to be visible or invisible. Thus, trolls can take advantage of the various levels of anonymity or identity-masking that news portals provide or use to create perceptions of a genuine public sphere debates. Thus, sociotechnical configurations of news portal comments matter. For example, the Lithuanian news portal Delfi.lt allows for anonymous posting. The majority of comments on the portal are anonymous, with no user identifiers other than IP address. Even if users register to post comments, they use social media screen names. Otherwise, they opt for Delfi.lt accounts that permit them to select any self-identifying screen name. Previous studies of Delfi.lt indeed found that anonymous IP posting dominated commenting on Delfi.lt (Zelenkauskaite & Balduccini, 2017). This shows how anonymity can be a tool that is utilized to project publics and what scholars call counterpublics—the movement that challenges the established status quo (Asen & Brouwer, 2001). Discussion regarding Russian trolling becomes a terrain to uncover the relationship between various types of publics and anonymity.

Let's first look at media systems at play and how they allow for anonymity to be revealed. As described above, Delfi.lt account settings and user options do not enable greater transparency. They are, in fact, very similar to those employed by the *New York Times* or *Breitbart*. As for Gab, users create

accounts, as they would for any social networking site. During the data collection period for this study, all Gab posts were publicly accessible. However, by using the third-party Disqus platform, *Breitbart* allows users not only to create accounts to comment on multiple sites but also to preserve the privacy of their accounts. The platform promotes such user options by stating: “Most importantly, by utilizing Disqus, you are instantly plugging into our web-wide community network, connecting millions of global users to your small blog or large media hub” (“Disqus, What is Disqus,” n.d., para. 1). Making accounts private prevents other users from accessing posts across multiple news stories when they open a specific user account.

The analyses referring to the individual user activity and anonymous vs. public user commenting practices presented in this section is exclusively based on *Breitbart* because it is the only news portal in the sample that uses Disqus, a third-party platform based on individual user accounts, rather than message-level presentation of the comments. These individual accounts provide a lens for understanding online masks, as users can choose to have their archives visible or invisible to the public. About 53% of comments, or 19,152 comments, were found to be sent from private or “masked” accounts in the analyzed sample of comments in response to *Breitbart* news stories on Russian trolling. These private accounts do not allow for a reader to see any other content associated with a given account or their frequency of posting.

To account for the typicality or atypicality of private commenting for stories related to Russian trolling, stories on unrelated topics were also collected, such as *Breitbart's* sports stories on the South Korean 2018 Winter Olympics in Pyeongchang. This additional sample was collected with the expectation that users act similarly on both samples in terms of choosing anonymity in the posting. Twenty stories generated 4,554 comments. Of this total, 1,761 (or 39%) were posted privately. Yet Russian trolling and the sports story posting by users indicate vast differences in two ways: First, Russian trolling stories received more comments overall; second, they also had more comments from private accounts. This finding further supports the claim that masking is a major behavioral characteristic of Russian trolling news story commenters.

To identify the level of content circulation through masking, amounts of repeated posts or duplicate comments were assessed in both samples. In the analyzed sample that includes 13 *Breitbart* stories on Russian trolling and 37,137 comments, 7.6% ($n = 2,851$) were duplicate posts. By contrast, examination of *Breitbart's* news stories on sports topics yielded far fewer duplicate comments, at 2% ($n = 94$), which shows how comments on Russian trolling were more likely to recirculate the same content, indicating

either automated content circulation or repeated frames to try to convince someone of something, compared to the comments on the sports story, which had a limited number of duplicates.

Analysis of public comments also yielded divergent results in the analyzed samples. This part of the analysis excluded comments for which users had selected private commenting options. On average, 1.9 comments per user were publicly posted in response to sports stories. For these stories, 1,467 users posted a total of 2,793 public comments; 965 of these comments (or 66%) were posted by users who posted only one comment, and the maximum posted was 36 by one given user. However, the Russian trolling news story sample included 16,985 public comments posted by 4,050 users, with an average of 4.2 comments per user. In this same sample, 1,847 users (or 46%) posted one comment, while one user posted a maximum of 152. This shows that commenting for news stories that covered Russian trolling was much more active, with twice as many comments posted by a given user on average than for the sports stories. As conceptualized by CUT, these contrasts in commenting, together with the posting frequency for a given story at a steady rate of one comment per minute, point to automation or at least intentional intensity of the posting process.

By reviewing duplicates within comments' sample for news stories that covered Russian trolling in the *Breitbart* sample, the following results were tabulated.

Table 1. Number of duplicates

Type of comment	Total comments	Duplicates	Percentage
Private user comments	19,152	2,613	13.6
Public user comments	16,985	136	0.8
Total	37,137	2,749	7.6

Results in table 1 indicate, for example, the significantly greater number of duplicates in private comments compared to their public counterparts. Timing is also relevant for the successful continuation of disinformation. If the audience is privy to only a brief performance, that fleeting glimpse diminishes the potential for embarrassment that results from exposed inconsistencies within that performance. Posting frequency varied in commenting behaviors for Russian trolling and sports stories. Thus, staging of that which can be seen is another technique that Goffman has elaborated on. In other words, the performer must be cautious about the conditions under which the performance is to be staged. The same caution must be exercised for messages left in news comment spaces. For Russian trolls to succeed, it is crucial to send the right persuasive messages at the right time. Such

messages need to follow news story cycles—that is, immediately after news story release—for maximum exposure. In cases where online trolling is a masquerade, timing is particularly critical. Thus, trolls need to latch onto relevant news portal stories the moment they are released. Interestingly, previous research on tactical commenting in online news portals found that there was a percentage of users who posted frequently right after news stories were published (Zelenkauskaite & Balduccini, 2017).

The following repeated comment sequence exemplifies such frequency. The comments were spawned by an anonymous user within four minutes in response to a Russian trolling story:

Breitbart Example 1

2018-02-16 19:13:54 Wired Sources @WiredSources

BREAKING: DOJ issues indictments against 13 Russian nationals and three Russian entities for election interference, organized anti-Trump ‘resist’ rallies. https://twitter.com/WiredSources/status/964566099865030656?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fredstatewatcher.com%2Farticle.asp%3Fid%3D117940

SO THE RUSSKIES WERE COLLUDING WITH GRANNY! BWHAAAAAAAAAAAAAAAAA

2018-02-16 19:14:44 Wired Sources @WiredSources

BREAKING: DOJ issues indictments against 13 Russian nationals and three Russian entities for election interference, organized anti-Trump ‘resist’ rallies. https://twitter.com/WiredSources/status/964566099865030656?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fredstatewatcher.com%2Farticle.asp%3Fid%3D117940 SO THE RUSSKIES WERE

COLLUDING WITH GRANNY! HOHOHOHOHOHOHOHO

2018-02-16 19:17:33 Wired Sources @WiredSources

BREAKING: DOJ issues indictments against 13 Russian nationals and three Russian entities for election interference, organized anti-Trump ‘resist’ rallies https://twitter.com/WiredSources/status/964566099865030656?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fredstatewatcher.com%2Farticle.asp%3Fid%3D117940 SO THE RUSSKIES WERE

COLLUDING WITH GRANNY! BWHAAAAAAAAAAAAAAAAAaa

2018-02-16 19:29:12 Wired Sources@WiredSources

BREAKING: DOJ issues indictments against 13 Russian nationals and three Russian entities for election interference, organized anti-Trump ‘resist’ rallies.

2018-02-16 13:24

GRANNY COLLUDED WITH THE RUSSKIES ON THE ELECTION
<http://redstatewatcher.com/article.asp?id=117938>

The example above illustrates a sequence of repeated comments by a given user. Time stamps of the comments show a rapid reposting. The consistent frequency of the repeated comment indicates automation behind its propagation. Otherwise, it can be deduced that the posting user intended the comment to stand out among the others. In either case, it is worth noting that one of the comments in the sequence had been linked to a tweet from a suspended Twitter account. This finding illustrates how users can try to promote content through news portal comment sites after they had already violated other platform regulations and are subsequently blocked from them using them. Moreover, the RedStateWatcher article link directs to a page with story claiming that Russian trolling does not exist. That online story also vouched for the innocence of Donald Trump and the need to investigate his political opponents (e.g., Hillary Clinton). Public users posted the following duplicate comments:

Breitbart Example 2

2018-02-17 03:14:01 “There is no serious person out there who would suggest somehow that you could even rig America’s elections.” ~Barry Obama

2018-02-17 00:55:03 “There is no serious person out there who would suggest somehow that you could even rig America’s elections.” ~Barry Obama

For a story headlined, “Putin ‘Couldn’t Care Less’ About Russian Interference Claims,” these duplicate posts emerged:

Breitbart Example 3

2018-03-11 06:25:27 He doesn’t care, because he is SANE.

2018-03-11 01:49:41 He doesn’t care, because he is SANE.

2018-03-11 02:01:25 He doesn’t care, because he is SANE.

As seen in the examples above, although posting times vary, these comments were sent on the same day and in response to the same story. These examples illustrate the facility of duplicate concealment through private posting. In other words, private posting obscures the sequence of duplicated posts. Duplicate postings as a type of content memetic circulation have been found in other platforms such as 4chan, typically used to circulate hate and anti-Semitic content (Zelenkauskaitė et al., 2020).

Facets of Commenting

Looking at specific users and the frequency of their posting patterns online to stories related to Russian trolling on *Breitbart* provides a more fine-grained insight on attack and defense interplay. Such a coexistence of attack and defense tactics (i.e., comments that support Russian trolling or are against it) may look like what is referred earlier to as perceived counterpublics. To identify what type of narratives are projected to discuss publics and counterpublics, the most frequent posters who intensely and repetitively posted in a condensed period of time were further analyzed.

Within the sample of users who posted more than 50 comments within a comparatively short time, atypical behavioral traits that included posting frequency were identified. For example, user 276975563 (users were assigned an arbitrary number to preserve anonymity) posted on two separate days and in response to two different stories. In the first instance, posting began on 16 February 2018 at 20:43:28 and ended on the same date at 22:34:06. During those two hours, the user generated 67 comments. One comment per minute appeared in the first 17 minutes before the posting rate decreased. Within the next 111 minutes, the user posted 67 times, for an average of approximately one comment every 2 minutes. The remaining two comments were posted in response to a different Russian trolling story nearly six months later, on 21 August 2018. For this later story, the user generated three comments within 2 minutes. According to the user's self-description and overall activity via Disqus, the user is from a broad geographical location ("the Midwest"); joined the platform on 13 January 2018; and since that date produced 25,292 comments and registered 58,420 "likes" across the Disqus platform. Comments posted by the user include the following sequence:

Breitbart Example 4

- 20:43:28 Trump never colluded–EVER I hate liberals
- 20:44:13 He's your leader.....for seven more years
- 20:44:28 TRUTH
- 20:45:12 Liberals are the true enemy. Pray to God one doesn't get elected president. . . . or we're all f­ucked
- 20:45:48 ((((((WAN)))))))))
- 20:46:56 There are more beasts.....never forget
- 20:47:45 The FBI found 13 Russian f­ucks but couldn't find one teenage boy after two alerts?
- 20:50:06 Chris Steele colluded with the Kremlin to meddle in our election!

The Frequent Poster

User 67599310 generated 152 comments, the greatest number of posts in the analyzed sample. These focused on three stories related to Russian trolling. User's self-description and overall activity via Disqus reveals that the user did not provide a location; joined the platform on 2013 August 15; and since posted 10,085 times and registered 4,315 "likes" across the platform. Although the user had occupied platforms 5 years longer than user 276975563 in the first example, the user 67599310 generated approximately half the number of comments during the same time on the *Breitbart* news portal. This number indicates that the behavior of user 67599310 is atypical where posting frequency is concerned.

User 67599310 focused on two stories in the sample that cover Vladimir Putin and a video report on Russian troll indictment. All three commenting sessions occurred on three separate days when the news stories were released. Seven comments were posted in response to the first story, five of which were produced within five consecutive minutes at 5 p.m., and two within two consecutive minutes at 6 p.m. The greatest number of comments from this user (134) pertained to the 2018 February 16 Russian troll indictment story. The user continuously posted 130 comments from 19:27:34 on the story release date to 02:46:20 on 2018 February 17. Of these comments, the first four were posted within the first 4 minutes. The user resumed posting after 30 minutes, and within the next hour produced 33 comments. This commenting frequency can be calculated at approximately one comment every 2 minutes, a similar rate to that of user 276975563. Within the next hour, 48 comments were generated, or approximately more than one comment per 1.5 minutes. In the next hour (10 p.m.), the user's comment count dropped to 24, or less than one comment every 2 minutes. At 11 p.m., the comment production rate further decreased.

Multi-Story Poster

User 2832674 was unique due to the 131 posts generated in response to five different stories related to Russian trolling. The user defended Russian trolls with comments like these:

Breitbart Example 5

2018-02-16 20:15:38 It's possible some Russians did . . . but not Putin . . .
He is as opposed to the Soros Globalist ilk as American Conservatives are . . .

for different reasons of course. Russians are no longer ideologically “pure Communist”, as they once were.

2018-02-16 18:59:39 It's nothing new that Russia would like to influence elections, politicians, even Charities or Foundations ran by ex-Presidents. Lets get on with more Indictments.

2018-02-16 21:38:24 Now I bunch of Ruskies who had fake twitter accIts . . . you have a vivid imalation . . . i'll give you that. Trump was vindiled today . . . Did you miss that part?

Most of user's 2832674 posts focus on two stories about Russian troll indictment released on 2018 February 16. In response to the 2018 February 20 story, the user left seven comments at 11 p.m. that were written within 6 minutes. This multi-story user was found to engage in frequent posting. In response to the 2018 February 16 Russian troll indictment story, the user posted 53 comments from 18:45:55 to 21:07:25. In the first hour, 21 comments were posted at an average rate of one comment every 3 minutes. Thirty-two comments emerged during the second hour.

In response to another 2018 February 16 story covering Russian trolling, the same user posted 62 comments between 9:28 p.m. and 11:52 p.m. In the first hour, 31 comments appeared at an average rate of two comments every 2 minutes. This rate continued throughout the second hour, in which 24 comments appeared.

The user also posted comments in response to news stories published through 2018 (e.g., on 20 February, 1 March, and 3 October). In response to the 2018 February 20 story, the user left seven comments at 11 p.m. that were written within 6 minutes.

Thus, it can be deduced that this user is yet another, what can be perceived as, hyperactive online commenter. Examination of user's 2832674 self-description and overall activity via Disqus reveals that the user did not provide a location; joined the platform on 2010 April 29; and since produced 88,573 posts and registered 163,609 “likes” across the platform.

The Opposition Poster

It was discovered that within the same sample, another user, user 280308805, had registered on 2018 February 16 to post comments. This is the same date that user commented on a story about the indictment of Russian trolls. The user produced a total of 227 comments and registered 72 “likes.” In response to a specific story on indictment, the user left 53 comments between 20:18:08 and 21:40:21. This frequency can be calculated as one new post per 1.5 minutes within 82 minutes.

This user embodied the Russian trolling opposition in a form of a sequence of rebuttal comments that acknowledges Russian trolling existing. The used tone degraded political opposition (i.e., the Republicans). The following user posts were created in a sequence:

Breitbart Example 6

- 21:15:22 The kremlin has waited 75 years for the orange low-IQ anti-American racist bigot. The Kremlin become the number one power in the world.
- 21:17:30 The orange traitor has more ties to the Kremlin than he does to the United States.
- 21:19:06 Putin rubs his hands together when he sees Trump.
- 21:20:38 Putin rubs his hands together when he sees Trump. like a child predator sees a 12 yr old little girl lost in the woods.
- 21:23:40 The question is, why did the Russians want Trump to win the election so bad. Russians see Trump and his deplorables for what they are.. low-IQ uneducated Un-American bigots that can be used as tools to destroy the greatness of America.
- 21:24:30 Putin is counting on Trump and his deplorables to destroy America from within.
- 21:25:23 Trump destroys a bit of Irica daily..... as Putin commands.
- 21:26:40 American Patriots are gonna take the White House back from Putin's MAGAts!
- 21:28:12 Deplorables, Why pussyfoot around with Donald Trump when the person you really want to lead the country is Vladimir Putin.
- 21:29:47 Putin is most displeased with the performance of his trained dog Trump.

Similarly, this user is critical of president Trump's supporters by evoking their lack of literacy:

Breitbart Example 7

- 2018-02-16 20:56:16 You can tell the difference between the Russian Trolls here and the Trump sheep. The Russian trolls speak better English. Russians know the difference between there, their, and they're.

Further, this user invoked the "cracks in society" discussed earlier by bringing into the online forum issues of racism that are not directly related to the topic of Russian trolling. These are some examples of the user's posts.

Breitbart Example 8

2018-02-16 20:57:37 Fact is, Trump supporters couldn't care less even if Trump gives the whole country to Russia. they are happy as long as Trump keeps throwing them pieces of red meat regarding their grievances against black and brown people.

2018-02-16 20:46:41 Trump supporters forefathers are the southern conservative confederate traitor trash who waged war on America to keep slavery. Old habits die hard.

The user brought in other “cracks in society” issues, such as the Ku Klux Klan and racism, although they are unrelated to the indictment of Russian trolls.

Breitbart Example 9

2018-02-16 21:12:11 the Republican party really is a big tent! It holds both the Kremlin and the KKK.

2018-02-16 21:06:08 Trumps horrid, evil supporters are so blinded by racist hatred and hyper-partisan idiocy that they don't care that they are helping Russia rape our democracy.

It can be concluded that this *Breitbart* user is an opposing voice, as advocated by the anti-Russian-troll stance. Moreover, the user's comments exemplify attack-based language. This user either represents an authentic “opposition” or due to unusual frequency of posting and focusing on contentious topics and degrading language can be considered as an example of a camouflaged siding with opposition to further stir chaos.

Discussion

Arguments that support Russian trolls or call them out not only create divisive chaos in online spaces but also prove the difficulty of neutralizing denial of the Russian trolling phenomenon. Identified user techniques included reactive strategies, such as rebuttal responses. Some users simply stated, “You are a Russian troll.” Or, depending on content type, they claimed that they are *paid* Russian trolls. These rhetorical strategies typically refer as to debunking—that is, the exposure or uncovering of something after it happened. Yet such rhetorical strategies are hardly effective. Instead, “prebunking,” according to inoculation theory, has been proposed as a more effective

tive alternative for combating misinformation (Cook et al., 2017). In other words, it is much more difficult to change entrenched attitudes.

While debunking and prebunking are both tactics that can be used toward fighting disinformation, they differ in timing. While debunking is post-factum strategy, prebunking allows for the possibility of preventing something from happening. Thus, Russian trolling might be effective when tapping into existing divisiveness and preexisting attitudes. Inoculation theory postulates that people can be inoculated against misinformation through preexposure to refuted versions of comments (Cook et al., 2017). The question lingers, however: To what degree can inoculation counteract disinformation? Based on evidence throughout this book, tapping into vulnerabilities and preexisting partisan divisiveness is a tactic for justifying Russian troll interference in online spaces.

News portal comment spaces resemble backstage areas where information is packaged. And posting news stories comments can be considered as a backstage performance. Goffman (1959) described such spaces as the front- and backstage areas of discourse: “The character staged in a theater is not in some ways real, nor does it have the same kind of real consequences as does the thoroughly contrived character performed by a confidence man; the successful staging of either of these types of false figures involves use of real techniques—the same techniques by which everyday persons sustain their real social situations” (p. 255).

While an actor who occupies a theater stage does not experience real consequences, in online scenarios, malicious *self-staging* can provoke the negative repercussions that typically accompany foreign influence (e.g., Russian troll exposés). And while unmoderated online comment spaces are open to all users for engaging in civil discussions, their undeniable backstage, elaborated on in Goffman (1959) as an element, renders user news commenting both authentic and vulnerable. Goffman (1959) described two situations on a societal level: leveling out of society through the idea of keeping guard of the front stage, for example, when institutions create spaces idea for everyone to be invited. This is authentic because it allows comments to be less filtered. Yet at the same time, anonymous posting invites behaviors that can exceed the scope of individual opinion. Additionally, commenting in online spaces such as news portals can be influenced by foreign governments.

Thus, this chapter records public ambivalence toward the construction of Russian trolling and its various interpretations. On the one hand, such interpretations involve the “noncooperative audience” described earlier—that is, users who call out Russian trolls. On the other hand, they involve recurring Russian troll denial frames that recall Soviet propaganda tactics. Such tac-

tics are adapted and converted into today's digital propaganda techniques that operate according to the active measures. Interestingly, they are also known as the propaganda techniques that are closely related to the tactics of performance whereby the online performer achieves discursive objectives through repeated messaging and the self-concealment that anonymous posting enables.

Tactics of successful performance have been contextualized according to Goffman's (1959) theory of defensive and protective measures. Although propaganda deployment tactics have multiplied, they still resemble these Goffmanian measures. The resemblance illustrates how disinformation, as government-influenced tactics, can be repositioned within the discourses of social anthropology. However, where foreign influence is concerned, such strategic behaviors for influencing public opinion are not mere performative acts. Performative acts in daily interactions, however, can shape perceptions of reality—especially if those acts do not appear contrived and if they manage to resemble typical discursive rituals in news portals' comments (e.g., democratic debates). However, the complication involved in employing disinformation is the possibility that foreign governments can also appropriate them. In other words, foreign government operatives could use such measures to influence public perception by creating division and chaos, and by subverting the democratic debate process.

If Russian trolling is assumed to be a masquerade, the assumption explains the paradox concerning the invisibility of real "faces." The assumption is especially relevant for online spaces where invisibility is inscribed in online technological affordances, such as the kind of anonymous posting that can be automated. A popular *New York Times* cartoon from 2000 illustrates this online invisibility with the motto "anyone on the web can be a dog" (Fleishman, 2000). While performativity encourages the staging of authentic self-presentation, it also enables users to hide beneath a created mask that can be crafted and circulated as authentic. In other words, the tricks of identity subversion show how Russian trolling can be constructed in online spaces.

Russian trolling, when centrally coordinated and ideologically orchestrated has the power to subvert, deconstruct, and obfuscate reality. Consequently, the impersonation of authentic online debaters can invalidate news portals' comment spaces as legitimate forums for democratic debate. Instead of providing clarity, such impersonations generate public distrust. If that distrust escalates into the suspicion that public online spaces are being infiltrated by foreign agents, news portal comment readers can become paranoid. Specifically, claims that Russian trolls are omnipresent yet invisible

generate a destabilizing sense of helplessness—the paranoia that Russian trolls are watching constantly.

And while identity performance through text in online spaces allows Russian trolls to remain masked like typical online participants, the same text, as callout comments, renders Russian trolls visible. Thus, text online involves a paradox of visibility: The text can hide or highlight specific facts but also people. Yet comments online are not equally exposed in terms of being found by the targeted audiences and remain invisible for the undesirable ones. In the case of Russian trolls, they want to be seen by the people who allow them to amplify their arguments, but they do not want to be called out by the opposition. What measures do online commenters take to be seen? And since visibility is key in what Davenport and Beck (2001) called the attention economy, what kind of information do Russian trolls need to conceal to retain their performative masks?

The concept of Russian trolling as a masquerade involves acknowledging the possibility that trolls can wear masks and that Russian trolls, in particular, are actors whose performances are based on the requirements of given masks. Moreover, if it is assumed that Russian trolls are Russian government operatives, it can only be hypothesized how the mask functions as the fluctuating barrier between real and performed identities. Thus, we revert to the fundamental questions regarding how identity can be performed and the performative elements that can be optimized in online spaces. After all, the “real” identity in online spaces is tenuous—a construct that can be inferred only through sociotechnical information fragments, such as location, frequency and timing of posting, and intentionality embedded in posted comments.

By contrast, however, the mask can be created through multiple comment types and by employing technological affordances that allow for anonymity and automation of online spaces. These include visibility and the content propagation features of social media or news portal comments. Whether a troll is a performed identity or a person paid to serve as an online actor, the troll’s messages will be archived along with the plethora of other news portal comments. Thus, it becomes evident that the online mask comes to life when performative packaging is fully prepared and the troll’s performance is carefully pre-scripted.

The concept of performative packaging can be explained by comparing techniques for masking to those of classical propaganda, discussed more in detail in Chapter 2. More specifically, the Russian troll mask is analogous to the propagandist mask whose wearer simulates authentic news commenting behaviors. Russian trolling masks come to life through overt and hid-

den propagandist techniques. As discussed earlier, Choukas (1965) specified different types of propaganda, such as covert and overt. Choukas (1965) argued that while the hidden, or covert, propagandist adopts the mask of an opponent's ally—or, better yet, impersonates an actual member of the opposition, the overt propagandist addresses the opponent as you while producing such demands as “You have to do this” or “You must think about this.”

By contrast, on infiltrating the opponent's camp, Choukas (1965) argued that the covert propagandist becomes an opposition member who addresses the others within the group with first-person plural pronouns (e.g., we, us, our, ours). Examples of such propaganda techniques can be found in Russian troll callout comments. Complications arise when such comments are read as infiltrated texts, and they generate the question, Who are the opponents of Russian trolling? Thus, the possibility of infiltration creates more uncertainty rather than greater understanding about what happens in online spaces where anyone can be a Russian troll and where online chaos is a constant source of public anxiety.

Russian trolls have been detected behind online locations, IPs, and anonymous posting masks—all of which are used to construct online identities. The mask is supported by the online platforms that allow the troll to craft identities in controlled ways—namely, by highlighting specific parameters while de-emphasizing others, given that an online profile can be created without providing a real name or user photograph—certainly without explaining or justifying one's personal beliefs. Such user information privacy is central to the democratic principles that govern the online public sphere. As discussed earlier, online news portals typically allow anonymous posting. According to democratic ideals, the wider the range of voices and the greater the multiplicity of viewpoints, the more fulfilling is democratic deliberation. Yet democratic deliberation can also be challenged by the anonymity that enables users to conceal their identities. And those users concealed behind masks could very well be paid workers who disseminate the kind of propaganda that can undermine democracies.

Summary

Invisibility with malicious intent can fuel the antidemocratic processes that take place through the seeding of chaos and uncertainty about what constitutes truth. While such processes go against the construction of clarity, they endorse turbulence and opacity. Given the number of tasks that bots can perform in online spaces, Russian trolling is easily included among them.

Chaos is the desired outcome of Russian trolls whose goal is to sway online public opinion. Currently, public opinion can be influenced by local actors who have the resources to do so. At the same time, such influence can be activated in any nation's public sphere if that nation has an active, public online presence. Such an active presence enables persuasive efforts to appear genuine. The tactics for influencing public opinion have been discussed in the contexts of masking and self-presentation. Through online news portals, any nation can influence another nation's political arena by replicating the content sets used in classical propaganda. Yet online news portal comments and social media, rather than traditional mass media, provide online spaces for the individualized messaging that promises authenticity. However, such projected authenticity masks foreign government operatives. Ultimately, however, it is not crucial to distinguish these various types of comment senders. Rather, it is more urgent to acknowledge that the goal of such persuasive efforts is to instill mistrust or to seed unresolvable doubt—all of which leads to chaos.

Chaos creates an unprecedented state of uncertainty where government and intelligence community are compelled to act on something intangible, ephemeral, and dynamic. Online spaces invite all users to join the “public debate”—especially where societally urgent topics like Russian trolling are concerned. Chaos is ephemeral, since one comment can diminish the significance of another. It is also dynamic, since there is no clear evidence for its source. After all, access to comments can be changed by creating “attention” patterns, and messaging can be manipulated through the technological affordances of news portals. Chaos is also intangible, since online spaces lack materiality.

Divide and Conquer

Exploiting Political Polarization

New York Times Story 5, Example 1



Faywood, NM September 20, 2018

A Consumers Guide to Detecting Russian Trolls. 1. If the comment says the U.S. interferes in lots of elections so it is ok i–Russia does it—It is probably a Russian Troll 2. If the comment tries to deflect by blaming–Hillary Clinton—it is probably a probably a Russian Troll; and if they blame Obama, it is definitely a Russian Troll. 3. If the comment says that it doesn’t matter because no votes were actually changed–by the Russians—than you should be on alert. 4. Any suggestion that Putin is not a thug should cause serious concern.

This comment showcases how to recognize tropes that typically are pushed by Russian trolls in online news. They are geared to inflame issue-based polarization. The expression “divide and conquer” is a metaphor that encapsulates the polarizing Russian trolling debate. In fact, polarization has been found across news portals’ comments across news stories covering Russian trolling as a rhetorical strategy for shifting the focus of public conversations from Russian trolls to blaming political opponents and conspiracy theories as alternative explanations to Russian trolling. This chapter exemplifies chaos creation through the lens of what Oates (2016) called rewired propaganda, used to reshape narratives. Such shaped narratives that shift the focus from Russian trolls to other actors—tactics found in historical examples of propaganda discourse—are further contextualized in this chapter.

A shift of the conversations from Russian trolling to any other, typically controversial but unrelated issues gradually shed the guise of civil debate to assume the rhetoric of political mudslinging. Conspiracy theories infused into such polarized discussions form the epicenter of online chaos. Such discussions, then, accuse members of opposing political camps of being paid trolls. And such accusations in turn revise preconceptions of Russian trolls as paid operatives, while insisting that the operatives for the paid influence at work is not Russian trolling—that instead, the paid influence is actually an “insider job.” The insider-job conspiracy theories are not new; the same frames were prevalent after 9/11 (Bell, 2018). This chapter is about the techniques geared toward division in the propaganda of the past and today through computational propaganda.

Such polarized Russian troll justification arguments, charged with affect, can be tailored to elicit responses that resonate with different segments of the readers, as argued in Chapter 1. And the purpose of such elicited responses is to change the focus of the main argument regarding Russian trolling rather than clarifying its premises. Furthermore, denial of Russian trolling involved the transfer of blame from Russian trolls to political opponents. In the *New York Times* blame is shifted to Republicans; on *Breitbart* and Gab, Democrats are blamed. In addition, a heavy use of conspiratorial explanations was found to justify this shift in discourse. This chapter discusses the rhetorical strategies of blaming that have been identified in news comments in the stories on Russian trolling that argue against the existence of Russian trolls.

There are different strategies to exploit the existing political polarization to justify Russian trolling: Russian trolling can be posited as a fact; culprits for Russian trolling can be exposed or by merely shifting the blame to anyone else. Paradoxically, it has been found that Russian trolls themselves were not exposed as the culprits; instead, political opponents have been framed as such. Such political scapegoating can be strengthened by the *whataboutism*. Whataboutism is a rhetorical strategy that prefaces arguments with “what about . . . ?” It is a tactic because it deflects attention from, in this case, Russian trolling to other, many times unrelated, issues. Those other issues are unfounded or characterized by conspiracy theories. Whataboutism, in short, are deflection tactics where the important information is obscured by diverting attention to something else.

Any unverifiable narrative can be used to hone a whataboutism rhetorical procedure that resembles a hide-and-seek game. The procedure functions like hide-and-seek because the hidden objects of the rhetorical game are the Russian trolls that are obscured from online visibility or justified by accusing political opponents as culprits. Thus, it is hard to pinpoint Russian trolls; they

merely lurk in the cyber-background. However, the traces of Russian trolling are visible through a wide range of news comment arguments that aim at justifying them. Thus, collaboration or alliance among users is required for the hide-and-seek of whataboutism to be effective. In other words, if a user is already prejudiced against a political candidate, that user is likely to automatically agree with any statement validating that prejudice. Thus, Russian trolling has been justified within discursive contexts that pit conservatives against liberals. Such sociopolitical polarization creates the complex rhetorical justification that ultimately extends protection to Russian trolls online.

This chapter provides a panoramic view of the approaches used to understand Russian trolling by shifting gears from the sociotechnicality of Russian trolling and considerations of them as masks, detailed in Chapter 1—i.e., from the technological affordances that enable one to manage one's identity through technological means and social practices of a given online community or platform—to the mechanics used in propaganda and persuasion. It begins with an overview of the forces of influence as comparable to mosaic pieces—when assembled, the contours of Russian trolling emerge. To develop the previous chapter's discussion of Russian trolling contextualized as a mask, it can be posited here that influence is yet another piece of the mosaic of the problem of invisibility of Russian trolling. This chapter focuses on the history of how influence has been considered as rendering Russian trolling visible and its connection to the empirical examples of typical propaganda techniques used to justify Russian trolling. The goal is to specify the principles of influence through which invisibility is sustained.

Each piece of this mosaic presented in this book uncovers one side of Russian trolling. The process of exposure begins with these three assumptions about the invisibility of trolls. The first assumption can be formulated as follows: When Russian trolling is approached as a communicative act, its online effects will become visible. The second assumption is based on these premises: If Russian trolling is treated as a communicative act based on influence, mechanisms of influence rooted in various disciplines will be useful for exposing trolls. Examples of these are mass communication persuasion models, propaganda mechanisms, and computational propaganda mechanisms. Finally, the third assumption is: If exposed as persuasion techniques, Russian trolling mechanisms should be related to the repertoire of communicative tactics that have been deployed in the past and included within propaganda studies.

Even if Russian trolling can be treated as a form of influence, influence through which Russian trolling is manifested in online spaces is embedded within a complex media ecosystem. Thus, to tackle this complicated topic,

Russian trolling is rendered visible by focusing on overarching frameworks that contextualize current tactics of influence with the past ones. Such focus aims at illustrating how information infrastructure and automation of content can produce chaos.

The frameworks presented here raise the following questions: What information do we have so far that can enable Russian trolling to be visible? What methodological and conceptual frameworks can work in conjunction with that information? What frameworks of influence could be productively used to understand influence in the era of the digital media ecosystem? Understanding information influence includes knowledge of traditional mass media paradigms and related scientific fields that highlight the complementarity of these paradigms.

The process of exposing Russian trolls is presented in this chapter as a set of lateral sense-making efforts within the following contexts: influence in traditional mass media, such as newspaper comments, followed by historical propaganda cases and computational propaganda modes. This lateral detour toward additional knowledge is presented here by examining what is already known to understand what Russian trolling entails.

These approaches allow us to delineate visible elements of Russian trolling to offer frameworks derived from them and explain the premise behind Russian trolling's "divide and conquer" tactic discernible in analyzed news portal comments. Thus, examples from news portal comments are here contextualized within a network of multilateral approaches to current forms of information warfare. Such contextualization is necessary because Russian trolling on the surface of a given platform is invisible to the public eye. Influence is intangible, and yet continuing analysis of its various forms testifies to its relevance today. Thus, the goal is to expose the complexity of Russian trolling as a form of online influence and to specify how multiple approaches are crucial for tackling this complex issue.

Frameworks of Information Persuasion

Twitter is among the new battlefields of information warfare in which claims of truth emerge and are contested. It has become integrated into military operations and harnessed for public relations campaigns by governments during wartime, but it is also being used by insurgents and terrorist organisations to launch (dis)information and propaganda offensives, as well as by humanitarian organisations, inter-

national observers, the news media and media advocacy groups to provide more ‘truthful’ accounts of the events. (Ojala et al., 2018, p. 299, citations omitted)

This quote by Ojala et al. (2018) specifically referred to Twitter to compare online spaces with information battlefields. An impactful and troubling comparison, it reminds us that information battlefields are invisible, intangible, and obscure. Thus, online spaces are also conducive to hide-and-seek tactics where various invisible players coexist and employ a wide range of tactics. The anonymity and potentials for automation of such players provoke the question: How can we possibly substantiate the existence of information warfare? The key element to consider here, as emphasized earlier, is the type of invisibility that both online information warfare and Russian trolling have in common. While human efforts associated with information warfare can fall within realms of visibility, they can be identified only with prodigious difficulty. Moreover, automated tools that have been developed for information warfare are also invisible because they are deeply embedded within the software of information infrastructures.

While the information battlefield is characterized by invisibility (or partial visibility), Russian trolling has other elements that distinguish it as a relatively new phenomenon. Specifically, it can be viewed as part of a larger cyberwarfare apparatus—a hybrid phenomenon combining astroturfing and targeted influence (propaganda). Yet scholars like Jamieson (2018) claimed that it is a sign of information warfare, provoking a series of questions such as, What can we learn about Russian trolling by reviewing previously analyzed information about warfare mechanisms, propaganda, and cyberwar? Which specific information warfare techniques have been at the disposal of the Russian government? What elements can be identified in the discussion of Russian trolling online?

Communication Persuasion Models

In the 1950s, influence was treated as an interpersonal phenomenon. Katz (1957), for example, proposed that information does not flow directly from mass media forms to targeted audiences. After being introduced to new information, whether through mass media or through other discursive means, information recipients process and make sense of what they have just learned by sharing and discussing it. Katz also observed that information can circulate in different ways, depending on contextual variables, such

as individual personal traits of information carriers. This variable can be extended to include an information carrier's personal social circle that influences decision-making processes. Consequently, Katz postulated that influence can be exercised in two distinct ways: Some people experience influence in the form of public opinion through interpersonal networks exclusively. Yet for others, it is mediated through mass media channels. Such channels in today's media landscape include news portals—and specifically, news story comments generated by regular users, who actively participate in the formation of public opinion, in addition to social media platforms.

Where influence is concerned, classical communication persuasion models have included the following: individual cognitive capacity to process and access information about the influencer, the language used by the influencer, and frames within which specific topics are presented. These theoretical models have been considered for identifying specific ways to increase persuasiveness in mass communication. One such approach is priming or giving prominence to a specific issue. By emphasizing a given issue, priming renders information recipients more likely to remember the content in question. Moreover, if a communicator initiates discussion of a specific issue, the content of that communication will stand out and stimulate additional discussion. Consequently, such discussion items acquire more public prominence. In today's online spaces, such discursive prominence can be achieved through sociotechnical metrics, operationalized, for example, by the amount of repeated content, number of "likes" accompanying a social media post or a news story comment, and by the ranking of such posts and comments by time or user popularity.

According to McCombs and Shaw (1972), agenda setting creates a distinct array of ideas that are catered to and digested for the wider public. For example, when an agenda item becomes the central focus of discussion, it can generate a sense of urgency that drives discussants to elaborate on it. Thus, agenda setting has been typically viewed as a concept applied to information circulation practices based on a centralized mass media model, where someone like an editor in chief can decide which stories to feature. However, what happens when agenda setting falls into the hands of users? What if there are forces beyond the control of regular internet users that start to set agendas through informal information networks, such as news portals or social networking sites, by using automated tools?

To address these questions, it is worth underlining that persuasion has been typically construed as a rhetorical enactment that occurs through mass media and interpersonal networks of face-to-face exchanges. Currently, however, public online spaces, designated by social media and news portals,

have acquired mass media's communicative functions. Typically, mass media audiences are exposed to the content of communication through the frames that mass media organizations provide. While frames remain the organizing structures of content, they are elaborated, cut, prepared, and preselected for audiences. However, today's user-generated content does not adhere to traditional journalistic principles to inform users under the expert guidance of an editor in chief. In short, anyone can contribute to the practice of public opinion formation.

Furthermore, in the current media landscape, framing through language can facilitate content priming's emphasis on selected issues. Such priming makes specific content items more prominent than others. This content "featuring" can favor one type of Russian trolling over another. In the case of Russian trolling, it can be framed as "existing" or "justified" or projected as a cyberhoax. While previous research has proved that interpersonal networking and mass communication can effectively impact public opinion, it is becoming increasingly evident that social media posts and news story comments can achieve the same effect today.

Thus, that influence departs from the previous models of persuasion by taking advantage of network-based structure and accessibility of online spaces, yet the orchestration of influence remains similar. In her analysis of Russian hacking and the 2016 US presidential election, Jamieson (2018) identified the following mechanisms through which such hacking could have occurred: "Use of agenda-setting and framing; Weighting of the message environment (priming negative messages of the opposition); Reinforcement of content that is already circulating; Focus on a specific time window; Exploitation of susceptible voters" (p. 60).

Thus, Jamieson (2018) demonstrated how influence functions as a multiple-level collective effort—one that propaganda exemplifies when it assumes the rhetorical contours of orchestrated persuasion models. This chapter, therefore, revisits historical techniques and approaches to propaganda to inform the current state of ideological influence.

Mechanics of Propaganda

"Everything old is new again" was Abrams's (2016) assessment of Russia's propaganda playbook from its historical roots. We are witnessing how mass and social media influence have evolved alongside interpersonal persuasion models and have been frequently incorporated into propaganda during times of political turmoil. Abrams (2016) continued to explain the shift

with this eloquent parallel: “Plant, incubate, propagate has been replaced by tweet, retweet, repeat” (p. 20). This chapter extends these frameworks to discuss the mechanics of propaganda: how disinformation is readapted for different sociotechnical environments. Furthermore, the goal is to uncover some content-specific frames used to solicit response and affect.

To critically evaluate the current media ecosystems and what they entail for disinformation, this chapter reproposes the overview of the use of classic propaganda models to hone today’s information wars—models that had been developed preceding or during wartimes, currently they are utilized in information warfare. Thus, the current influence models, such as those underlying computational propaganda, can be traced to propaganda techniques deployed during World War II.

In the recent aftermath of reported interference in the 2016 US presidential election, the need to acknowledge information infiltration as result of “active measures” has resurfaced. Such active measures include the ways in which the former Soviet Union orchestrated its propaganda dissemination. According to *Operation InfeKtion: Russian Disinformation From Cold War to Kanye* (Operation InfeKtion, 2018), a *New York Times* video series, the propaganda tactics underlying information warfare have never been forgotten but rather perfected. *Operation InfeKtion* presents such tactics by specifying rules that are based upon three message components: sender, receiver, and context. While these components underly all communicative settings, the seven directives in the active measures playbook are exploiting the “cracks” in society (i.e., the discursive spaces into which propaganda can infiltrate), creating a big lie, including an element of truth, concealing the source (of information), finding a useful idiot, denying everything, and playing a long game (Operation InfeKtion, 2018).

Such a propaganda apparatus functions like an interpersonal network of rumors, where the exploitable “cracks” are vulnerabilities, doubts, or unresolved and silenced social issues, such as exploitation of political polarization. All countries have their own particular social issues that are frequently unvoiced or are sensitive and potentially divisive—the metaphorical “elephants in the room.” These include racial or gender inequality, immigration, or movements like #BlackLivesMatter and #MeToo. Thus, a “big lie” is formulated around a sensitive issue to initiate provocation. To make that “lie” appear plausible, an element of “truth” is retained within it. Thus, the lie’s credibility enables its wide circulation—so that, like a contagious virus, it infects all who come in contact with it. An important aspect of this analogy is the concealment of original information sources, which complicates their verification. When the lie’s fabricator establishes a semblance of plausibil-

ity and conceals its origin, the fabricator can find a human medium that endorses it and increases its audience reach. When charged with lying, the fabricator and all accomplices deny the charge and prolong the lying game for as long as possible. This entire active measures sequence, then, becomes a long-term investment in a specific issue—one that is fueled by the compulsion to divert public attention toward an issue that has been problematized to widen extant “cracks” within society.

Propaganda, as a form of information influence in various social contexts, can achieve a wide range of objectives. As a result, propaganda can shape dogmatism, maintain the status quo of authoritarian regimes, and influence the citizens of other countries to resist their government’s authoritarian practices. The comparison of propaganda with rumor enables the invisible to become visible through meaning-projection mechanisms. Paradoxically, however, as with rumor, Russian trolling strives for visibility, as noted in Chapter 1. The phenomenon is visible within specific contexts where contention is present. Consequently, Russian trolling’s visibility requirement is determined by its need to “infect” and to propagate within online spaces. Thus, visibility is achieved through a content-crafting process that maximizes the virality of messages—or at the very least, their repeatability. Expanding the frames in traditional mass media took place through highly orchestrated, top-down mass media channels where the one-to-many transmission medium of TV allows to mass spread disinformation. Social media allows for information or rumors to spread without editorial support.

The concept of information warfare is related to propaganda exploitation. Typically, information warfare is grounded in concessions between states where rivalry strategies are constantly employed and are based on indirect cyberinstruments (Valeriano et al., 2018). Information warfare’s coercive strategies that can employ propaganda include disruption, espionage, and degradation, as well as types of signaling a given message. While typically argued to involve states rather than citizens, they can be applied to target susceptible internal populations (Valeriano et al., 2018). Similarly, Abrams (2016) added to this list multiple examples of what he referred to as exploiting political rifts to forge Western alliances, such as financing the nationalist far-right political group led by Marine Le Pen, where this political front was running with anti-immigrant rhetoric and belong to a “pro-Russian” bloc in the European Union.

Propaganda has been typically viewed as the effect of mass media’s centralized messaging efforts. Despite its decentralized status today (considering the integration of user-generated content), it paradoxically retains its centralized objective of information dispatch. Welch (2013) identified the rise

of propaganda as the result of conflicts while viewing it concurrently with the emergence of centralized mass media. The essence of propaganda, Welch further argued, is its power to shape and to manage public opinion. Moreover, he described propaganda as a technique that “sparks the flame.” In other words, for propaganda to be employed effectively, its main ideas need to have developed from preexisting beliefs. Thus, propaganda capitalizes on preexisting beliefs while sharpening its focus on specific interests.

Just as Russian trolling, as an information influence strategy, includes an element of invisibility, propaganda (also a form of information influence) is equally invisible. Propaganda is constructed through rhetorical means; it is seamlessly incorporated into existing discourses; it is not explicit—it is covert. Thus, while propaganda can help explain the phenomenon of Russian trolling, it can be perceived as intangibly woven into familiar individual (authentic) fabric of online discussions. Choukas (1965) took the definition of propaganda to an extreme by stating that it is an instrument of social control and manipulation, accessible to any individual or group with the means to employ it in their own interests and against those of their opponents. Moreover, Choukas (1965), to a certain extent, compared propaganda to crafted political forces. Although his description of influence exceeds the immediate concerns of propaganda to address public relations strategies, his premises for mass persuasion are presented within the broader frameworks of direct manipulation. Such frameworks are useful for articulating the definition of propaganda in this book’s ensuing chapters.

Throughout this book, influence as propaganda is also treated as an ideological force. Such forces can be automated or not—but in any case, they have been found in recent online media contexts, as detailed earlier. Moreover, frameworks of direct manipulation can provide a general overview of how these forces are harnessed and unleashed. According to Choukas (1965), specifically, when direct manipulation occurs, the propagandist’s role is not to impart the valid truth, but to implant a correct judgment in minds—the kind that would eventuate in the desired response. This idea assumes that once the paradigm or way of thinking is introduced within a convincing context, the individual to whom the messages are exposed will subsequently appropriate them. Thus, propaganda assumes the value judgments. The polarization of values can be exemplified as a compellingly contextualized paradigm or perspective that is easily internalized. Such value judgments can be polarized or presented as a series of dichotomies—or what Choukas (1965) called “two mutually exclusive, sharply delineated alternatives” (p. 190). Thus, the polarization of values is a rhetorical characteristic of propaganda techniques.

Where Russian trolling is concerned, the question arises: How are opinions formed? One way to approach the question is to specify the type of action that can be performed through direct manipulation. For instance, Choukas (1965) claimed that a certain level of direct manipulation occurs when interested parties aggressively promote specific values for public endorsement. He described this manipulation process by outlining mechanisms or situations that enable opinion formation. More specifically, he outlined three general principles of public opinion formation, all of which can be contextualized within propaganda persuasion models—their underlying assumption being that opinion formation can be subverted.

These three points show that direct manipulation works with a value system formed through the synthesis of subjective affect and objective facts. Thus, he argued that, first, an opinion is formed when an individual is experiencing a frustrating situation, and when the exercise of judgment is required to realize an objective. In other words, an opinion formed in unstable circumstances contains elements of the unknown. Any opinion, then, is better than no judgment. Second, an opinion is based on the idea that it is built from past experiences that serve as guiding principles. Thus, opinion bridges objective and subjective worlds—phenomena respectively experienced as external to the self (e.g., facts) and as bounded within its inner confines (e.g., affect). Third, greater emphasis is placed on the actual process of opinion formation. In other words, it is a value-based judgment.

When discussing propaganda tactics, deliberate influence is at its core. Such processes can be detailed through macro-level deliberate techniques, such as, according to Choukas (1965), “the controlled dissemination of deliberately distorted notions in an effort to induce action favorable to predetermined ends of special interest groups” (p. 146).

Additionally, Choukas (1965) summarized the underlying principles of macro-level persuasion include the following elements: The need to influence reflects a common social condition out of which macro-level persuasion elements arise—namely, conflict (e.g., between interest groups); the process of influence (i.e., propaganda) is manipulative, not informative; the desire to promote a viewpoint and to manipulate other minds; and the desire to gain supporters to advance such endeavors—all this emerges from conflicting views, interests, and ideologies. Persuasion is an element of manipulative effort; it is done by inviting people to adhere to ideologies in ways other than force, which would not happen if they had all the facts or information. Successful persuasion leads to actions, and deliberate distortion is an indispensable element. The deliberate intentionality to distort issues rises from the national interest, whether an organized political or economic interest.

Where Russian trolling is concerned, “national interest” refers to the foreign interest in influencing a targeted country’s value systems. The effect of such influence is the generated perception of the “new normal,” where deliberate distortion projects new realities that are presented in an affective guise.

Choukas (1965) distinguished propaganda techniques based on their scope—in other words, they can be strategic or tactical. While strategic techniques involve large-scale composition and are known for their long-term effects, tactical ones are limited in scope and time. Additionally, tactical techniques exploit specific situations and fine-tune them instead of creating them from scratch. Propaganda management has two stages: preoperational and operational. The preoperational stage involves the production of requisite frames into which ideological truths, values, or attitudes can be channeled. At the operational stage, propaganda management tactics involve action-driven items that are reaction based—in other words, items that elicit quick responses. Such tactics are intended for widespread appeal—to provoke or to demand action—and are perceived to be spontaneous. These propaganda elements are applicable to activities that can be performed online. Moreover, when online spaces are characterized by automation and anonymity, such as news portals’ comments, they can provide additional tools for implementing propaganda strategies.

Propaganda has also been characterized as both intuitive and empirical (Choukas, 1965). While its intuitive aspect can be directly related to the affect, generated through a specific emotive moment, its empirical aspect refers to the factual evidence for strengthening an argument’s rhetorical appeal, for instance, justification of Russian trolling. Since both propaganda’s intuitive and empirical aspects are primarily customized for audience reception, the goal is to expose the mechanisms behind that customization.

While the propagandist understands that the impermanence of propaganda models complicates their exposure, the propagandist constantly reinvents these models in response to changing public attitudes. Thus, these models of engagement must be dynamic. In fact, the propagandist must constantly adapt to new frames and exercise sensitivity toward the relevance and changeability of public discourses. In other words, the propagandist is compelled to be omnipresent within public spheres, to compensate for Choukas’s (1965) claim that propaganda has serious temporal and spatial limitations. Such “limitations” are discernible when we acknowledge that propaganda’s “intuitive” elements are the first to be challenged in the face of objective facts. Yet propaganda is primarily grounded in subjectivity. Over

time, propaganda can grow into a scientific apparatus that is systematically utilized and controlled.

Computational Propaganda

In the aftermath of the Russian troll allegations, Twitter released more than 10 million tweets that circulated propaganda (Romano, 2018). This evidence begs for questions such as: Which propaganda tactics remain relevant in current digital media landscapes? While cases of war propaganda discussed later in the chapter showcase how propaganda models of the past have been centralized through mass media forms of distribution, with the preferred modes of simultaneous message transmission being radio, in today's online spaces propaganda is decentralized, yet it can be still centrally controlled and dispatched, as well as further amplified through automated messaging.

The current forms of propaganda can be illustrated by the concept of computational propaganda (Woolley & Howard, 2018). Mechanisms of computational propaganda involve the following elements that are distinct from war propaganda described earlier. First, modes of information dispatching have changed. Computational propaganda involves various automated social actors—bots that are built to behave like real people who participate in human online interactions and can be managed to manufacture consensus or to provide the semblance of support for generally controversial viewpoints (Woolley & Guilbeault, 2017). A crucial approach to invisible computational propaganda involves examining the role of technological affordances and platforms. Thus, propaganda's virality can be explained through the sociotechnical means embedded in online spaces. Virality invokes the idea of content contagion, where popularized content travels through the web—contaminating the very online spaces where it replicates (Nahon et al., 2011).

Yet rhetorical strategies employed in propaganda have not changed from wartime propaganda. The informational content of computational propaganda needs to involve at least some credible aspects of truth—as is the case for more traditional mass media-based propaganda. Thus, to use computational means to generate disinformation, a widespread seeding of information needs to be initiated. This initial seeding can assume the form of opinion sharing. Narratives concerning past elections compare information wars to disinformation campaigns—a rhetorical maneuver that is particularly applicable to presidential elections.

Disinformation campaigns can be effectively launched when efforts are coordinated to share unverified information (Ferrara, 2017). Curiously, unverifiable information resembles rumors—a discursive phenomenon whose embodied medium had been the gossipmonger of face-to-face interactions. Today, the gossipmonger’s discursive function has been reassigned to the invisible agents embedded within online spaces. In their analysis of rumors as propaganda, Allport and Postman (1947) argued that it is particularly difficult to determine where a rumor starts and how it spreads. Russian trolling has been found throughout the examples of this book to be a topic not only of polarized discourses but also of speculation that Russian trolling does not exist. Such speculation, resembling rumors, found across repeated frames across platforms, indicate that it was intended to be spread online.

In the context of news portals, sociotechnical elements are found through designated news story comment fields that represent technological properties, enabling certain online behaviors. At the same time, user engagement can shape technological properties of a given platform. News portals provide a platform for such sociotechnical interactions to take place in a form of democratic deliberation while also enabling influence to take place.

New elements of propaganda include sociotechnical elements of online posting. Anonymity is one of them. According to Woolley and Howard (2018), anonymity enables cyberoffender identities to remain concealed. While such identity concealment bears resemblance to the behavior of masked trolls, automation allows for exposure and traffic. Disinformation campaigns are based on the anonymous user behaviors that online spaces enable. These include the intentional circulation of rumors. Thus, large-scale information behavioral frameworks are primarily used to interpret online behaviors like anonymous rumor fabrication. To account for rumor fabrication, a large-scale analysis of tweets have provided insights into account-level activities, as earlier reported by Romano (2018). Such analysis included user posting frequency, tweet content similarity, and the content’s audience reach. Ultimately, suspension, deactivation, or deletion of Twitter user accounts pointed to the detection of unusual behavior patterns.

While there have been sustained efforts to analyze bot behavior, findings related to this research area primarily focus on “abnormal” behaviors in online spaces. Even if there has been some research progress for assessing the verifiability of real-time Twitter accounts and messages (e.g., through Botometer), those that have been sampled post hoc remain limiting. This book in Chapter 1 presents results of duplicates in the news portal comments to account for the level of computational potential.

At this point, these questions arise: How can nonhuman actors embedded

in online spaces be identified? And, how can their behavioral development be traced? After all, computational means enable the repurposing of propaganda content as rumors—allowing new conditions for circulating them through online networks. And, where information warfare is concerned, such rumors can be reformulated as conspiracy theories that are intended to undermine political enemies and are prepackaged for dissemination through online spaces (Pitney, 2001).

Historical Propaganda

The roots of computational propaganda stem from their historical conceptualizations. However, historical and computational propaganda differ in terms of sociotechnical means of distribution. The means of propaganda has shifted from centralized dispatching (one-to-many mass media means such as radio, newspapers, or TV) to decentralized online operations through networked online spaces, social and mobile media. In contrast, such a centralized dispatch typically had a traceable source of information—one that was characterized by a limited number of official information channels that a few actors could use (Morris, 2000). Such channels were clearly specified and controlled by a centralized government. In computational propaganda, dispatch through networks is less traceable and can be viewed as more subtle. Propagandistic messages in online spaces coexist with other authentically produced user-generated content.

When comparing different types of historical propaganda models, Winkler (1978) observed that centralized messaging has been used to greater advantage in dictatorships than in democracies. In fact, Winkler contended that dictatorships, such as Nazi Germany, found it comparatively easy to produce single-stream messaging. Thus, Nazi propaganda was centralized since the beginning of World War II. The content of such messaging had been inflated, exaggerated, and distorted. Yet this form of messaging proved effective for Germany in the long run—and despite the challenges of maintaining a propaganda factory, especially when the citizenry began to observe discrepancies between projected realities and lived actualities. Perhaps it is inevitable that enlightened citizens resist centralized government propaganda—particularly when war atrocities are exposed to the public. Similarly, social media allow for recentralized dispatch of information to be shared in desired or targeted networks.

Another requirement for propaganda's effectiveness is that its underlying postulated beliefs include some element of truth. When all such require-

ments are met, propaganda can simulate authentic belief systems while also subverting them to divert attention from general questions to their more specifically contested elements. Historically speaking, scholars have argued that the greatest amount of modern era propaganda had been deployed during World War II (Welch, 2013). General tactics distinguish the Soviet propaganda era as the time when information was inaccessible or strictly controlled by the government (Welch, 2013).

Stringent information control functions like calculated rumor circulation, whose intent is to create chaos. By obstructing a given phenomenon, rumors can effectively allow chaos to proliferate. In Soviet times, propagandists exploited rumors by converting them into unverifiable information for widespread dissemination (Hazan, 2017). One such notorious instance of rumor exploitation was the HIV “hoax”—the malicious deception of the origins of the disease. This hoax included the following narrative: After HIV virus was described and published by *Science* journal in May 1983, in July 1983 Indian newspaper *Patriot* naming claimed that a well-known but anonymous American anthropologist allegedly disclosed that the disease samples were brought to the US; and then the virus was engineered and was released allegedly through experimentation with humans (Geissler and Sprinkle, 2019). As Geissler and Sprinkle (2019) exemplified, such rumor techniques successfully proliferated in a pre-internet era.

There are common features, as well as variations, among approaches to propaganda. One shared aspect among approaches to internal propaganda is the requirement of a “closed society,” one whose information flows and systems are strictly regulated, as in Nazi propaganda (Welch, 2013). A closed nature of a given society is self-authorized to halt information circulation—and to do so without approval or disapprobation from beyond its self-circumscribing boundaries. In the current world, the context is different—in democratic countries information is not withheld, since the premise of democracy is informed citizens. However, disinformation and propaganda can use the opposite technique—providing too much information so that it cannot be verified or sorted out.

Pratkanis and Aronson (1992) summarized the Nazi propaganda techniques employed by the minister of propaganda Joseph Goebbels accordingly: “Labeling events with easily learned slogans; creating ‘pictures in the head’ by using innuendo and rumor; using historical symbols and monuments; creating a ‘band of supporters’; ‘inoculation technique’ to defend any defeats; shifting the blame to the ‘opposition’ (e.g., through anti-Semitic sentiments); depicting Hitler as a father figure who embodies all positive social roles (friend/protector/father)” (pp. 252–254).

By using these tactics, Pratkanis and Aronson (1992) furthermore argued that propaganda functioned as a political affiliation technique, even if on the surface such affiliation was not easily traceable. In some cases, alliances are formed for mutual opposition. In the case of denying the existence of Russian trolling, a propagandist might need to form a coalition of a group through a selective set of shared values to form a temporary alliance, such as by exploiting political polarization. These groups had to be found within the American population even if overall trust in Russia was not high in the United States (Poushter, 2018).

Thus, divide and conquer can take place through forming the most unexpected affiliations, especially in politically polarized societies. Contentious issues allow the formation of alliances based on lateral values, that at a given time match, regardless of differences. Russian trolling can exploit polarized issues to create such unexpected alliances by capitalizing on accepted shared values by expecting American conservatives or liberals to justify Russian trolling, evident through numerous examples on *Breitbart* comments in this book. The lateral values that enable such a justification is the common goal to create an allied opposition from liberals.

Historical cases of such an unexpected alliance include the case of Nazi propaganda in the Arab world. Herf (2009) described such an unexpected alliance by asking, If Hitler had written that the “Aryan master race” was placed at the top of the hierarchy, with the other being inferior, how could Nazis find allies among non-European “races”? Regardless of the fact that anti-Semitism could potentially be perceived as targeting Arabs and Muslims in the Middle East, Nazi propaganda was launched and such propaganda was selectively created for anti-Jewish Semites. The explanation for this unexpected alliance is supported by the Nazi propaganda claim that there are ideological parallels and affinities between National Socialism, radical Arab nationalism, and the religion of Islam (as the Nazis interpreted these). Being against someone, creates an opportunity for an alliance.

Techniques of propaganda deployment had some shared properties but were also tailored. World War II was characterized by the propaganda technique development that peaked across countries. Objectives underlying propaganda techniques varied, however, together with modes of deployment. Welch (2013) specified these differences by observing that, for Hitler, propaganda was based on the concepts of simplicity and repetition, and its goal was to persuade average citizens—to direct their focus toward facts to which they had not been previously exposed. The points to be made through this rhetorical maneuver had to be minimal but required frequent repetition, throughout which appeals to contrasting emotions (e.g., love and hate) are

made. By contrast, Soviet propaganda targeted only several party members, while populist agitation was orchestrated through a separate technique involving several key ideas pitched to the masses. Thus, the former Soviet Union's propaganda had been launched through centralized means.

Welch furthermore argued that the German propaganda was distinct since it presented one specific idea to the masses, which had to go through the rounds of repetition to reach the minds of the masses. Repetition, thus, remains a relevant technique of persuasion in the online sphere, given that repeated duplicates online can be dispatched easier than in print media.

Another case of centralized propaganda is Japan during World War II. While military victories were highlighted and exaggerated, corresponding losses were concealed from public knowledge (Winkler, 1978). This dual propaganda strategy shifted public conversations from disconcerting facts about military setbacks to euphoric illusions about Pacific victories.

The British propaganda apparatus in the 1940s had been developed for the management of Britain's African colonies (Morris, 2000). This development started with the establishment of the Dominions Office and the creation of the press officer role. Messaging focused on the following messaging focus sequence: home, empire, allies, forces in the field, the United States of America, the enemy, and neutral countries other than the US. Throughout the British empire, messaging was based on the following principles: First, information needed to be truthful and straightforward. Second, propaganda was to be expressly adapted to the country or group of countries for which it was originally intended. Such straightforward messaging can be illustrated in the examples of binary dichotomies describing Russian trolling: Russian interference happened versus Russian trolls are victims.

Over time, resistance to coordinated messaging surged throughout the US. Newspapers were among the first media forms that provided a forum for objecting to unilateral depictions of war through manipulative messaging. Winkler (1978) exemplified such a resistance of unilateral depictions of war through a quote from the columnist Lindley: "It is better that the public should be confused temporarily than that the opposing viewpoints should be muffled or suppressed" (p. 53). Consequently, to protest the suppression of free expression, numerous heads of news bureaus began to resign. Such resignations were fueled by the fear that their statements to the press could backfire—preventing them from continuing to serve organizations, where even messages crafted in full honesty could be received with stigmatizing suspicion to reinstate democratic ideals.

Communicative Tactics: Attack, Defense, and Whataboutism

Historical propaganda models speak about contexts, motivations, and broad strategic frameworks associated with them. Yet how do they work through the text as a communicative act? While online environments enable rich multimedia and text-based access to public perceptions and beliefs, the analysis of polarization can be projected through theoretical underpinnings of ideology expressed through text. Van Dijk (2011) articulated the complications involved in such analyses: “For the practice of ideological analysis this also means that ideologies cannot simply be “read” of text and talk. What is an ideologically relevant expression in one discourse or context may not be one in another, or may have an opposed ideological function at another moment. This means that ideological discourse analysis is very complex, and needs to take into account all levels of text and context, as well as the broader social background of discourse and interaction” (p. 194).

Thus, van Dijk (2011) cautioned that contexts for ideological analyses are dynamic rather than static. Moreover, he claimed that they underlie ongoing interpretations of language use within social situations. Examples of such ideological analyses include the communicative tactic of “attack versus defense” which can be clarified through categorization—a powerful, albeit reductively polarizing, rhetorical technique that creates simple binaries to be processed by communicative recipients. Such a reductive categorization of self was found to be a powerful rhetorical technique for creating audience rapport and enabling political mobilization. Attack and defense techniques might closely resemble typical forms of online hate speech or internet trolling. However, such techniques are distinguished by the types of messages used for attack or defense. Such messages include the ideological messages that target specific “societal cracks.”

Due to their simplicity, rhetorical categorization devices have been frequently used to shape political discourses—in other words, such devices are not new. “Offense versus defense” communicative frames provide other categorization techniques used in political discourses. For example, in his discussion of “offense versus defense,” Pitney (2001) prioritized the former over the latter: “While the defense is the stronger form of combat, the offense is the preferred form, for only through the offense can we truly pursue a positive aim. Offense provides the only way to achieve victory instead of mere survival. . . . Offense and defense depend on each other because attackers must defend themselves and defendants must strike at the opposition” (p. 36).

Moreover, Pitney (2001) contended that militaristic rhetoric is closely related to political rhetoric. Attack versus defense tactics have been found, for example, in mobilization discourse. Analysis of such a mobilization discourse was also found to be used with the goal to promote “ordinariness” and to justify the resurgence of anti-immigrant sentiment that characterizes right-wing politics. Rhetorical devices in this context included categorization, in the specific analyzed case of the “Australian self” as “ordinary” (Rapley, 1998). Thus, such self-categorization was intended to promote expectations of normalization.

Such defense and attack strategies seem to prevail in ideological discourses, and they are found universally across the web and in various cultural settings. In fact, defense and attack behaviors can characterize warfare, since they intentionally create conflict. In specific cultural settings, however, such belligerent, conflict-generating rhetoric threaten an opponent with loss of face, considered within the framework of facework, discussed in Chapter 1. Thus, this face threat might have driven opponents to relocate face-to-face combat to online spaces for a heightened sense of self-empowerment. Such a rhetorical maneuver has been identified in what Siegel (2015) called digital warfare. Moreover, according to Siegel (2015), the opposition sentiment is signaled through the use specific phrases.

Unlike categorization, whataboutism is a technique that permits new topics to be introduced into an argument. In its most basic form, whataboutism redirects attention (“Don’t look here, but look there instead”). Thus, this technique’s outcomes can range from innocent distraction to a conspiracy theory-based distortion of facts. In fact, the systematic analysis of media networks by Benkler et al. (2018) found that right-leaning networks use whataboutism techniques to disinform viewers.

Whataboutism is a classic rhetorical strategy that has been used in propaganda, where counterarguments are presented by introducing unrelated topics. In fact, whataboutism has been considered a Soviet Russia’s propaganda technique with which Russia’s government deflected criticism by prefacing statements with the question, “What about . . . ?” (Dougherty, 2014). This rhetorical maneuver redirects attention from main problematized issues to new but potentially controversial topics that are frequently unrelated. Such attention shifting becomes the prototypical strategy for discussing trolling behavior—spawning a series of responses that shift attention from Russian trolling to other discussion topics.

Whataboutism typically exploits the “cracks” in society. While these are context specific, they invoke sensitive or divisive social issues that are challenging for analysis and debate. And while such issues are often historically

rooted, they can also generate newer ones based on more immediate socio-economic concerns. Because these divisive issues include uncomfortable truths, they threaten social volatility while eluding simple solutions. Thus, Russian trolling can exploit the potential divisiveness of a whataboutism that facilitates argument shifts. Popularized in recent years, whataboutism has been broadly discussed through various media outlets. For example, the political comedian John Oliver said in a 2017 YouTube video: “[In whataboutism] [t]he assumption is that all actions share moral equivalency. And since nobody is perfect, all criticisms are hypocritical, and everybody should be doing whatever they want” (Olin, 2022). Moreover, John Oliver explained how whataboutism is a communicative strategy that diverts attention from main topics.

At this point, the question arises: What does it mean to use whataboutism in online news discussion? From the topic development structure, whataboutism can be considered a structural conversation technique that promotes topical decay. Thus, when viewed through the lens of coherence from a linguistic structural perspective, whataboutism can be classified as the topical drift of discourse analysis. As Herring and Nix (1997) have explained: “Topical coherence looks at the relation between an individual message and its preceding discourse context, as a means of measuring topic development or drift” (p. 4). This topical assessment was developed by Hobbs (1990), who characterized discourse as either topic focused or digressive. Furthermore, discursive shifts have been defined in terms of parallelism, explanation, or metatalk, and as breaks or ruptures in a given conversation. In other words, a shift occurs when the semantic distance increases between the time when an argument is initiated and when a response to that argument is formulated. Herring and Nix (1997) furthermore argued that such a topical shift is part of not only face-to-face communication; it also is detectable online and frequent in synchronous conversations. Yet during the topical shift conversation drifts on a microsyntactic level.

Thus, when specific topics such as Russian trolling are discussed in news portals, the expectation is that posted comments would be relevant, or at least related to the story. However, if an internet user were to strategize topical digression, the user could employ the whataboutism rhetorical tactic. Specifically, by changing the conversational focus, attention is redirected from Russian trolling toward other topics or issues. This technique becomes particularly powerful if users manage to shift the focus of conversations to other contentious issues. In other words, if the issues to which public attention has been redirected are controversial and domestic (e.g., abortion, gun laws, religion, women’s rights), then the conversation ceases to be about

“them” (Russian trolling or foreign interference) and begins to concern “us”—we, who are “still handling these issues.”

Tactics Used in Online News Comments

Rhetorical tactics such as offense and defense and whataboutism seem to be theoretically clear, yet how do they function in news portal comments? What are the communicative elements used in propaganda today and to what degree? And what can we learn from the historical propaganda today to validate the Latin epigram *Historia est magistra vitae*, or history is the teacher of life?

Online propaganda’s discourse structures are divisible into three messaging-related components: content, structure, and medium-specific tactics or practices for circulation and reinforcement. The concept of communicative propaganda is invoked through the potentials of “computational enhancement,” which refers to a series of discursive tactics found in online spaces. As discussed earlier, whataboutism as a technique can be mere sign of conversational drift or treated as a conversational topical shift. Thus, in some instances, whataboutism can be a deliberate technique to subvert conversations. While this book’s objective is not the identification of levels of intentionality behind posts, its primary concerns are the denial frames that justify Russian trolling and how they are constructed. Such denial frames become mechanisms for delegitimizing the existence of Russian trolling—or at the very least shifting the topical focus of discussions. Moreover, when conversations digress from Russian trolling toward other familiar topics, the controversy surrounding Russian trolling dissipates. Used in this way, it can be a powerful discursive technique that produces tangible outcomes of deflection and denial.

In online US news portals specifically, attempts to shift the object of public scapegoating from Russian trolling to political candidates have been identified. Such attempts are exemplified by attacks on Hillary Clinton and other Democratic Party members. Hillary Clinton and democrats juxtaposed with Russian trolling on an equal grounds, thus exemplifying a case of false equivalency in the following *Breitbart* comment.

Breitbart Story 6, Example 1

Hillary ordered a pee pee dossier that used Russian spies as it’s sources, and was used by the FBI to spy on Trump. I wonder if that is more illegal than Russian trolling?

This commenter shifts attention from Russian trolls to Hillary Clinton. Other *Breitbart* users perform this type of rhetorical maneuver, resorting to political mudslinging that justifies Russian trolling. The objects of such attacks include Hillary Clinton, Barack Obama, Bernie Sanders, and liberals in general.

Breitbart Story 15, Example 1

Hillary had the entire D.C. political swamp trolling the Internet for her. Hillary had the entire NY MSM trolling the Internet for her. Hillary had the entire Hollywood establishment trolling the Internet for her. Hillary had the entire Soros apparatus of paid political protesters trolling the Internet AND Trump rallies for her. Hillary had the entire U.S. Intelligence community led by the Federal Bureau of Investigation trolling the FISA courts for her. And now we're supposed to believe that it is only because of 13 Russian Internet trolls that voters were influenced to vote for Trump rather than for stinky Crooked Hillary? Even the most delusional of libtards don't really believe that.

Breitbart Story 9, Example 1

After Mueller is done investigating Trump and the Russian trolls, hopefully he'll have time to investigate Crooked Hillary.

Yet another *Breitbart* user insinuated that liberals had hired foreign trolls.

Breitbart Story 15, Example 2

Maybe you are. Everyone knows that liberal trolls are owned by foreigners.

Conspiracy theories about Barack Obama were also promoted on *Breitbart* comments:

Breitbart Story 15, Example 3

@ali Russians favored then-candidate Obama and then President Obama in 2008 and 2012, respectively. Let's declassify our counterintelligence in relation to Russian activity then. Because it wasn't simply a catering company's troll army. Let's tell the public. Shall we, @FBI?

By implying that the "real" issue involves Bernie Sanders trolls rather than Russian trolls, several users changed the object of political scapegoating.

Breitbart Story 15, Example 4

They are bernies trolls . . . lol

In this instance, attention is being deflected from Russian trolls to political opponents. This comment is followed by “lol,” which means “laughing out loud” and typically refers to mocking or degrading tone (Fichman and Sanfilippo, 2016).

Breitbart Story 15, Example 5

Is there a difference between russians and liberal trolls?

Similar Hillary Clinton attacks were found on Gab. More specifically, some posts that disavowed Russian trolling simply incorporated a competing “what about Hillary” frame of reference.

Gab Example 1

The most effective thing the Russians did was to use their troll farm to convince Hillary not to visit Wisconsin.

This example creates a rebuttal and shifts attention from Russian trolls to Hillary Clinton. In the following example, whataboutism shifts the conversation from the legitimacy of Russian trolls to French elections and attacks on allegedly Barack Obama’s CIA as meddling in the elections of other countries. Thus, these Gab commenters claim that Barack Obama influenced Marine Le Pen, a right-wing candidate of the 2017 French presidential election.

Gab Example 2

Obama’s CIA meddling in French Presidential Election in 2012 by hacking candidate Marine Le Pen is real Election Interference not 13 Russian trolls & a few thousand dollars on Facebook ads. anti-Russia hysteria is to force a Cold War 2.0

Response: The disgusting little shit also sent hundreds of thousands of TAX DOLLARS and several operatives to Israel in an effort to defeat Benjamin Netanyahu. Not that it was meddling or anything.

A *New York Times* user also deflected public attention from Russian trolls by criticizing Barack Obama.

New York Times Story 7, Example 1

New Jersey Feb. 21, 2018

Outrage is all the left seems to traffic in; it gets tiresome. BTW, speaking of unprecedented violations of sovereignty, what do you think of Obama's (unsuccessful) meddling in Israel's PM election against Bibi? Or because we give Israel so much dough, which makes them our client (and subordinate) state, so it's OK? My, my, there are so very many contradictions to being a leftist, one can hardly comprehend them all.

Yet other *The New York Times* users implied that internal politics are a greater national concern than Russian trolling.

New York Times Story 6, Example 1

Raleigh Nov. 15

Where does this come from? We don't need Russia. FoxNews has no equal. TV is easy-peasy for electronically challenged geezers (like trump). What a propaganda machine. The biggest retirement enclave in the US, The Villages in FL, pumps Fox over public loudspeakers. 3/4 are republicans & some have enough bravado to egg Dems houses before elections. . . . 75 year olds!

Self-Guilt: What About the United States Interfering in Other Countries?

This section illustrates comments from news portals that dealt with what-aboutisms as one of the divisive techniques of propaganda described popularly as “cracks in the society.” The “what about US influence” frame is related to the cracks in society discussed earlier. It is, in fact, an appeal to guilt for justifying Russian trolling—one that is frequently found in news story comments. The aforementioned self-guilt frame, like other what-aboutism frames, has been normalized in the news comments in several ways. An instance of a normalizing argument would be this: “If the US can be charged with foreign interference, then Russia cannot be held accountable.” Other examples are “Because it happened elsewhere, it doesn't matter,” or “Russian trolling occurs in many countries, so why worry about it?” Other normalizing rhetorical gestures include the potential accountability of others: “What about Israeli trolls?” or “What about Chinese or Canadian trolls?” In other words, variations in Russian trolling normalization were

interrogated through whataboutist rhetorical questions about trolls in other countries. At the same time, self-blame was the identifiable psychological subtext in the rhetorical question, “What about us influencing others?” All such rhetorical maneuvers generated these most frequent utterances in news story comment spaces: It is “us,” not Russian trolls—or what about Israeli, Chinese, or Canadian trolls?

Whataboutism spawns arguments based on false equivalence, such as comparing Russian trolls to US-run influence campaigns. This comparison positions Russia and the US on the same political stage, implying that the two countries are not democracies.

Gab Example 3

TrollBot: NY Times Frets About Russian Propaganda. Ignores the Massive Troll Farms Run By America and Its Allies <https://www.alternet.org/grayzone-project/The-New-York-Times-prints-government-funded-propaganda-about-government-funded-propaganda/>

Gab example above uses Russian Trolling defense frame by shifting attention to the alleged massive US Troll farms. Russian trolls are victimized through false equivalency—that is, by comparing Canadians with Russians, citizens of countries that are respectively democratic and nondemocratic. And the reader is left to “question more.”

Some *Breitbart* users justified interference in elections.

Breitbart Story 7, Example 1

Election meddling has gone on since there’s been elections doofus. The US does it too. Most recently in Israel, France & the UK . . . by Obama. Like most people with a brain, I listened to the candidates & made a choice. Puttin didn’t whisper in my ear. Not even once.

By naming other contexts for scapegoating, some *Breitbart* users implied that Russian trolls are victims of unfair treatment. Similarly, other users implied that Russian trolls are not unique in their trolling efforts by listing a number of other trolls:

Breitbart Story 8, Example 1

It’s like Russians are the only trolls. What about African scammers? Hamas and Iran trolls?

Specifically, by including African scammers and Israeli trolls among possible scapegoats, users implied that trolling is not unique to the US, thereby trivializing its seriousness. Other comments implied that some trolls are protected and not investigated, thus making Russian trolls uniquely positioned as victims:

Breitbart Story 9, Example 2

What if they went after all the Israeli hasbara trolls? They'd have to indict half the country.

Yet others mocked Russian trolling investigation attempts.

Breitbart Story 9, Example 3

^^^ Here's a Chinese TROLL Mueller. Have them arrested.

Here is an example of yet another whataboutist attempt to divert attention ("what about British spies?").

Breitbart Story 15, Example 6

So we have 13 internet trolls from Russia indicted for trying to influence our election, but a British spy who invented the pee-pee dossier gets a pass?

The following comments exemplify deflection from the seriousness of Russian trolling by evoking self-guilt of influencing elections of other countries:

Breitbart Story 9, Example 4

Obama tried to influence Brexit vote in UK and elections in Kenya, Libya, Egypt, Israel, Honduras, Macedonia. He gave US tax payer money to anti Netanyahu groups in Israel. I'd wait for a rational response but your a DBAG TROLL so I expect nothing.

Breitbart Story 9, Example 5

How pathetic is this? This troll team only did what dozens of American and Canadian trolls do each day on this site, like Lethal Lily, a Canadian who tried to influence the outcome of our '16 election with his/her posts. If you can go after a Russian troll, why not a Canadian one?

Similarly, *New York Times* users claimed that because the US has influenced the presidential elections of other countries, Russian trolling should be legitimized as a comparable international political activity. In fact, some users invoked US propaganda to create an equivalency between Russian trolling and “Radio Free Europe” implied deviant activities:

New York Times Story 7, Example 2

██████████

Hawaii Feb. 21, 2018

What in the world does anyone think Radio Free Europe was doing all those years? But despite its efforts, did it succeed in toppling communist tyranny? Nations, very much including our own, have been engaging in these sorts of activities in different ways and using different technologies since the dawn of nation-states, and it is bound to continue. Does anyone truly believe it was only Russia trying to sow discord? All this hand-wringing is utterly ridiculous, as are Mueller’s indictments. If anything is to be done, do something akin to what the Soviets did during the Cold War -- jam radio signals and distribute counter-propaganda. I certainly can’t recall any Soviet indictments of Americans over this type of commonplace activity, and for good reason. It’s pointless.

Yet other users expressed concerns about other forms of propaganda.

New York Times Story 6, Example 2

██████████

Montclair NJ Nov. 13

Can you blame them? US propaganda and disinformation makes the Russians look like amateurs.

Several users resorted to “shifting the blame” from Russia to Israel.

New York Times Story 5, Example 2

██████████

Manhattan September 21, 2018

A long piece without naming the Russian oligarchs who cooked up the entire thing and left an intentional footprint pointing to Putin? *The New York Times* has to explain how if Trump is Putin’s guy instead of Netanyahu linked oligarchs, how is it that Russia hasn’t drawn any benefit from Trump

presidency outside of words? How is it that another country has gotten everything they wanted and then some if the entire episode wasn't cooked up by them?

What About Cracks in the Society?

Other forms of whataboutism, related to the concept of cracks in the society, deflect attention from Russian trolling to other social issues. Such blame shifting that targets country-specific cracks in society were reinterpreted within frames for Russian trolling denial. Focus on the following issues in US media comments were found to encourage deflection of public attention from Russian trolling to instilling fear, hate, and prejudice: illegal immigrants (voting), Islamophobia, and self-blame.

This comment exemplifies the whataboutist rhetorical maneuver of shifting blame from Russian trolls to immigrants.

Breitbart Story 6, Example 2

@DropTha_Mic25 Russians in 🇺🇸 get indicted 4 trolling but illegal aliens can protest, block traffic, go to the SOTUS, scream at the sky in the middle of the Capitol, make themselves “more important” than American citizens, mooch off Americans, steal SS#s & be protected in sanctuary cities 🍑

Some users argued that the main issue of contention concerns illegal voting, not Russian trolls, as in the example below:

Gab Example 4

Over a million illegal Hispanics and negroes are voting. Many blacks vote multiple times for Democrats. When caught they do not get fined or go to jail. The democrats thinking cheating is good. They even want criminals in prison to assume that Trump knew about this and was on it. No proof
 Response: The niggers, spics, and Jews know that elections are a joke.
 Joke: Russian trolls are systematically subverting and destroying our political system!
 Woke: Jewish trolls have been doing that for decades.

This user evokes shifting the blame from Russian trolls by evoking anti-Semitic and racist arguments.

Another comment exemplifies the whataboutist targeting of immigrants that underlies Russian trolling denial.

Breitbart Story 1, Example 1

they love another kind of foreign interference, illegals voting.

In this comment, opponents are constructed by invoking the term “they.” Thus, Democrats are otherized along partisan lines.

Breitbart Story 15, Example 7

Yes the Russians brought 13 trolls, the Democrats brought 5 million illegal voters.

This comment replaces Russian trolls with Mexicans as scapegoating objects.

Breitbart Story 15, Example 8

Talk about weak- lmao Where are the “Any day now” trolls? Does this mean all those illegal Mexicans showing up at Trump rallies to Protest are going to be indicted?

Such scapegoating of allegedly illegal Mexicans was also found on Gab.

Gab Example 5

Tucker Carlson pointed out last night that lying liberal hypocrites whine about how Russia “interfered” (used Macedonian social media trolls) & three our election.

But these lying Commiefornians want to give millions of illegal Mexican immigrants the right to vote & ask for sucession (#CalExit).

Response: Wow, when we supported Trump’s campaign the left called us Russian trolls. When we oppose this stupid Syria bombing Trump says we’re Russian trolls. I want my freaking paycheck!

This user shifts the conversational focus from Russian trolls to illegal Mexican immigrants. The post concludes with a new topic (illegal voting). Furthermore, the response to this comment (ironically) claims the “Russian troll” label and requests subsequently to be paid (as Russian trolls are typically considered to be paid.)

Yet other users implied that those who “look like Russians” should be blamed instead of Russian trolls. Such users scapegoated ethnic minorities.

Breitbart Story 12, Example 1

“Ukrainians, Tatars or Jews, but with Russian citizenship”

No instances of Islamophobia or attacks on immigrants were found in the *New York Times* news story comments.

Blaming from Russian trolls was often shifted to the argument “What about Democrats?” Posts like this one imply Democrats should be blamed, not Russian trolls:

Breitbart Story 1, Example 2

what did lenin say, he would defeat the US without firing a gun? He has the democrat party to thank for that. collusion my arse.

This comment exemplifies how conversational focus is redirected from foreign influence to partisan issues.

The majority of comments acknowledged Russian trolling by blaming “the left” for it. Specifically, the left was framed as a group of collaborators, enablers, or scapegoats for Russian trolling. Some users even resorted to sarcastic mockery to claim that liberals finance trolling operations. In some instances, such comments included attempts to “expose” Russian trolls who are hired by liberals.

Breitbart Story 15, Example 9

So you are one of those sorry little anti-Americans liberal trolls that the Russians hired.

Response to this comment included the following comment that speaks about the uncertainty that anyone experiences online with regards to “who is a Russian troll:”

Breitbart Story 15, Example 10

Read my post, I was being sarcastic and far from anti-American. With the amount of pro-Russia posts here I skeptical myself ron g, ur avatar looks like what a Russian troll would pick. Jk. All I’m saying is Any American should be happy that mueller and America have and now will hit back. Find out

the involvement of these 13 pricks and punish them to the extent that no person or country will want to attack democracy again. This is a cause for celebration, muellers got them by the b@lls now

Another user lamented about the effects of the chaos created online, with everyone being suspected of being Russian troll:

Breitbart Story 4, Example 1

The increasing tendency for Democrats to blame Russian trolls for just about anything these days is reminiscent of how witch-hysteria spread and maintained itself in late medieval and early modern Europe. Everything is Russian trolls to the left! You disagree with them online anywhere you are a Russian troll . . .

This comment exemplifies the fallacy of false equivalency.

Breitbart Story 9, Example 6

There's no difference between Lib-idiots infesting the U.S. and Russian trolls other than Mueller will NEVER indict one Lib-idiot much less 13 b/c he knows they would all be found guilty.

Other comments digressed from Russian trolling by implying that Democratic trolls exist and are paid by foreign agencies.

Breitbart Story 9, Example 7

And the 1000+ Shareblue trolls. Shareblue gets cash from Mexico, Saudi Arabia, and China (and others)

Blame shifting has been identified in “what about Hillary” posts like this one.

Breitbart Story 6, Example 3

Hillary started with 10 million for her ‘correct the Record’ trolls, which David Brock quickly morphed into Shareblue. They literally employ hundreds of trolls and use automated bots.

Other users opposed Hillary Clinton and Russian trolls accordingly:

Breitbart Story 15, Example 11

Russian trolls . . . very bad. Crooked H!llary RIGGING her primary and buying the DNC . . . no problems. White Wash it up boys because the FBI is dirty as they come.

This comment exemplifies the whataboutism that denies Russian trolling by blaming the media and leftists:

Gab Example 6

Russians trolls were on the internet and no collusion. No American involved. Meanwhile media matters, thousands of leftist bots/shills, Soros, Obama and all of left wing MSM colluded with Democrats to prop up Hillary Clinton <https://www.foxnews.com/politics/13-russian-nationals-indicted-for-interfering-in-us-elections>

In this example, the Gab user points to the link from Fox News and justifies Russian trolling by deflecting the argument to the “left” as being responsible.

What about Republicans? Other users emphasized the part that Republicans play in in constructing damage for America, which is more important than Russian troll narrative. However, such news comments were published only occasionally.

New York Times Story 6, Example 3

██████████

San Diego, CA Nov. 15

The very concept of objective truth is fading out of the world. Republican lies will pass into history. -George Orwell (updated)

What About Conspiracy Theories?

Conspiracy theories can be embedded in the whataboutism that exploits cracks in the society. The deployment of conspiracy theories provokes self-guilt through statements such as “It is not others but *our own selves* doing the harm to ourselves.” The following conspiracy theory objects were identified in sample news story comments: George Soros (“He is paying people to comment on behalf of the left”), the “blue wave” (“Democrats are paying people to comment”), and the glibble (“the ones who fell for Russian trolling”).

Because conspiracy theories do not require such bases to be deemed plausible, and because they are unverifiable, they can be invoked by anyone at any time and can spread easily from seemingly nowhere. One such theory concerns “blue wave trolls,” otherwise known as “Soros trolls,” that become players in the “information battlefield.” In this case, “Soros trolls” are staged in parallel to Russian trolls, thus making both of them either legitimate or illegitimate.

Breitbart users, for example, have implied that liberals treat Russian trolling as one of numerous conspiracy theories intended to divert attention from significant issues. For example, such conspiracy theories can involve efforts to shift the blame from Russian trolls to George Soros.

Breitbart Story 15, Example 12

this is another deep state frame job to distract us from their crimes.. anyone talking about trump collusion is a treasonous soros paid troll.

George Soros was, in fact, found in the comments as one of the most frequent conspiracy theory targets. In some instances, the letters that spelled “Soros” were interspersed with swastikas, blatant symbols of anti-Semitism.

Breitbart Story 11, Example 1

Why can't SꞤOꞤRꞤSꞤ trolls fabricate better canards?

Some users self-righteously resorted to deflection techniques by invoking George Soros within conspiracy theory contexts.

Breitbart Story 9, Example 8

Saying mean things about Hillary in the first degree, while her Himalayan mountain of crimes go investigated. You see a couple of internet trolls interfered with the election, but Gorge Soros's multi-millions dollar super-pacs didn't. We're living in the Twilight zone, folks

On Gab, George Soros was also a conspiracy theory target. Russian trolling was ignored, instead users were asking “what about Soros agenda?”:

Gab Example 7

RT MAGAPILL

George Soros literally owns several politicians such as John McCain.

Soros funds ANTIFA, pays protesters and interferes in our elections more way more than 13 Russian trolls.

What is Soro's agenda? Who's investigating George Soros?

#ArrestSoros #Russians #Mueller #QAnon <https://pi> [link is inaccessible]

Response: He owns the ballot machine company which provides machines to 25% of all states. These machines can be set up to change every 2,3,4th ballot. Any number you want and you would not be aware. Takes 5 mins to set up

This conspiracy theory sets up George Soros as a funding source who allegedly interferes with the election. The person who responded to the post further exemplified this theory by stating that George Soros “owns” voting machines and creates outcomes of the election as he pleases. This comment also includes hashtags referencing QAnon “movement,” sociotechnically affiliating users who already follow a conspiracy theory, as argued in the academic scholarship (Miller, 2021).

Other conspiracy theories insinuate that Russian trolls have been replicated in the US and that Russian trolling is an “insider job:”

Breitbart Story 7, Example 2

Putin loves Russian interference claims. He could never have hoped to create the mess that democrats are creating for him. If you're a democrat, you're Putin's useful idiot.

Specifically, the comment alludes that the interference claims were invented by liberals. Similarly, another user claimed that media invented the story about Russian trolls:

Gab Example 8

The NBC article cited the firm New Knowledge, which created fake Russian troll accounts on Facebook and Twitter in order to drum up false claims that the Kremlin was meddling in the Alabama Senate election. <https://theduran.com/neocon-war mongers-nbc-slammed-for-drawing-on-dodgy-russiagate-org-in-Gabbard-smear/>

Other users reinforce this narrative by using Russian troll denial frame that blames Robert Mueller for convicting “nonexistent” Russian troll farm, as these posts exemplify:

Gab Example 9:

Mueller “indicted a proverbial ham sandwich—somebody that didn’t exist,” says the lawyer for Russian companies in “troll farm” case #ReasonRoundup <https://reason.com/2018/05/10/mueller-indicted-a-ham-sandwich/> It’s unclear if or when Concord Catering began doing any business in the United States @POTUS

Reference to a lawyer for Russian troll farms who allegedly argued against Mueller was included in this Gab post.

Yet another Russian troll denial frame on Gab included the image of a cat posing as a news anchor that owns a YouTube channel. The image was juxtaposed with a whataboutist reference to the rap artist Eminem.

Gab Example 10

Did Eminem hire a Ukrainian AND Russian Troll hordes to dislike a Digital Cat Avatar News Channel? Also #BootGate, Oh McCain You’ve done it AGAIN. This world is truly has gone bat-shit crazy.

<https://www.youtube.com/watch?v=5dl7mJTjOZO>

@GW

@JoshC

@JonBowePolitix (seen U made a comment there on YT)

[still image and a link to the video with the cat as a news anchor with the headline of #Bootgate 2017 Cat News Network The Truth Factory Breaking News Your home for real news]

The link embedded in this comment leads to *McCain and Clinton Bootgate 2017 and Eminem/Russian Collusion*, a video by the YouTube vlogger the Truth Factory (The Truth Factory, 2022). The Truth Factory uses a cat as its mascot and as of 2022 has 143,000 subscribers. The Gab video post features this cat that represents a right-wing vlogger who critiques the left and everything associated with it. The cat implies that it is actually Eminem paying Russian trolls, downplaying seriousness of the issue of Russian trolling.

Several *New York Times* comments implied that Russian trolling is an “inside job by the FBI.” The implication is a schemed narrative that presents conspiracy-style arguments.

New York Times Story 5, Example 3



phoenix September 20, 2018

What is it that you and all the Trump haters like about an investigation created, plotted and carried out for the express purpose of taking down Trump. An investigation which by now, even the most deranged of Trump haters still retaining minimal brain function must acknowledge, has only exposed the treachery and deceit of some within the FBI and intelligence agencies and ex-Obama officials in manufacturing this hoax. Something at which they have failed miserably.

Delfi.lt users endorsed a conspiracy theory purporting that trolls are paid by the Lithuanian government. In fact, some users circulated the idea that the real trolls are government minority leaders.

Delfi.lt Example by Anonymous Users 1

Headline: trolls are upset

Comment: Our conservative party's so-called elites—is the gang that trolls all Lithuania and all the nation

Response Headline: And the ones who are against this gang

Response Comment: All of them are trolls

George Soros is also mentioned as one of the culprits in the Lithuanian news comments, as seen in the following comment:

Delfi.lt Example by Registered Users 1

Headline: A troll

Comment: We are paid so that we would bark against Russia

Response Headline: I am jealous about kremlin

Response Comment: They have their own propagandists, ours are located in Daukanto street [author's note: The Presidential Palace is located on that square]. Dogs of Soros fund are left to run around

These posts propose that the opposition is treated as a faction of propagandists and points out that trolls can be found on both sides. Additionally, there is a clear projection of the Lithuanian president herself (at the time, Dalia Grybauskaitė) as involved in trolling. Yet, in reality, she is attacked in these posts.

The Gullible Falling Into Traps: We Are the Gullible

After the idea that “Russian trolls do not exist” was amplified in online spaces, the “we are the gullible” trope threatened to generate chaos. “We are the gullible” places the burden of responsibility on the American people for the outcomes of elections and for being duped by Russian trolls.

On *Breitbart*, “the gullible” theme acknowledges to some extent the existence of Russian trolling. However, blame is shifted to the American people, who have allegedly fallen into the traps rigged by Russian trolls. Thus, sources considered internal, rather than external, to the US generate collective self-blame and the ensuing sense of responsibility to tackle the outcomes of having been duped by Russian trolls. An example of an external source is a foreign government accountable for the US presidential election interference. The following comment implies that American gullibility and self-blame derive from external sources (i.e., the Russian government):

Breitbart Story 8, Example 2

We are sooo dumb—Mr and mrs Igor CONTROLS US!!!

Yet rhetorical acts of blaming were polarized—and specifically through statements that shifted blame and gullibility from self to others. On *Breitbart*, while some users acknowledged the existence of Russian trolls, they also claimed that the gullible were the leftists.

Breitbart Story 4, Example 2

It is quite interesting that how the lefties are the ones who bite the baits of the foreign trolls.

Similarly, other comments suggest the gullibility attribution to the “left:”

Breitbart Story 7, Example 1

All democrats are morons. They’ll believe anything you tell them. Why? Because they’re morons.

The “gullible” theme was also identified in *New York Times* user comments. More specifically, individual responsibility was invoked for the need to interpret media content and to identify forms of propaganda. In fact, users resorted to degrading accusations claiming that those who cannot discern propaganda are “stupid.”

New York Times Story 1, Example 1

Phoenix AZ Dec. 19, 2017

Anyone can put words to any photo and create a controversial image. If you have half a brain you could see this is garbage. The problem is not Instagram, the problem is people are stupid.

Yet other users claimed that Americans are “gullible,” not Russians. While they do not directly justify Russian trolling, they attribute current overall poorness of media literacy to failed individual or institutional responsibility to educate US citizens to resist Russian trolling hoaxes. This idea concerning the failure of media literacy education is actually a form of Russian trolling denial.

New York Times Story 2, Example 1

San Francisco Aug. 24

Make. It. Stop. Russia didn't meddle in our election. They made laughingstocks out of Americans who think that twitter, facebook, instagram, (& whatever else) are actual sources of news. That's all they did. Now the whole free world is freaking out and Putin is sitting back, congratulating himself on creating such overblown uproars. With nothing but posts to social media. People, a monkey could probably be taught how to post to facebook. Certainly an intelligent parrot could. There's something called “discernment.” All of America -- definitely including what passes for actual media these days -- needs to learn how to use it.

This comment includes the false premise that users generally believe that they have a solid understanding of what (social) media is or what it does.

Discussion

This chapter showcases how the mobilization of polarized denialism of Russian trolling took place through whataboutism and by blaming political opponents. These are the political scapegoats who have been most frequently invoked to deny the existence of Russian trolling in the analyzed news comments: Democrats, Hillary Clinton, and Barack Obama (on *Breitbart*/Gab); Hillary Clinton and Donald Trump (whataboutist references, typically on

the *New York Times*); and the opposition party that criticizes Putin's Russia (typically on Delfi.lt).

Since whataboutism was identified across news comments and media platforms, it can be concluded that it is one of the most popular rhetorical features. Whataboutism, in such instances, produces false equivalencies—in this specific case, between the US and Russia. This false equivalency implies that because trolls have operated in the US, the object of public focus should not be Russian trolling. Moreover, whataboutism was found to exploit an affiliation tactic—by evoking something that is familiar and agreed upon by the receiver of the message—in this manner by casting partisan divide as whataboutism. Those arguments of affiliation tactic included attacks on democrats on Gab and *Breitbart* and attacks on republicans through the *New York Times*.

While numerous arguments, such as immigration or illegal voting concern “the cracks in the society” and are prone to partisan division while interpreting them, it can be concluded that such issues are actually invoked to divert public attention from Russian trolling. Furthermore, the use of divisive issues to divert attention from Russian trolling could further divide the publics to mobilize against such ideologically charged issues. Such a divisive and fear-instilling rhetoric toward illegality of immigrants has been found to dominate right-leaning media as by Fox News, as noted by Benkler et al., (2018). The same rhetoric was found in examples of this book on *Breitbart* to divert attention from Russian trolling and potentially appeal to these audiences to be sympathetic toward Russian trolls.

In fact, comments used othering and scapegoating as the rhetorical tactics involved in conspiracy theory formulation and deployment, and these are not new rhetorical devices. Even if the ancient nature of such rhetorical maneuvers does not justify their existence, they can be traced to the documents written in Latin. Interestingly, in Roman antiquity, public scapegoats were foreigners, women, or slaves (Pagán, 2012). Thus, conspiracy theories became embedded within the mythologies that were circulated as forms of social control. In other words, when uncertainty prevails, conjecture becomes compelling.

Similarly, blaming can be attributed to what Davis (2020) called *anti-public* discourse. Davis (2020) described antipublic discourse as “a specific ideological form, linked to a particular moment in political and media history” (p. 9). He distinguished the following six what he called “thematic continuities” of the antipublic discourse: selective lack of rationality; antagonistic and divisive discourse that is typically based on rage, othering, anti-Semitic, anti-immigration, antirights, antiexpert, and anti-institutions; anti-

elite and anti-Hollywood; antistatist (freedom from formal and informal); antic cosmopolitanism (fear of global identity protection of the national or local); and conspiracy driven. However, while these themes are evident in this study, they are instrumentalized to achieve one single goal—to justify Russian trolling. All of these arguments served to state that “Russian trolling” did not happen.

Today’s manic fixation on partisan issues is increasingly justified as a legitimately concerned political attitude on the part of public. Yet it is actually the effect and the exercise of widespread rhetorical strategies intended to divert public focus from the urgent problem such as Russian trolling to other issues. The issues toward which focus is diverted tap on previously established affiliations by appealing to reader’s values and emotions, such as hatred, by inviting them to take sides. In such an instance, a message that includes an appeal to hatred of political opponents could render compelling any ensuing presentation of truth from that same discursive source to seek unexpected affiliations, such as described earlier in the historical propaganda examples proposed by Herf (2009). Denial of Russian trolling can serve within the repertoire of such truths. Thus, the call to affiliation becomes a persuasive rhetorical strategy, especially when combined with denial. By itself, it is just opposition, in conjunction with Russian troll denial, or when used as a juxtaposition, it becomes a tactic.

Summary

Influence and persuasion in Russian trolling justification resemble classical propaganda techniques that shift attention from the main issue—here, from Russian trolling to something else. To enable an understanding of how influence spreads through online news story comments, this chapter has aimed at connecting propaganda of the past with the forms of influence of today. This connection enables, at the very least, a partial delineation of the contours of information warfare. Such delineation, in turn, shows how propaganda corresponds to a fragment within a larger information warfare mosaic. All fragments combined, the complete picture of information warfare emerges—and specifically through the frameworks discussed earlier. First, communication theories of persuasion address the perceived elements of influence and how they take place in face-to-face contexts. Such discussions help to explain how the internet continues to incorporate elements of mass communication.

Second, the concept of propaganda is invoked through a survey of clas-

sical propaganda models from World War II and responses to propaganda in the US media. This chapter documented how previous studies have fruitfully crystallized the concept of influence within the context of propaganda. This chapter has contributed to such studies, first, by contextualizing influence within the propaganda models that had been constructed through elements identified in historicized accounts of foreign influence. The chapter's objective was to outline microelements that pertain to the models of influence and apply to them in historical context-specific (social) media ecosystem. However, because the mechanisms covered throughout this chapter relate, overall, to strategies of influence, sample news story comments serve to exemplify how influence can be embedded in messages. Finally, computational propaganda in this chapter was presented as a lens that facilitates the visibility of online influence.

The third point includes influence frames, for the example, the use of conspiracy theories, a crucial tactic within the Soviet propaganda playbook. Conspiracies become weapons that target “the gullible,” or those individuals otherized by commenters on both sides of sociopolitical divides. The trope of “the gullible” is based on a third-person rhetorical construct that posits “others” as the ones who are susceptible to influence (“not I” or “not us”). And that susceptibility pertains not only to beliefs promoted through the discursive medium of Russian trolling but also through the multitude of conspiracy theories.

The gullibility frame found in the comments confirms O'Shaughnessy's (2019) argument that disinformation comprises two facets: not only other manipulation but also self-manipulation. Message writers typically positioned themselves as immune to gullibility and attributed that quality to others. Such attribution, followed by othering projection, is known as the third-person effect (see, e.g., Jang & Kim, 2018). O'Shaughnessy (2019), however, argued against the idea of gullibility by stating that the victims are not naïve; on the contrary, being gullible is an indicator of a co-conspiracy with their perpetrator to join what he calls as a shared fantasy. Susceptibility to false information, even if projected through the third-person effects, is part of the current media landscape, and news portal comments are not an exception.

There are at least two takeaways from these early models of communication persuasion and from more recent persuasion accounts of Russian influence in the 2016 US presidential election. First, interpersonal settings for persuasion take place not only through traditional mass communication sites such as television or newspapers or radio but also in their social media counterparts and user-generated content spaces. Second, despite such relo-

cation of influence to user-generation spaces, previously identified mechanisms can provide a clearer rationale for the continuing relevance of message framing and the use of mass media influence at specific times.

While previously described communication persuasion and propaganda models have been known to scholars since the first analyses of mass media, new elements deriving from the creation of online spaces have emerged more recently. These elements include the concepts of contagion (the ability to expose new users to content), automation, and anonymity in user-generated content diffusion. Online news portals accommodate all three concepts. Yet rhetorical moves tap into classical propaganda techniques.

Even if computational propaganda is deeply rooted in historical propaganda techniques, it remains a communicative practice, vested in rhetorical moves, that is mediated through online spaces. The computational element is identifiable in the use of algorithms, automation, and human curating. At the same time, the propaganda element refers to the communicative means, frames, or discourse types that influence public opinion. Thus, the term “computational propaganda” encapsulates the concepts of digital misinformation and manipulation. Woolley and Howard (2018) further expanded these concepts to include what they called dubious political practices, such as astroturfing, state-sponsored trolling, and new forms of online warfare that influence social attitudes and behaviors. Such inclusion implies that there is a proposed purposeful tactic for managing and distributing misleading information through social media networks.

Additionally, Woolley and Howard (2018) claimed that the computational part of computational propaganda qualifies earlier notions of propaganda. Thus, computational propaganda departs from the established origins of propaganda within communications studies and is applicable to the current media landscape that involves new technological configurations of content distribution and of such content’s production forms. Thus, computational propaganda is not an isolated phenomenon; it is a worldwide phenomenon—one that transcends geopolitical borders.

Automation and anonymity function in conjunction with information the echo chambers online that currently define information consumption online (Garrett, 2009). Information bubbles entail that users consume information that is similar to their belief systems. And information bubbles can be amplified online, like ideologies in online spaces that acquire prominence, as arguments that justify Russian trolling. And when the argument gains prominence, online it can be exponentially amplified. Thus, it can be said that ideologies have moved to online spaces.

Fuchs (2018) distinguished between ideologies *of* the internet, ideolo-

gies *on* the internet. It is the latter that creates a difference in how information circulates. Furthermore, there are algorithmic implications to online ideologies. Algorithmic implications particularly pertain to amplification. Such a tailored algorithmic amplification can be determining to sway positions one way or the other. For example, circulated information can gain online traction through persistent reuse across multiple media sites. As this study has shown, Russian trolling denial frames exemplify such information circulation.

Exposure to online content can provide positive effect—in cases when users access additional information to augment or validate their knowledge. But in information infiltration scenarios, such exposure is designed to disrupt the core ideas without leaving space for debate, with a goal of destabilizing the online public sphere. Thus, contagion is the mechanism by which online users become carriers of infiltrated content. Typically, such content is hard to verify, and it is not based on *logos* but *pathos*—that is, it is emotionally charged content. The widespread circulation of such information threatens with consequences such as sociopolitical polarization and online chaos.

Knowing this, today's propagandists can exploit the concept of contagion to advance their agendas. Thus, within the contagion model context, the dissemination of information depends on networks, and their involvement with the content at stake. In such a scenario, audiences become the amplifier (Wanless & Berk, 2019).

At this point, the questions arise: What can we learn from early propaganda models? If we approach Russian trolling as a form of computational propaganda, what are some common denominators underlying both phenomena? To answer these questions, we first need to acknowledge that algorithms are used for political communication. Second, we need to consider, as Woolley and Howard (2018) put it, that these algorithms allow “small groups and actors to megaphone highly specific, and sometime abusive and false information into mainstream environments” (p. 7).

While recent scholarship showcases that computational propaganda is employed in many countries within their own borders to promote political ideologies, it has been found that Brazil, Taiwan, and Russia (all authoritarian or quasi-authoritarian regimes) do so with relatively greater frequency than others (Woolley & Howard, 2018). Specifically, Taiwan's subjection to influence from China distinguishes it from Russia and Brazil. And what distinguishes Russia from Taiwan and Brazil is its active engagement in computational propaganda practices that produce repercussions worldwide. Similarly, case studies prove that Russia had been a foreign actor in Poland's computational propaganda. Such studies also verify Russia's moderate

involvement in the US computational propaganda, and in Ukraine's, to an even more substantial degree (Woolley & Howard, 2018).

Similarly, online platforms through which influence takes place vary based on their sociotechnical factors, which can be useful in determining their reach and types of vulnerabilities for foreign influence. And each country has its own unique media ecosystem. In all instances, “media ecosystem” refers to the media that is adopted in particular ways by citizens, users, or audiences. The same audiences, users, and citizens can be exploited in the process of influence—a phenomenon known as participatory propaganda (Wanless & Berk, 2019). Participatory propaganda entails engaging of the audiences in creation and spreading messages that help propagandists to obfuscate its origins and increase receptivity of messaging. These types of behaviors allow for audiences to be “used” to make messaging to be more receptive. Thus, legitimate and illegitimate actors can coexist.

Similarly, media ecosystems can be employed for such participatory propaganda based on their levels of adoption by a given population. As a result, analysis of news portals attempts to provide some tangible criteria for uncovering signs of Russian trolling in user-generated content. The analyzed cases of media ecosystems differ in their media ecology: for example, the US leads with 9% of its population using Twitter in 2021, while Lithuania trails at 3% (“Global Stats, Lithuania,” n.d.). By contrast, Instagram and YouTube have high penetration in Lithuania, at 17% and 7.5%, respectively, while in the US, Instagram has 3% penetration and YouTube, 1.6%. Facebook use is high in Lithuania, with 63% of penetration, and in the US (72%) (“Global Stats, USA,” n.d.). These contrasting percentages indicate that Twitter and Facebook are used for not only interpersonal communication purposes but also for political ones. As a result, influence can be expected to be more impactful, when devised for media platforms that are more prolific for a given sociotechnical context.

As countries differ in social media use for political deliberation, so they do with news portals and user comment spaces. Furthermore, platforms such as Twitter are not very popular for political communication in Lithuania. For example, according to a 2009 study that surveyed social networking sites for political communication, Twitter was not mentioned even once as a platform for political communication, as argued by, for example, Šuminas (2009), while Facebook was found to be the primary communication medium for Lithuanian political parties, which are officially represented through web page content.

The findings of this chapter consolidate this book's premise—the existence of computational propaganda is a fact, and Russia is an important

global player. Some critical takeaways about computational propaganda are the following: The automation level of online spaces and the coordination level at which automated accounts (or bots) operate. The latter ranges from sleeping accounts to active bots that operate in online spaces. Thus, the presence of multiple coordinated actors corroborates the treatment of online spaces as information warfare's automated control sites, where accounts are mined and ready to be appropriated when the right time arrives for an offensive strike. As noted earlier, such online attacks can involve the creation of levels of disbelief. These, in turn, can generate the confusion that escalates into online chaos.

Instilling Mistrust in Institutions

Gab Example 1

We have Mueller indicting imaginary Russian Trolls, Nancy Pelosi saying the grass should be mowed in AZ along the boarder, as a security measure, incase Mexicans are hiding in it! Put this in a book, no one would publish it they would think you insane.

In the comment above, Russian troll denial frame suggests that Russian trolls are merely figments of Robert Mueller's imagination. The author of this Gab post attempts to persuade readers that US Department of Justice Special Counsel Robert Mueller has indicted "imaginary" Russian trolls. While invalidation of the Mueller investigation underlies this persuasion attempt, the very existence of Russian trolls is questioned through the statement that no book on the topic stands a chance of being published. Such rhetorical attempts exemplify this chapter's main subject: How online comments retaliated against media and government institutions (by challenging their credibility) that scrutinized and covered stories on Russian trolling.

This chapter examines conditions that contextualize inauthentic participation online that leads to chaos. Specifically, it details how media institutions have been facing continuous attacks and those attacks were used to deflect attention from Russian trolling. Such trivialization of Russian trolling, while attacking news media as institutions, has been identified in all analyzed media sources comments, exemplified by attempts to undermine public trust. In addition, attacks in the analyzed comments were addressed against US government agencies such as the FBI, by criticizing for its involve-

ment in Russian trolling investigations. This chapter's goal is to introduce how reputable news media institutions, despite following the best practices to foster democratic debate online, have become targets of attacks to justify Russian trolling or divert attention from it.

To contextualize online news comments, it is critical to point out that print media have transformed in the past years and adapted to digital formats by moving online while retaining their print versions. Scholars have expressed continuous optimism for the role of technology and automation as ways to increase quality of the production of the print press of the future and even the potentials to leverage automation to enhance the quality (Diakopoulos, 2019). Through digitalization, as some scholars such as Usher (2014) noted, news organizations have changed. Similarly, news portals have embraced the emergence of the new values—immediacy, interactivity, and participation—that online platforms offer. News portals reflect such a trend by fostering an increasing engagement of their readership by soliciting comments to news stories. Such comments can be interpreted as a form of readers' participation in the sense making of the news or at least in response to news stories.

Yet with the emergence of inauthentic participation, news comments are paradoxical: On the one hand, they deliver a promise of a deliberative online participation. On the other hand, by the virtue of being open to anyone, they also represent a “weak link” that technologically allows for inauthentic participation to creep into online spaces even if unintentionally. Thus, this chapter discusses how, with the emergence of inauthentic participation, news comment sections can, to a certain degree, challenge the democratic principle underlying online discursive participation and debate and can be exploited by forces beyond democratic ideals. While the option to post comments exemplifies the democratic ideal of free speech (since any user can post), this option can also be exploited to advance agendas that are actually predetermined by specific stakeholders—possibly even foreign governments.

Because comments are written by users instead of professional journalists, news portal comments are less codified than the news stories to which they respond. By no means does this chapter argue for disabling news comments, as they are vital for the public sphere because they represent multiple voices and a potential for multiple points of view—based on ideals of the democratic public sphere. Instead, this chapter exposes challenges journalists today face with contentious phenomena, exemplified here through Russian trolling, and the attacks that have been launched to the news media organizations through the same news comment sections.

News comment exploitation for inauthentic participation has been con-

ceptualized through the lens of dark participation. Frischlich et al. (2018) described dark participation as “comments that transgress norms of politeness or honesty with partially sinister motives” (p. 1). This chapter argues for news comments and especially the attacks on media as institutions playing a critical role in breaches to democracy. When it comes to online participation, newspapers have to constantly adjust in relation to incorporating reader comments. And this balance has not been easy. Some newspapers function as fierce gatekeepers; others observe it more passively, as argued in the recent research on dark participation mentioned earlier; and others are leveraging artificial intelligence and machine-learning techniques to deal with dark participation.

This chapter documents how news media organizations and journalists have received numerous attacks in the commenting sections of the news portals, attacks focused on challenging the credibility and authority of traditional journalism. Specifically, considering the hostility expressed toward mainstream media, as demonstrated by recent research, for example by Ihlebaek and Holter (2021), this chapter starts with some of the contexts based on which online spaces can become preconditioned to unwillingly “hosting” Russian trolling, along with any other online participation. By doing so, this chapter discusses the conditions in which disinformation as chaos can be created in news portals by detailing conditions that have transformed news portals’ commenting section into information battlegrounds.

Living in Media

Deuze (2011) has insightfully observed that we are not living with media, but in media. This heightened sense of *being in* media reconfigures our ability to make sense of it. In other words, the more we are enmeshed in media, the more our ability to grasp the complexity of increasing information streams diminishes—even if our confidence in media savviness increases, as demonstrated by Allcott and Gentzkow (2017). In their study on the 2016 US presidential election, Allcott and Gentzkow (2017) revealed that 14% of Americans considered social media their most important source of information. Yet, false stories about presidential candidates were shared 38 million times (30 million favoring Donald Trump and 8 million favoring Hillary Clinton). Remarkably, Americans were exposed at least with one fake news story. These statistics indicate an overconfidence in assessing online sources.

Conditions that have generated the vulnerability of online spaces to Russian trolling had been steadily evolving throughout the past decade. Such

vulnerability is, in part, attributable to the paradoxical situations in which media and information communication technologies had evolved. The first paradox involves the false perception of user empowerment through technology, related to the celebration of “you” phenomenon. Specifically, in 2006, *Time* magazine named “you” Person of the Year where the cover reads: “Yes, you. You control the information age. Welcome to your world” (Grossman, 2006). In short, the message is that “‘you’ inhabit the center of all media.” This message implies that general users, ordinary citizens, and online comment writers (all designated by “you”) are positioned to define information and to control it. It is, indeed, a very powerful and potentially self-transformative message for everyone in this information age. The front cover design for the 2006 issue of *Time* reinforces the message’s power: The word “you” is centered on a gray area that doubles as a computer screen and a reflective mirror surface. Thus, the subliminal message behind this design is that “you,” an ordinary person, has control over technology and information flows.

This message encourages the reassurance that ordinary people define online spaces, be it from the information infrastructure perspective or content—and that all online contributions are actually authentic, even if it is not entirely true. This assumption has been challenged on several grounds ever since the resurgence of automated and coordinated online behaviors through the information warfare and dark participation practices mentioned earlier. While now more than ever, all users can contribute to the content within online spaces, we, the ordinary people (i.e., who *Time* addresses as “you”), are less informed about how networks enable information flows—despite the fact that each of us has acquired a certain degree of familiarity with our own personal networks of information flows.

Moreover, our capacity to store and own our contributions online (in a form of posts or comments or video) is limited, let alone to access to other users’ data and network. Some exceptions to owning one’s data include some mobile platforms such as WhatsApp, which give users the option to download and store it. Even if there are visionary open data initiatives (for example, by the Open Data Institute (“About the ODI,” n.d.), at the current point, this is the exception, not the norm. Otherwise, online data are available (typically in formats that are not conducive to be saved) within the specific platform, owned by the platform, or for purchase.

Similarly, even when we had the technological means to look at other networks, it could be difficult to make sense of them. News portal comments illustrate this challenge—as readers of news portals’ comments, we typically look at each individual post at a certain time (e.g., when

we access it) rather than at a series of posts over an extended time. Nor is it easy to access individual user's posts, since typically comments are not designed with such a purpose. Thus, we do not "get to know" these anonymous online writers through their posting over time. Our network experiences can be somewhat different on social media platforms, such as Twitter, where users who follow one another can gradually get to know one another through posts. On many platforms, however, users cannot easily access their own produced data points—let alone gain easy access to networks of data. Exceptions include user comments that are outsourced to third-party platforms such as Disqus that function as social networking sites and user-level posts are available, if a user is set as public. Yet such third-party platforms do not necessarily foster a sense of community for a given news portal or share their data.

Access to data becomes even more critical during times when new actors emerge into media spaces. Frequently, such actors become known for their vested interests. For example, media analyses of the 2016 US presidential election reveal that internet users have scrutinized concerted efforts to circulate information through advertisements or bot activities (Stromer-Galley, 2019). Yet the constant flow of messages—specifically, in social media, complicates the identification of the initial sender of a given message, let alone the rationale for sending it. Moreover, in the current media landscape, knowledge of larger-scale networks and message flows has acquired unprecedented importance. In other words, the use of online spaces through the observation of our own individual network had formerly sufficed. Today, however, the forces behind dark participation reconfigure our expectations about what we need to understand within the online world.

Nearly a decade and a half since the popularization of the "you" phenomenon, its repercussions have emerged through the paradox of dark participation. After all, the phrase itself is paradoxical because it implies that not all types of participation are equal. Furthermore, dark participation entails an orchestration of participation that we are facing in the current media landscape, and this is posited by the following excerpt from Massimo Calabresi's (2017) *Time* magazine story "Inside Russia's Social Media War on America": "Marrying a hundred years of expertise in influence operations to the new world of social media, Russia may finally have gained the ability it long sought but never fully achieved in the Cold War: to alter the course of events in the US by manipulating public opinion. The vast openness and anonymity of social media has cleared a dangerous new route for antidemocratic forces" (para. 4).

Here, Calabresi (2017) mentioned the unprecedented nature of Russian

influence in the US public sphere. He then cited Rand Waltzman, who led a major Pentagon research program enabling the identification of propaganda threats that social media technology posed: “Using these technologies, it is possible to undermine democratic government, and it’s becoming easier every day” (Calabresi, 2017, para. 4).

“Antidemocratic forces” and “undermine democratic government” are keyword clusters that can be singled out from these quotations to emphasize the new role of media institutions and news comments. Antidemocratic processes can take place not only through actual warfare, where military troops are deployed for combat in designated territories, but also through what Simons (2015) called soft influence. In other words, forms of soft influence (the online counterparts of military troops) are subliminal, algorithmic, and fully embedded within the contexts in which they appear. While such contexts can be social media sites, soft influence can also emerge as dark participation in news story comments.

Forms of soft influence are embedded in that they can resemble comments or opinions written by ordinary users. Of course, there is always the possibility that such messages are authored by actual human users, given that they can be further amplified by users for whom they resonate—even if, only partially, and despite their function as the means of spreading conspiracy theories or rumors. Such rumors do not need to be real—in other words, verifiable, through factual debunking. Instead, it suffices if their recipients perceive them as real. Such contested truth illustrated here through the case of interference in the 2016 US presidential election—an issue discussed here within the context of dark participation. To account for dark participation in online news, as argued by Quandt (2018), the following sections conclude with the challenge of post-truth that create uncertainties not only for news comments interpretation but also for the treatment of news organizations.

Exploiting Post-Truth

Delfi.lt Example by Anonymous Users 1

Headline: kremlin trolling.....

Comment: The current Russian propaganda differs from the one that has been used in the soviet times since it has adapted to the principles of the western liberal democracy. For example, Russia registers their own channels in the European Union countries and in them they project their own propagandistic positions as a ‘different opinion’ and the Western countries

see it as some kind of expression of the pluralistic opinions. The problem of the West is that, there is no truth and everyone just merely needs to have their own opinion.

This Delfi.lt comment answers the question: “How does Kremlin trolling work?” It suggests that there are certain vulnerabilities inherent in the democratic premises of the need to include and foster alternative viewpoints. Such vulnerabilities are exploited by Russian trolling. The primary objective of democratic deliberation is clarification through debate. Thus, as Zelizer (2004) put it eloquently, the goal of journalism is the presentation of problems rather than their solutions. Moreover, through news stories or exchanges with news readers, journalists can clarify issues, shed light on obscure speculations, and provide evidence and interpretation. However, regardless of the sense-making mechanisms that news readers are offered—be it framing or community journalism—all of them are geared toward clarifying issues.

Such striving for clarity has been challenged by the rise of what is called *fake news* over the past several years—a phenomenon that has revived questions concerning truth in the mass media—thus, the concept of truth is yet another condition that challenges news portals. Over the years, best practices in journalism were prescribed to safeguard the truthfulness of information to alert citizens about the most pressing issues. Thus, while journalistic practices have changed over time through adaptation to new communication information ecosystems, commitment to information’s truthfulness remains the primary ideal of the journalism profession. Despite such shifts to online platforms, news portals retain their original objectives: holding news reporters and writers to the highest standards of journalistic practice to inform readers about current events. After all, confirmed truthfulness—for example, through verified sources—has become a main cornerstone of democratic deliberation. Consequently, fact-checking has been proposed as a crucial means of combating fake news (e.g., “Factcheck, Factcheck: A project,” n.d.). After all, citizens have the right to access accurate information. Furthermore, they have the right to produce their own interpretations of that information.

Today’s journalists are also challenged with the threat of democratic subversion through information influence tactics that closely resemble those of propaganda. Because such influence models are based on information subversion in news portal comments, they elude fact-checking to a certain degree. Thus, they are more related to disinformation—a phenomenon that can, in turn, be related to what constitutes truth in the modern and post-modern worlds.

The transparency of journalistic practice has been considered yet

another cornerstone of democratic deliberation (Phillips, 2010). Consequently, journalists have focused on source verification as ways to achieve transparency. Yet the term “post-truth” entered dictionaries in 2015 directly before the US presidential election. Post-truth refers to circumstances where objective facts are less influential in shaping public opinion than appeals to emotions and to preexisting beliefs (Tsipursky, 2017). For example, Tsipursky (2017) argued that the concept of post-truth was exploited by Donald Trump’s 2016 presidential campaign and throughout his first year in office. Trump’s communications team caused multiple truths to morph into alternative facts within popular vocabularies. This communicative metamorphosis implies that facts and truths are far from synonymous and that news media facts are particularly susceptible to public skepticism. Such attitudes exemplify subversive postmodernist views of the truth and validate the inclusion of alternative practices, such as Russian trolling, within information ecosystems.

Russian trolling can be part of a broader discussion about who disseminates what types of information. Over the past several years, information sources for trolling have included discussions about fake news detection and resistance. “Fake news” is a label that can be used to degrade all categories of information. In fact, that label can be similarly attached to the misinformation spread by automated bots. Moreover, “fake news” also has become a convenient coinage used to interrogate the legitimacy of journalistic sources. Thus, the controversy about what constitutes fake news rages on. The arbitrary “fake news” label that depreciates journalistic sources can also discredit other legitimate sources even if they can serve to scrutinize bot-based or trolling behaviors.

However, even in the face of supporting evidence, truth remains contested, as described through the “fake news” accusations. The concepts of post-truth, fake news, and alternative facts are strongly related to the uncertainty about legitimate objects of belief or constructions of reality—or even the possibility that foreign governments use online commenting for agenda advancement, as detailed by Khaldarova and Pantti (2016) in their assessment of post-truth in the Ukrainian conflict coverage. Such uncertainty has also led to the interrogation of the bases of information communication technologies, and their affiliated institutions.

Thus, through the notion of “fake news” news organizations are facing heightened interrogation. In fact, such interrogation has intensified to the point that, in some instances, a pledge of truth has been drafted as an initiative where journalists can use their sources to profess their commitment to

tell the truth (“Protruth Pledge,” n.d.). This practice is problematic, since its default premise is that journalists are untruthful. It also implies such pledges of truth are necessary, while exemplifying how postmodernist definitions of truth have been interrogated.

Postmodernist treatment of truth complicates the treatment of all information, including comments in online news portals. Ideally, multiple truths should provide more clarity and certainty. In actuality, however, such multiplicity challenges facts and pushes the boundaries of human understanding. And such post-truth can be exploited for information warfare. The beginnings of the post-truth movement, which permits the coexistence of multiple and subjective individual claims to truth, are identifiable before it even affected the US around the time of the 2016 presidential election.

Yet the concept of post-truth was a discussion item for news organizations prior to that. For instance, in the UK media in 2015, the notion of post-truth had been linked to Russian propaganda techniques, as outlined in an editorial from the 2 March 2015 issue of *The Guardian*: “The idea that there are multiple interpretations of the truth has become the founding philosophy of state disinformation in Putin’s Russia” (*The Guardian* Editorial, para. 2).” *The Guardian* describes, however briefly, the interrelation of propaganda techniques and the exploitative, obfuscating aspects of post-truth. Even so, it can still be argued that a lens for interpreting post-truth is merely being offered. In fact, other scholars (e.g., Heinrich & Pleines, 2018; Pomerantsev, 2014; Roudakova, 2017), have identified the concept of post-truth within the extant repertoire of classical propaganda techniques.

There is a list of dangers to media ecosystems presented by post-truth. Post-truth positioned as alternative interpretation of controversial or ideological events serve to instilling cynicism. Cynicism, instilled particularly by the alt-right media, or what Rae (2020) urged us to call hyperpartisan media, has been found to be detrimental to the media institutions and their credibility. And, for example, there is increasing evidence showing that alt-right media sources push boundaries of the post-truth (Rae, 2020).

Dangers and mechanics of post-truth as the discursive cornerstone for justifying authoritarian regimes have been also exposed by scholars like Pomerantsev (2014). Similarly, Roudakova (2017) specified how post-truth originated in an overarching Soviet propaganda model. Thus, by situating it within authoritarian contexts, she advanced her argument that, in the former Soviet Union, even though citizens could have distrusted media content, they still upheld high modernist notions of the truth—in other words, that the truth existed and was determinable, even if media, such as newspapers, were prohibited from exposing it. Consequently, the public learned to

read between the lines of newsprint, knowing that there were always variations of the truth—those that were unavoidably visible in their daily lives.

Roudakova (2017) also argued that authoritarian regimes, such as Vladimir Putin's Russia, manipulated the notion of truth as ways to silence their critics. The rationale behind such attacks can be formulated thus: "If there is more than one version of the truth, then, who is to say your version is better than mine?" Such rhetoric exemplifies the whataboutism discussed earlier. Whataboutism invariably presents alternate explanations, or counterarguments, that generate false equivalencies in response to previously stated claims. In addition to whataboutism, Kalpokas (2019) argued that post-truth is enabled through mediatization and affect.

The debilitating effects of post-truth have been attributed to politics as well. Categorized as post-truth politics, it typically represents American conservative ways to defend established status quo, as argued by Andrejevic (2013). In other words, postmodernism is useful only if it can augment our understanding. Postmodernism has been exploited to create more uncertainty or to craft influence by provoking oppositional thinking. Uncertainty is created by diverting attention from a given issue when multiple truths are invoked through whataboutism, discussed in Chapter 2. Such a rhetorical maneuver can prevent the augmentation of understanding about an issue that was originally the main focus of attention.

Moreover, endorsement of postmodernist multiplicity of viewpoints can complicate understanding of everyday life facts. Because some aspects of postmodernism are historically rooted, they can provide elements of plausible truth. More specifically, postmodernism can appropriate the ideological premises of various belief systems to produce a confusing theoretical synthesis. Thus, the post-truth paradigm of postmodernism creates challenges for news interpretation. Yet the postmodernist philosophy paradoxically challenges the very assumptions about reality that it contextualizes. In sum, because multiple realities are acceptable in the postmodernist world, postmodernism challenges our understanding of truth.

Comments as Forms of News Deliberations

Having specified that the first of these paradoxes involves the "you" phenomenon and that the second relates to dark participation, and the consequences of post-truth, the third is based on a set of preconditions. When the democratic deliberations are a priority, news portals strive to intentionally implement technological affordances that foster such a democratic debate. Thus, given such objectives, the news portals, selected for this analysis,

among numerous other news organizations worldwide, adhere to a mission that encourages sense making of the news stories by their readers in the commenting section. While news portals share many similar features, there is a certain amount of variation in their approaches to soliciting user participation. Thus, it can be said that all analyzed news portals in this book endorse the same principles of democratic deliberation through their commenting affordances—and whether their respective political leanings tend toward the right or to the left. Such principles include the sociotechnical means that enable and provide online spaces to encourage the discursive involvement of all citizens—spaces where they can freely process and interpret news stories. On the one hand, the challenges of online deliberation limit the control that news portals can exercise over the content of reader comments. On the other hand, they do retain a certain level of sociotechnical control over such content.

The first thing to consider is that news portals take online participation seriously. They create and reinforce rules for participation from the outset and specify what constitutes meaningful user participation. Each of the analyzed online portals here outlined participation values in its guidelines. For instance, the *New York Times* specified these guidelines: “We are interested in articulate, well-informed remarks that are relevant to the article. We welcome your advice, your criticism and your unique insights into the issues of the day. To be approved for publication, your comments should be civil and avoid name-calling. Our standards for taste are reflected in the articles we publish in the newspaper and on *The New York Times*; we expect your comments to follow that example. A few things we won’t tolerate: personal attacks, obscenity, vulgarity, profanity (including expletives and letters followed by dashes), commercial promotion, impersonations, incoherence and SHOUTING” (“New York Times Home, Comments,” n.d., para. 1, 2). These guidelines emphasized the focus on “on-topic” comments and their perceived relevance to a given discussion.

As for Delfi.lt, not only were text boxes provided for user commenting, so were guidelines on what constitutes participation. Thus, even if readers do not read the actual fine print for the guidelines in other Delfi.lt spaces, they pop up each time they create a new post in the designated text boxes. The Delfi.lt comment box example includes the following text:

Write your opinion. Connect via Delfi.lt, Facebook, Twitter, Google+, Yahoo or create an account here.

[Box for a comment] Post your opinion. You agree with the rules. [Post button.]

As this Delfi.lt comment box illustrates, users see the following invitation: “Write your opinion.” To enable them to do that, they are invited to register through social media logins of their choice. These include Delfi itself, Delfi.lt, Facebook, Twitter, Google, or Yahoo, even if most users post comments anonymously. By clicking onto the hyperlink, they can access participation rules. Delfi.lt’s discussion system allows for readers to express their opinions regarding any of the news stories. Readers can also add information, share ideas with like-minded readers, or simply disagree with others in a confidential way. However, Delfi.lt displays the IP address of authors (“Delfi.lt Apie,” n.d.).

Similarly, *Breitbart* provides a link to their user participation rules within commenting boxes and the following text in the commenting box:

Number of comments Breitbart News Network Login
 Recommend Tweet Share Sort by Newest/Oldest
 Join the discussion [write a comment]
 Login with Disqus, Facebook, Twitter, Google+ or sign up with Disqus
 [name]

The link for *Breitbart’s* terms and conditions leads directly to a new page where user participation rules are outlined in a nine-page document. These include their policies on incivility and bot-based activities (Breitbart, 2020). Specifically, *Breitbart* explicates the legal rights of the commenting:

You agree not to provide User Content that: Infringes on, misappropriates or otherwise violates the copyright, trademark, patent or other intellectual property right of any person; Is false, misleading, libelous, slanderous, defamatory, obscene, abusive, hateful, or sexually-explicit; Violates a person’s right to privacy or publicity; Contains advertising or a solicitation of any kind; Degrades others on the basis of gender, race, class, ethnicity, national origin, religion, sexual preference, orientation or identity, disability, or other classification; Contains epithets or other language or material intended to intimidate or to incite violence; Or violates any applicable local, state, national, or international law, or advocates illegal activity (Breitbart Terms of Use, n.d., para. 11).

As for Gab (2020), the site described itself as “Welcome to Gab.com: a social network that champions free speech, individual liberty and the free flow of information online. All are welcome” (para. 1). The Gab website also specifies terms and conditions that include the legal aspects of posting. For

instance, Gab stated: “The Company reserves the right to take any action with respect to any User Contribution that we deem necessary or appropriate in our sole discretion” (“Gab. Gab AI INC,” n.d., para. 8).

Even if news portals clamp down on user discussions about controversial issues, they provide users with the option to engage with such content through the traditional letters to the editor, as exemplified in the following *New York Times* section that has been closed to commenting: “The comments section is closed. To submit a letter to the editor for publication, write letters@nytimes.com.”

As discernible from these four platforms, all users are invited to participate in online discussions within designated parameters. Nevertheless, based on platforms selected for such participation, news portals will determine content engagement levels for users. For instance, news portals can decide to include text-based reactions (e.g., comments, responses). Otherwise, they can favor visual icon-based ones (e.g., a thumbs-up symbol for “likes,” thumbs-down for “dislikes,” other emoji). Similarly, Delfi.lt includes user IP addresses, in addition to or in lieu of other forms of authentication. Finally, the institutional practices of news portals can determine the extent to which user information they will collect. While some news portals permit anonymous posting, others do not. Moreover, while some include third-party posting (e.g., via social media platforms), others, such as *Breitbart*, outsource commenting to a third-party platform (e.g., Disqus).

Other news portal practices address policies on user comment archiving. While some news portals archive stories for an unlimited time, they can also limit user access to comments (e.g., up to one month on Delfi.lt). Others do not place such limits (e.g., *Breitbart*, *New York Times*). Procedures for reporting message posting times also vary among news portals. For example, while some include the chronological time reference (e.g., 12 April 2018), others use the chronologically reversed time (e.g., 5 minutes ago).

Even if all the discussed portals solicit comments, subsequent sections of this chapter specify the challenges that news portals face with the current participatory readership that can comment and be part of the news deliberation. These address the price of being open and inclusive in the turbulent era of dark participation.

News Portal Comments as Information Warfare Zones

At this point, we might ask, What is trolling within the context of influence, and why is it relevant for analyzing comments? To address this question, it is relevant to contextualize how information circulates. Typically, news

portals host stories and articles written by professional journalists, and these undergo an established editorial process. Because the editor in chief retains the final stamp of approval for all journalistic content, predetermined editorial practices strictly regulate news portal spaces. By contrast, news story comments posted by users are rather uncoded. As specified earlier, because anybody can write and post these comments, they are neither edited for style nor filtered for content (there are exceptions to that, detailed later in the chapter, such as community-based flagging that can lead the content to be removed or AI-based tools that allow to flag comments that do not adhere to the norms detailed by the specific platform).

Not only content of the comments is not a strictly codified practice, but the structure of the comment is also not limited by platforms, either. The structure, such as the length of the post, can vary significantly, in contrast to some platforms that limit posts' length (e.g., Twitter has a limited post length). When it comes to the "genre" expectations of comments, while it is generally expected that comments should be somehow related to the news story or article to which they are allegedly responding, as explicitly urged by the *New York Times* to its commenters, as pointed out earlier, they can, at times, defy such expectations.

There are at least two main paradoxical ways in which news portals can be treated. As noted earlier, the first of these pertains to the deliberative premises underlying user comments. One such premise relates to the ideal of democratic deliberation that is based on Habermas's (2010) equation of online spaces with public spheres where discussions can be fostered. Habermas (2010) posited the need for a public sphere for interpreting news. More recently, this concept of a public sphere has been expanded to include online spaces. Specifically, designated comment fields within news portals encourage users to express their opinions about social or political issues. Thus, they are also invited to participate in the complex processes of news story interpretation through a mutual exchange of comments.

The democratic premises underlying such comments are central to this overall discursive process that enables users with varying perspectives to convene online. Ideally, the convergence of ideas encourages them to achieve clarity about issues. This clarity is expected to be achieved through the sharing of ideas (even if contrasting ones) and discussion. Thus, the ideal of democratic deliberation is based upon the convergence of ideas, as well as the shared sense of online community among users. And the precondition for the success of such deliberation is the receptiveness to alternate viewpoints or to unique counterarguments (Degli Carpini et al., 2004).

For decades, mass media, such as newspapers and TV, was treated as the

sole bastion of legitimate truth. Since the primary function of these mass media forms was informative, newspaper readers and TV news viewers alike, are stimulated to ponder what they had read or viewed to make sense of the world's ongoing events. In fact, journalists themselves contribute to that sense-making process. Journalistic practices include content coverage that enables news readers and viewers to receive synthesized information. In election coverage, for instance, frames have been solidified over time, and they become familiar and reintroduced in each new election cycle. Thus, framing has been a preferred sense-making mechanism when delivering information to media audiences.

Blumler and Gurevitch (2002) illustrated how mass media plays a critical role in sustaining democratic expectations by listing eight ways in which media enables democratic deliberation that are geared to provide clarity: "Reports of developments that impinge the welfare of citizens; Meaningful agenda setting, identifying key issues of the day, including forces that have formed and may resolve them; Platforms for advocacy by politicians and interest groups; Dialogue across a diverse range of views, as well as between power holders; Mechanisms for holding officials accountable; Incentives for citizens to learn choose and become involved; A principled resistance to the efforts of forces outside the media to subvert their independence, integrity, and ability to serve the audience; A sense of respect for the audience members" (pp. 25–26).

While the objective of this list is to highlight main ideas, the authors also discussed journalism and its various aspects to address the responsibilities of news media. These included contribution toward the collective efforts to sustain democracy. News organizations are invested in this particular responsibility because they use a mass medium to distribute information. In fact, news has evolved within democratic contexts to fulfill the public craving for information and to clarify for citizens their civil rights and voting choices. Thus, news serves a role of a purveyor of information. Moreover, news is a crucial journalistic practice that encourages analyses of available information to enable democratic deliberation.

However, what happens when specific interpretative frames are perpetuated through user-generated content, such as news comments written by the general public? News portals face vulnerabilities through online comments. One of these, as mentioned earlier, is the possibility that attempts to realize the democratic deliberation ideal could backfire. Specifically, indiscriminate news story comment solicitations render news portals vulnerable targets for the agents of dark participation. In other words, in instances where user participation is accessible to anyone, online spaces can become targets for

subversive agents that intend to exercise influence. These can be automated bots created by foreign governments. Thus, authentic user participation can be infiltrated by orchestrated disinformation campaigns that push specific agendas. In such instances, messages that contain specific inauthentic affective narratives can be distributed from a centralized apparatus and be mistaken for authentic user comments. Upon entering news portals, they are read and eventually redistributed—initiating the cycle of viral proliferation by authentic writers and readers of news stories.

This entire scenario involving news portals is further complicated by the fact that we live in postmodern times when truth is no longer an agreed-upon construct. Thus, the practice of questioning publicized truths has become a discursive trend where news outlets are concerned. For example, high-ranking government officials, such as former US president Donald Trump, have charged news organizations with manufacturing “fake news” (“BBC, How President,” 2018). This denigration of news as “fake” signifies diminished public trust in media organizations as credible institutions that are invested with discursive authority. Thus, disinformation can further exploit this mistrust to circulate rumors as legitimate alternative truths.

Consequently, there is a philosophical clash rooted in the inquiry of what constitutes “truth.” As mentioned earlier, truth can be positioned within the modernism-postmodernism polarity. These two contrasting philosophies can be invoked to explain the complexities involved in defining “truth” and generating a consensus for the term. Specifically, Habermasian deliberation is based on the premises of logic and consensus building. Because such premises are geared toward common understanding, they exemplify aspects of modernist philosophy. In short, the Habermasian deliberation ideal can be rearticulated as “the convergence of ideas.” The ideal of the participation in news commenting striving to bring multiple points of view can be subverted by non-genuine participation. Postmodernist approach, that invites multiple interpretations, and should enforce the idea of multiple voices online, paradoxically creates conditions for the subversion of truth. In other words, postmodernist philosophy is based on the idea that multiple outcomes and explanations are plausible. Thus, it rejects the assumption that there can be single and unified or binary and dualized outcomes and explanations. Divergence of ideas, then, becomes the outcome of postmodernist reasoning—the opposite of the convergence ideal underlying modernist philosophy. Thus, by adopting the premises of postmodernism that allow for greater complexity and encourage multiple interpretations of “the truth,” news story commenting sections can be exploited to seed confusion rather than optimized for providing clarity. As argued earlier, such maneuvers cre-

ate chaos online. Thus, the goal of next section is the discussion of aspects of these deliberative premises within the context of online news commenting.

Contexts That Situate Online Public Deliberation

I list several reasons that explain how and why news portal comments can be double-edged swords for deliberative democracy outlined so far: since they foster online deliberation but also can become ideological battlefields of influence, as seen in the Russia trolling phenomenon, with its masked and unmasked actors. I start with the underlying premise of this book that news portals' comments matter and deserve to be treated seriously, even if, at times, they are treated as "in the margins" or secondary to the news story itself. Yet I also argue that news portal comments can be vehicles for online influence through both Web 2.0 technology and communicative practices, where the diversity of viewpoints in news portal content can be subverted and vulnerable to manipulation.

2016 report on reader engagement with news comments, conducted in the US shows that 55% of Americans left a comment online, and 77% have read comments at some point (Stroud, Van Duyn, & Peacock, 2016). Thus, I start here by saying that online news comments matter. Journalism scholars have emphasized the promise of news comments not only to reflect diversity points of view provided to the story (e.g., Baden & Springer, 2014) but also to serve as a litmus test for the story's credibility (Naab et al., 2020). As journalism is under attacks, news portal comments are essential in mediating this role. Even if news comments typically do not provide praise for the coverage, it has been found that equally the tone of the comments can hurt the content of the news story by diminishing its credibility, as argued by Naab (2020).

Similarly, news portals comments as a type of online user-generated content can be viewed as secondary to the news stories, but with the potential of influence, or small things that matter, argued by Beyer et al. (2009). Barnes (2018) emphasized the interactional exchange value of the comments by stating that they remain the primary discursive modes through which "we engage with and react to each other in the online space" (p. 3). Her description is specifically applicable to news story comments. Reagle (2015) contended that while comments are a phenomenon at the margins of social media discourses, they are part of today's media ecosystem. Because such comments comprise only one aspect of an online media ecosystem, they are part of an online media ecosystem (e.g., news portal readership). Thus, they

go beyond a formal definition of comments, provided by Reagle (2015), as being reactive, asynchronous, and short.

Comments are also subjective, opinion based, and capable of expressing individual emotions—and those emotions can be constructed and manipulated. While scholars like Mansbridge (1999) have observed that online news portals represent “everyday political talk,” news portals can be vehicles for online influence. Also recognized as deliberative spaces, or as forums for interpersonal communication, they can provide arenas for mutual influence among news readers. At the same time, social media has become popular due to its convenience, which derives from accessibility and anonymity. Social media is, in fact, designed to encourage interpersonal exchanges and open up spaces for influence. Due to its network-based structure, it was initially perceived as a mode of self-presentation and resource sharing in community-like spaces. Consequently, online spaces now provide a new terrain for achieving this goal.

More recently, however, mass media, including news portals, have also started to incorporate social media to reach out to online content readers. Also, news portals provide a new space for deliberation—for sharing and exchanging ideas. Furthermore, with the rise of social media—based on two-way communication technologies (otherwise known as Web 2.0)—news story readers have been provided with new sense-making mechanisms, such as comments or third-party provider interactive platforms (e.g., Disqus). Such provision is partially because news portals and other media have moved online and started to include comments. By moving online, news portals have been required to adapt to new rules stipulating online interaction norms. Such adaptations include, as mentioned earlier, the task of determining which comments are to be included and to what extent.

Thus, while news cycles change rapidly online, readers enjoy the option of discussing news topics in greater detail. The drawback of this option, however, is that diverse viewpoints can be subverted by bots and other automated actors that are launched to infiltrate online commenting platforms. Such automated infiltration, in turn, promotes orchestrated opinion-shaping mechanisms (see more in Woolley & Howard, 2018). Engaged communities are critical for today’s healthy journalism, as argued by some of the leading scholars in the field, such as Wenzel (2020). However, what happens when online communities are utilized to manipulate affect? Affect has been found to weaponize online spaces by focusing on discourses of fear and anger noted as hostile “emotional regimes” present in online comments (Ihlebaek & Holter, 2021).

News organizations need to stay in constant vigilance about the online

spaces they provide for participation. Currently, they have to not only ensure values such as inclusion and diverse of points of view and civility but also handle foreign interference and manipulation. The idea of online comments as permeable spaces for subversion derives from the interrogated democratic ideals behind news commenting. Although news readers today perceive comments as crucial modes of information access, debates continue concerning the management of two-way interaction streams in mass media and the overall value of user-generated content as treated by mass media (see, e.g., Zelenkauskaitė, 2017).

In addition, another dilemma concerns the navigation between democratic premises to promote diverse points of view while incorporating news reader comments, given that the diverse points of view have been considered a gold standard for fostering the sense of the public sphere (Baden & Springer, 2017). Such comments preceded the internet—specifically, when they were published as letters to the editor. Publication of such letters to the editor predated the web, long before the emergence of online news, and those letters were selected for publication by the newspapers. It is not surprising that the democratic ethos of the inclusion of various opinions make scholars like Hart (2018) treat letters to the editor as representing civic hope, even if is driven by affect.

In fact, the ideal functions of online spaces for democratic processes have been outlined according to various perspectives. While one such perspective compares the web to a mirror, Bailard (2014) has a two-fold perspective about online spaces: that the internet provides users with a greater amount of information than would otherwise be accessible through traditional media. And, compared to traditional media, the internet provides users with more diverse types of information, and a wider range of perspectives for evaluating that information. Thus, the internet, based on these views, enables the inclusion of more voices at any one time and in response to a specific news story.

Yet online spaces, including news portals, are viewable as extensions of traditional mass media—ones that are endowed with specific medium-driven advantages. Thus, the rise of social media and the interconnected web provides new opportunities for news portals to achieve the goal of fostering diverse viewpoints in democratic contexts. Scholars have, in fact, applauded social networking sites for civic engagement, thus encouraging hopes that such idealistic treatment of online spaces would enable the achievement of democracy's deliberative goals (e.g., Gil de Zúñiga et al., 2010). Yet it is evident that within the current media landscape, online spaces can rapidly degenerate from forums intended for deliberation to those that are actually nondeliberative and divisive (Boutyline & Willer, 2017). Thus, in many

instances, online spaces have been reduced to political echo chambers (Garrett, 2009) or mere propagators of information—a situation that reifies the comparison of the web to a mirror or the physical world divided into cliques of opinions.

Within the context of online comment subversion, the forces of influence are far more important than the homogenization of opinions through user interactions (or lack thereof) involving diverse viewpoints. Some of it has been further attributed to a technologically-driven arguments such as filter bubbles. For filter bubbles to occur, the algorithms further take agency of online content distribution, thus shifting the power from an individual to technology. Instead, these technology-mediated algorithms create filter bubbles, even if filter bubbles can be viewed as rather reductionist, as argued by scholars like Bruns (2019).

Yet if it is not about the algorithmic agency, the question that remains unanswered is this: How can dark participation be exploited? How can the vulnerabilities to such participation in online news be exposed? More specifically, how is dark participation exploited for political polarization? And, how are online spaces exploited by foreign governments that attempt to sway public opinion? While governments might vociferously deny charges of interference, they can provoke suspicion through the traces they leave behind in online spaces—regardless of the verifiability of such charges. Moreover, while it is crucial to acknowledge the bases of interference, it is equally important to consider the formative role of public perception about it. Such perception can evolve through online news portal comments and shapes the realities within user mindscapes.

To conclude, while online news comments are important for public deliberation, they are not immune to manipulation and dark participation. While online news portals can function as hidden spaces, since they are not always immediately displayed for the reader, they are locally grounded and constantly updated, together with the news cycles that they are part of. Thus, due to such fluctuations, influence in news portals can be hidden in continuous streams of fluctuating user-generated content.

Discrediting Media as an Institution

Gab Example 2

We wouldn't have to rely so much on RT streams if Western media bothered to turn up and provide reporting on the ground. PS there's a shit loads of periscopes from protesters to watch if you're scared of nasty Russian trolls.

This comment celebrates *Russia Today* as a news source over the “Western” media. By doing so, it legitimizes *Russia Today* (RT), a state-sponsored Russian news source, at the same time that it degrades Western media and compares protesters with Russian trolls, thus creating false equivalencies. While news portal comment spaces offer platforms for all user voices, paradoxically, when Russian trolling is uncovered, the same platforms that give voices to their readers have been attacked. Specifically, arguments that are geared to discredit media institutions have been identified across analyzed news portals. Such arguments shift blame from Russian trolls to the media institutions that authorize coverage of the phenomenon.

The following comments exemplify the exploitation of the post-truth era to attack news media institutions. Such attacks that have been identified across analyzed news story comments accuse media institutions of circulating fake news.

Breitbart Story 7, Example 1

NY Times is Fake News.

Another comment elaborated on the attacks on mainstream media as follows:

Breitbart Story 9, Example 1

So true, the mainstream media, ABC, CBS, NBC, MSNBC, *The New York Times*, WAPO and their websites post fake, phony, lies everyday through their spoken words and web articles and then allow the Soros paid trolls to comment on said articles.....and it has been ongoing for years.....WHERE IS THE INDICTMENT? The Mueller Special counsel in nothing more than a witch hunt smoke screen to deflect attention away from criminals Hillary and Obama and their nefarious activities of the past 5 years.

Thus, the *Breitbart* user attacks primarily left-leaning media. Yet other users imply that such attacks can provoke discord, and destabilize democracy.

Breitbart Story 9, Example 2

Where do Media Matter trolls fall into all of this? They also tried to sow discord.

Even so, other news readers criticized journalists for failing to cover issues adequately.

Similarly, another user insinuated that it was not Russian trolls, but news organizations should be indicted, thus, attacking news media sources:

Breitbart Story 8, Example 2

Using this line of ‘reasoning’, WHERE ARE THE INDICTMENTS/
CRIMINAL CHARGES against CNN, ABC, CBS, NBC, The New York
Times, The Washington Post, et. al?

Other users insisted that the existence of Russian trolling is a lesser concern than its inadequate coverage by the *New York Times*.

New York Times Story 5, Example 1



America September 20, 2018

Reading this piece, and the Times over the past two years, I wonder if it will ever be able to recover from this debacle. Reporting like this is so extraordinarily myopic and gullible, trying so hard to exaggerate Russian trolling efforts, trying even harder to whitewash federal and Democrat wrongdoing. How can you do a piece on election malfeasance and not mention Steele one time? Strzok only mentioned once, in reference to being a target of Sean Hannity rather than multiple federal investigations. My only question at this point is whether they’re really this gullible, or they’re actually complicit to some extent.

Other readers criticize the commercialization of news.

New York Times Story 6, Example 1

London

Nov. 13

@ Spot on! I guess when US news is corporate controlled partisan entertainment, the ratings are in the fake news and results of it are the dividend - control.

And, yet, other readers in their comments blame institutions by implying that the *New York Times* is a propaganda machine rather than addressing the issue of Russian trolls.

New York Times Story 6, Example 2

██████████

Nov. 13

Of course *The New York Times* played a significant part in this campaign, willfully or not who knows. One could argue that *The New York Times* is still playing a part in this disinformation campaign along with most of the US media.

While the right-leaning media could be partially responsible for social tensions in the US, some *New York Times* users invoke it to justify Russian trolls existence:

New York Times Story 7, Example 1

████████████████████

Feb. 21, 2018

Relentless repetition of “Hillary is a corrupt liar,” with no details except lies could most certainly have turned the election. On a national TV focus group, a woman showed she actually believed the Planet Ping Pong libel. To be ‘sure’ Russian trolling did not turn the election is to be in deep denial of the effectiveness of propaganda, underpinned by decades of right-wing hate radio, TV, and websites.

Other users assert the need to restore journalistic integrity in news reporting and to hold media institutions to higher standards of responsibility.

New York Times Story 6, Example 3

████████████████████

Montreal, Canada Nov. 13

Excellent series. Bravo.

When can we expect a series on how mainstream media has become a propaganda tool of past and present administrations? The build-up to the Iraq War is a fine example of what I mean. How about a few honest accounts of the trials and tribulations of Palestinians? Ask any American today, why exactly Iran is an enemy of the US and you’re sure to find a lot of blank faces and a litany of the usual anti-islamic clap trap as a rationale. When will journalists delve deeper into this propaganda? And I don’t mean op-ed contributors that are influenced by a need to safeguard Israel.

Many readers here will poo-poo Fox ‘News’—justifiably so—as propaganda tools of the Republican Party. Are there not similar arguments to be made

about the Times or NBC? We need a return of newspapers and TV news as disseminators of information rather than entertainment & profit generating enterprises. Whatever happened to media companies making money from 75% of their divisions and agreeing to break even with the News media in order to stay unbiased? Doing so was once seen as a necessary component of the American democracy.

My point - which might be awkwardly advanced - is that we need a return of quality investigative journalism. We need less 'opinion' pieces, particularly on TV. We need a few trusted media sources that will refuse to be adherents of one political side or the other.

Yet another user criticizes right-leaning media (e.g., Fox News) as responsible for social problems in the US:

New York Times Story 7, Example 2

██████████ Feb. 21, 2018

The blow did not come from Russian trolls. The blow came from 25 years of Rush Limbaugh and Fox News. I have neighbors who still believe the Clintons had Vince Foster murdered.

While the comment specifies actual entities, such as Fox News, in the scapegoating process, the first statement, "The blow did not come from Russian trolls," is particularly noteworthy. The statement primes the reader to trivialize and thus dismiss the Russian trolling issue. As seen in the comments presented earlier, the rhetoric of such critiques where Russian trolling is concerned has been successfully deployed as a divisive crack in society.

News portal users in their comments have proposed various explanations for the reasons that allow for Russian trolling to perpetuate even if some users have been appalled by the inability of "special services" (e.g., Lithuanian "secret intelligence" services) to eliminate Russian trolls from news portals. One such theory presented on Delfi.lt concerns the evils of commercialism, discussed earlier as neoliberal critiques of media institutions, by exploiting neoliberal critiques, such as the one by Cushion (2012). Thus, it has been claimed that the news media has a vested interest in "feeding the [Russian] trolls" to increase interest and thus profit:

Delfi.lt Example by Anonymous Users 2

Headline: It is a pity

Comment: But these vatniks are protected by the news portals. The money is

the most important. Without vatniks there would be fewer views, comments, less money to the authors of the stories.

Furthermore, this comment claims that Russian trolls are protected by news portals. “Vatnik” as a term, in Lithuanian news portals used as “Vatnikas”, has emerged as a neologism from Russian, typically used derogatorily, to define patriotic Russian rednecks (“Wikipedia, Vatnik,” n.d.), here used as a synonym to Russian trolls. This user emphasizes the sensationalist nature of Russian trolling that has been exploited by news organizations. Consequently, the argument proposed by this user is that the news portals would have a financial incentive to continue that exploitation.

Media’s profit-seeking accusations are implied through reference to the (euro) “cents,” the Lithuanian currency where media is gaining profit:

Delfi.lt Example by Anonymous Users 3

Headline: And in Lithuania trolls continue to bark

Comment: When they want and how much they want. Media has no sense of pride. Just wet cloth. Delfi is not able to start registered commenting. All of it is in the name of cents. It was only 15 minutes [Author’s note: reference to another news portal in Lithuania] who managed this well because they are owned by Estonians who have taken care of trolls-land

This writer speculates that the media profits from trolling—that such profitability is the only obstacle for “taking care of trolls.” Thus, user registration is proposed to redress that obstacle. The word “cents” introduces an oppositional tone to the comment, since it is readable as an allusion to “ruble troll,” where “ruble” refers to “selling out” by the “Russian trolls paid by Kremlin.” And the case of “cents”—reference to the payments made in euro cents, the currency in Lithuania—refers to the gains from the clicks and views in the news portals’ readership advertising revenue.

The following Delfi.lt comment suggests that the media is populated by trolls with various agendas but news portals profit from them:

Delfi.lt Example by Anonymous Users 4

Headline: asw

Comment: When DELFI is going to start isolating kremlin trolls, who are telling lies and us fairy tales and similar?

Response Headline: Never

Response Comment: Because news portals gain from vatniks who increase activity and gain . . .

Response Headline: Let them tell fairy tales

Response Comment: One has to be a truly gullible to believe those fairy tales.

The user with the response headline “Never” responds to critiques of news portals that do not take action against Kremlin trolls. Additionally, “Never” invokes the impression of disillusionment by stating that trolls merely provide a convenient and profitable frame for news portals. Thus, the information warfare aspect of trolling is dismissed.

“Never” repeats this entire argument that “Russian trolls are part of the profit” within the same thread:

Delfi.lt Example by Anonymous Users 5

Headline: Never

Comment: Because vatniks help to earn money

This comment is repeated for argument reinforcement, thus, exemplifying an interesting instance of counterargument construction. The comment presents a partial truth through the claim that news portals are commercial, and that user views and clicks are essential for their business model. Thus, the argument is craftily incorporated and adapted in reference to information warfare, and within the ideological contexts that polarize pro-Russia perspectives and Lithuanian sovereignty ideals.

Deniers have argued that Russian trolling is a media invention. The following comment exemplifies such arguments that are seemingly influenced by conspiracy theories that speculate that Russian trolls are invented by opposition:

Delfi.lt Example by Registered Users 1

Headline: Andrius ██████████

Comment: Romualdas, what do you expect from them? Some time ago the government has invented these trolls so that they can justify lay people’s questions. Later this story has been just escalated. Delfi has even written an article about this: <https://www.Delfi.lt/news/daily/lithuania/premjer-as-vienijo-desiniu-sius-prie-pietu-stalo.d?id=6902>

This user posits that “trolls are invented” by the “political opposition”—at the time the government was a Christian-Democratic majority. Thus, the comment indirectly criticizes Christian-Democrats for inventing trolls and attacks news portals for covering it. It was subsequently removed from Delfi. It after provoking 25 “dislikes,” 10 “likes,” and 8 “crying” emoji.

Other users sarcastically downplayed the threat of Russia by mockingly using the word “horrifying” when describing Russia.

Delfi.lt Example by Registered Users 2

Headline: True Lithuanian

Comment: Russia is so horrifying, soon this cornered monster is going to start to blow the world.

Examples that accuse news organizations regarding monetization-driven agendas and the profitability exploit the narrative from the beginning of the 1990s since news organizations have faced critiques of commercialism, launched against them. Such charges provoked the interrogation of journalism’s professed democratic values—a process that is specific to the internal media ecosystem of Western democracies and to the United States, in particular, such neoliberal media critique of its commercial profitability, that has been found to be exploited in the comments to justify Russian trolling, as seen in the examples above, originally was led by the journalism commentator Stephen Cushion (2012). He critically questioned the values of mass media that originated in the continuous media deregulation efforts of the 1980s and 1990s.

Such a neoliberal critique of mass media has been further elaborated by Fenton (2010), who argued that the political economy of the news compromises the quality of information. Democratic intent remains at the core of journalism, even if Fenton (2010) argued that such efforts were fueled by the best intentions of the liberal market—that is, incentives to provide more options for information sources that could be made available through decentralized broadcasting. Critiques of the neoliberal model of media derive from the media’s conflicting needs: retaining profitability while informing citizens. More specifically, Cushion (2012) warned against unilateral treatments of neoliberal critiques of the media. Such critiques, they argued, merely aspire to profitability.

While contested as an argument, the neoliberal tendencies found in the news organizations have reappeared in the news portals comments as examples of crack in the society or as the media’s vulnerability—in other words, its commercial aspect, and overall profitability being the source of attack on

the media to delegitimize it while justifying Russian trolling, as exemplified in the comments above.

Attack on Government Institutions

Attacks on institutions besides media, such as the FBI, were criticized for their role in Russian trolling investigations in the analyzed US media comments. The rationale behind such criticism was that Russian trolling is unworthy of investigation, or such unworthy investigations are also too costly. Some users questioned public trust in institutions through expressions, such as “Too much money spent” and “They only find trolls.” Thus, their arguments exemplified the rhetorical strategy of delegitimization.

For instance, while focusing on delegitimizing Mueller’s investigation on Russian trolling interference in the 2016 US presidential election, this *Breitbart* user generates false equivalency (i.e., between the investigation and Hillary Clinton’s presidential campaign).

Breitbart Story 6, Example 1

So Mueller has spent tens of millions of taxpayer dollars to tell the American people that 13 Russian trolls tried to sway an election toward Trump and Sanders by buying ads on Facebook and Twitter. Hillary spent close to one billion dollars on her campaign but a Facebook ad swung Michigan, Wisconsin, Ohio and Pennsylvania? Yeah, ok

Other users employed the Russian trolling denial frame by attacking institutions (e.g., FBI). In such instances, the underlying claim is that Russian trolling investigations are unworthy public expenditures. While this frequently reiterated argument trivializes Russian trolling, others downplay the seriousness of social media.

Breitbart Story 9, Example 3

This is actually quite embarrassing to find out that they are indicting some trolls on the internet. What has the FBI become? A laughing stock of goof balls.

This comment exemplifies the most frequently repeated argument: “Russian trolling investigations are a waste of taxpayer money.”

Breitbart Story 6, Example 2

*** The FBI did not have the time or resources to investigate future Mass Murderer. * The FBI used \$15,000,000 to determine that Russian trolls posted messages on internet. Something is wrong America!**

Another *Breitbart* user resorts to mockery in the following comment.

Breitbart Story 6, Example 3

new t-shirt: Millions of dollars, dozens of lawyers and all we got were these trolls

This comment exemplifies the whataboutist focus shift from Russian trolling to other (purportedly) greater crimes.

Breitbart Story 9, Example 4

So glad the FBI is on this like white on rice. No point in wasting time investigating kids who promise to shoot up schools when you can get into something really important like this. Because there were millions of Hillary voters out there who switched their votes to Trump because of these two Russkies and their trolling. Yessirree Bob!

The same rhetorical maneuver is identifiable in the following comment. The user resorts to deflection by implying that Russian trolls are unworthy of investigation, and that the actual offenders remain at large.

Breitbart Story 15, Example 1

So they indict 13 FAKE Russian trolls while the REAL criminals remain in the FBI.

Yet another user mentions an unsolved crime to lessen the seriousness of Russian trolling.

Breitbart Story 15, Example 2

so two days after the FBI got 17 innocent children killed in Florida, the FBI has “indictments” against russian trolls? the timing is suspect and NO this doesn’t make up for dropping the ball on Cruz . . .

Others insinuated that because Russian trolls are merely a subgroup within the larger category of internet trolls, they do not merit serious investigation.

Breitbart Story 15, Example 3

lol,, how many million squandered on internet trolls,, and who pays any attention to them,, we find the trolls here on BB for free

The following rhetorical question is a strategy for making a similar claim.

Breitbart Story 15, Example 4

13 internet trolls cost 10 million dollars to investigate?

Yet others use a more direct line of attack through offensive language to devalue Russian trolling investigations.

Breitbart Story 15, Example 5

Another Wasted Dollar by another Wasted Bureaucrat. How much did this whole investigation cost finding out that there was Russian Trolls on Facebook. GEE - Take it from me. YOUR FIRED A\$\$HOLE!

Russian trolling deniers were also found to delegitimize Special Counsel's work by alluding that it is politically biased:

Gab Example 3

This Judge is an ass. I agree with the attorney who quoted Animal House: #Mueller's probe humor, now, should we?

Another Gab user shifts attention from Russian trolls to the "enemies within" and drug trafficking by packaging the following comments by alluding to "What About Narcotrafficking?":

Gab Example 4

Good Morning Patriots! Yesterday US Border Patrol seized 254 pounds (114 kilos) of Fentanyl. Think about that for a minute. That's enough to kill 57 million people and it cane in thru a legal point of entry. WOW! Can you imagine how much has come in ILLEGALLY? BUILD THE DAMN WALL!

Forget about Russia and China. We need to be worried about the ENEMY WITHIN ie . . . Pelosi, Schumer, Harris etc . . .

Discussion

Some *New York Times* users have summarized the existence of Russian trolls by paraphrasing the main ideas of the *Operation InfeKtion* video series.

New York Times Story 6, Example 1

[REDACTED]

Switzerland Nov. 13

This “Operation InfeKtion” is part of Russia’s long mastered art of “dezinformatsiya”, a term coined by Joseph Stalin, whose loan translation in English is “disinformation”. It derived from the title of a KGB propaganda department. When the Soviet Union realised that it couldn’t beat the West economically and militarily, it sought to weaken it by sowing divisions within a country or pitting countries against each other. The KGB created the fake news story in 1984 that AIDS was a US biological weapon to target Blacks and gays. Ironically Russia stands on the brink of an unprecedented HIV crisis in recent years.

Today, Putin resorts to the same KGB playbook and goes to great lengths to undermine the West. When the EU is weak and the US is embroiled in chaos caused by Trump, a resurgent Russia is seeking to regain its global clout. He has succeeded where his predecessors had failed—“We Will Take America Without Firing a Shot. We Do Not Have to Invade the US. We Will Destroy You From Within.” Nikita Khrushchev. Thanks to the Internet Putin helped Trump win, installing a stooge that obeys the seven commendments of fake news—look for cracks and deepen them; create a big, bold lie; wrap it around a kernel of truth; conceal your hand; mobilise useful idiots; deny everything; and play the long game, i.e. to destroy the country.

This comment outlines the essence of disinformation practices in online news comments. Thus, we might ask: What are enabling conditions for the subversion of online spaces? This chapter covered broader frameworks that render online news portal commenting analogous to information warfare to contextualize how information warfare is relevant today and the complexities and forces of the news commenting system. The conditions that enable Russian trolling to become embedded within news story comments can be

considered in relation to the post-truth era (briefly discussed earlier), subverted news culture, the rise of hate speech and the culture that promotes it, and technological affordances.

This chapter documented a paradoxical subversion of media logics to attack news media and government institutions to justify Russian trolling that takes place through commenting, which is supposed to be a space for democratic deliberation. Commenting is not a new discursive practice where information deliberation is concerned. Together with journalists, who provide information through stories to news readers and viewers, user commenters have contributed significantly to the information sense-making process. Such a sense-making process is typically considered a two-step flow, which Katz (1957) proposed as ways to conceptualize influence through mass media, where the content presented is reinterpreted and reconceptualized by citizen-viewers. Even if the two-step flow of communication is a form of an interpersonal influence, typically conceptualized through face-to-face networks, nowadays it can function similarly online, as since the emergence of comments in mass media, comments have functioned, to some degree, as forms of interpersonal influence through information.

Furthermore, the emergence of commenting options has encouraged news readers and citizens in general to engage with news content and participate in online debates. Yet these very same sense-making possibilities can convert commenting spaces into information battlefields, where automated online groups—even foreign governments—can unleash bots to carry out behaviors that influence public opinion. The structural properties of news portals alone can provide some insights into the specific contexts in which information warfare could take place.

Cited comment examples illustrate that while news portals maintain control over story content, they cannot completely manage user participation patterns or the content flow of news story comments. News portals have, in fact, become notorious spaces for contentious user interactions, otherwise known as “uncivil” discourses. Recent empirical accounts of leading US news organizations on Facebook reconfirm this discursive trend (see Su et al., 2018). Moreover, scholars (e.g., Herbst, 2010; Papacharissi, 2004) argue that civility is a fundamental principle of democratic deliberation and an important marker of a developed democratic society, even if this ideal does not appear to have been realized on social media. Thus, the forces that can provoke online incivility are treated as indisputable facts. The discursive trend of online incivility is far from new, as evidenced by news forums, the predecessors of online news comments. Yet it has been proved that online spaces can be used to exercise influence through content boosting, automa-

tion, and propagation. And thus the current media landscape is entrenched with various influence forces, of which incivility is only one facet.

The Russian troll denial frame was documented in this chapter through doubts about journalistic quality and integrity. In addition to such media blame frames, doubting or questioning frames were also identified in user comments. Particularly noticeable in *New York Times* user comments, such frames provide subtler rhetorical maneuvers than Russian trolling denial on its own (e.g., in Gab). In fact, the doubting frame has been used as a post-modernist doubt-seeding rhetorical tactic that ultimately generates greater confusion rather than clarity. Furthermore, clarity is obscured through absolutist claims that question premises or the supporting evidence behind them. Examples of such claims, introduced in Chapter 2, are “We will never know if trolls actually exist,” “There is no way to know if they exist,” “Trolling cannot exist, if it cannot be seen, or measured,” and “If we cannot know how trolls influenced voters, or the exact number of influenced voters, then, we cannot know if trolls exist.”

These claims exemplify targeting appeals to logic. They are, in fact, evidence-based rhetorical approaches that derive from the Western philosophical paradigms that are based on evidence and logical deduction. Such approaches are used to address general readers of news story comments who are also ordinary citizens and voters—to present them with puzzles that have no solutions. Such puzzles are like riddles that are seeded in our minds—especially when they are unsolved or unsolvable. While they do not provide certainty, they fall outside the discursive parameters of democratic processes. They also provoke distrust in established systems—in evidence providers that include the intelligence and scientific communities. Consequently, ordinary citizens can no longer rely on institutions to provide them with trustworthy answers.

This chapter also introduced challenges over overestimated empowerment that user-generated content brings. Ten years after the “you” phenomenon was presented by *Time* magazine, the European Union countries and the United States of America have been subjected to orchestrated information manipulation campaigns (e.g., Ferrara, 2017), including one that questioned the legitimacy of the 2016 US presidential election. Thus, control seems to have transferred from ordinary internet users to orchestrating regimes in online spaces.

The signifier “you” that promised user empowerment has been also appropriated for information warfare in at least two ways. The first of these involves the exploitation of the assumption that all internet users are authentic. In other words, democratic principles ensure the equal treatment of all users; they are equally entitled to their own opinions and equally encouraged

to post them online. Such democratic equality of user treatment is based upon the misguided assumption that all users are actually authentic. Thus, this assumption can be exploited to circulate information through automated and manual means. Twitter bots exemplify such online agents. Bots are *not* the ordinary users that the “you” movement addresses—authentic human users who facilitate information propagation across online networks.

The second form of “you” exploitation for information warfare involves the assumption that all internet users are infallible—that they are ordinary people who can make sense of new information spaces. The 2006 *Time* magazine cover design does not betray the slightest doubt that the same user (“you”) could also be susceptible to false information. After all, when the issue was published, online spaces seemed invulnerable to orchestrated dystopia.

Moreover, the “you” construct (i.e., “you, the online contributor”) is based upon the “user-as-consumer” business model rather than the “user-as-critical-thinker” cultural ideal. The problem of the construction part relates to what the issue with how the current social media ecosystems work and how people use them (Vaidhyanathan, 2018). Thus, because “you” has yet to appeal to users-as-critical-thinkers, today’s users remain vulnerable to online influence. Van Deursen and Van Dijk (2011) made similar observations while discussing the digital divide. More specifically, they claimed that users require access not only to technologies but also to the information technology skills that would enable them to make sense of online spaces. Consequently, the construct of “you” as “you, the media consumer” creates new conditions for the efficacy of Russian trolling.

Information influence does not occur only through predetermined media ecosystems—the medium and the form—but especially so through content, i.e., messaging frames. There is extensive evidence that messages not only shape perceptions but also stimulate actions in response to them, as argued by Aliaksandrau (2014). Thus, where actionability is concerned, messages exceed mere words. While it can be neutrally stated that trolling is an online discursive practice, far less innocuous are efforts to misinterpret it as a mere word-production process that is dissociated from actual consequences (e.g., information warfare). If we were to acknowledge information warfare as no mere variation of contentious online debate, then Russian trolling is comparable to an online masquerade in which the masks that Russian trolls adopt are integral aspects of information warfare. The following excerpt from by Aliaksandrau (2014) interrelates the two forms of warfare as follows: “Information wars used to be a necessary component that accompanied “real” wars, the ones with shootings, bombings, explosions and killing. Today it is

the opposite—shootings and bombings now accompany information wars. The more you lie, the less you need to shoot. And if you are very good at propaganda, you don't need to shoot at all to win a war" (p. 56).

Thus, while the exposure of Russian trolling seems to depend on successful efforts to combat propaganda, information warfare involves continuous efforts to sustain attack and defend narratives that obfuscate clarity. The combatants involved continuously manufacture oppositional narratives: One side circulates such narratives while the other continuously attempts to expose them as fabricated.

The challenges that accompany the "you" phenomenon are complicated by an additional caveat on the ideal conditions in which Russian trolling narratives can circulate. That caveat concerns a philosophical understanding of *knowing*. The act of knowing is inextricably related to the state of "not knowing." In other words, if we adopt a philosophical perspective, we can ask, How do we know that we know? Two basic premises are involved when we address this question: The first is the modernist assumption that considers that a given phenomenon produces a single, definite outcome; the second is the postmodernist position that challenges the existence of a single truth by positing the availability of multiple modes of understanding. As argued earlier, the postmodern era conveniently coincides with the emergence of new communication technologies. Thus, it can be argued that the convergence of postmodernism with such technologies can generate dangerous outcomes. Such is the post-truth era in the information age.

Vulnerabilities associated with the "you" phenomenon spill over to news portals' comments. News portal comment sections are intended to represent a wide range of opinions that can influence decision-making processes and determine truth and nontruth, reality and unreality. The decision-making thus can lead to action, or at least opinions enable *the channeling of action*. Choukas (1965) described the transition from opinion to action accordingly: "[Opinions] are compounds containing both intellectual and emotional elements with the ratio of each varying according to the amount of knowledge or the degree of feeling the individual put into them in the process of formulating them. They are different from the objective demonstrations of a scientist, or the dogmatic assertions of a theologian, for they cannot be supported rationally as the former and are more plastic than the latter. They vary in duration and strength. . . . Some of them have more depth than others, and hence, a greater resistance to change" (p. 174).

To conclude, news comments are particularly relevant for analyzing the potentially contentious forces of social influence. Such analysis is particularly urgent because the threat of Russian government interference in the

public opinion formation process has reemerged recently. The interference threat concerns not only the 2016 US presidential election but also the Russian government's alleged payment of employees to comment on foreign media sites about a particular 2015 news story that exposed the operations of Russian troll farms (Chen, 2015).

Summary

This chapter discussed how news organizations had employed a range of solutions to address the dilemma of fulfilling deliberative expectations of online public sphere and challenges of dark participation—one that involved striking a balance between the inclusion of more voices and the policing of online incivility. The need for this balance was urgent even before the Russian trolling phenomenon emerged as a major cybersecurity issue. Since Russian trolling, human moderation of online spaces has become even more crucial. Yet such moderation has more complexity associated with it—it is beyond uncivil content moderation, but it is about detection of an orchestrated affect creation. Such detection work for news organizations can be extremely time consuming and costly, especially if performed manually.

Solutions

News organizations have been challenged by dark participation and incivility, such as the interplay between generally rude comments and those that are specifically geared toward foreign influence—whether the medium for such influence is Russian trolling or web brigades.

Dark participation and chaos in news portal comments further complicate the future of online spaces for public deliberation. Moreover, it is crucial to learn how to correctly identify the various types of online content—specifically, to distinguish between orchestrated cyberattacks; innocuous opinions of concerned users, and the amplifications of both. What are some solutions to Russian trolling in news portals? There are several considerations on this front. Diakopoulos (2019), through his optimism about a technological turn in journalism, has proposed that newsbots could amplify engagement of the audiences. However, I view the potential of implementing newsbots as tools to warn moderators about

threats. For example, newsbots can flag repetitive content that circulates across media platforms. Flagged content can go beyond the items that fall under misinformation. Flagging can be designed to include newly emergent affect-instilled comments to stir discord and sway opinions as described in this book.

Another solution is authentication, proposed to discourage the anonymous commenting that could enable trolling. Authentication is particularly debated, given that in many contexts, anonymity is the driving force that fuels democratic debate. Additionally, source verification has been encouraged as the primary means of identifying fake news and other forms of post-truth that some online spaces have already implemented. Some of these initiatives are inherent in the social media platforms' design. Facebook encourages people to register with their real names. Similarly, Twitter has the function of verified accounts, marking those with a blue badge, even if this function is restricted to accounts that can be defined for the public interest ("Twitter Help Center," n.d.). For the news portals, however, user verification for enabling commenting for stories can be somewhat problematic, and news portals constantly face the following dilemma: On the one hand, news portals strive to uphold their gold standard by inclusion of diverse viewpoint. On the other hand, they also are limiting users to only those who are willing to accept the terms of registration to post comments. Such limitations complicate efforts geared toward viewpoint diversification on the part of news portals.

To mitigate the dilemma of inclusion and restriction of user participation, news portals have already taken various steps. Many news portals allow anonymous participation without registration. Yet, for example, in 2021, Delfi.lt announced it would move into registered-only posting. For that, it will provide a range of registration options, primarily outsourcing authentication to the third-party platforms—from social networking sites to email verification. Such verification, though, does not guarantee true authentication of a person. Rather, it might prevent impulse-based affective commenting. In addition, news portals have produced news stories and videos to contribute toward efforts to promote media literacy initiatives that expose techniques of dark participation to readers. For example, they have been involved in the promotion of large-scale educational programs that specifically discuss issues of online propaganda.

News story series have also been released to publicize definitions of online propaganda and to explain how to recognize and manage bots and

ideological trolls. Some sources that encourage online media literacy by specifying trolling characteristics are “How to Recognize and Neutralize the Propaganda-Spreading ‘Trolls’ and ‘Bots’ That Are Occupying the Internet,” by Janckus (2018, Delfi.en), and the video story, “How to Spot a Russian Troll,” by Aneja and Ifraimova (2018, Time.com). Aneja and Ifraimova (2018) also address the dangers of delegitimizing grassroots activism in the face of foreign interference. Similarly, NBC featured a video story, “Inside a Russian Troll Factory” (NBC News, 2018), that exposed the workings of the propaganda machine while addressing how propaganda had influenced the 2016 US presidential election.

Yet another online media literacy initiative that specifies propaganda techniques is *Operation InfeKtion: Russian Disinformation: From Cold War to Kanye*, a video series comprising three 16-minute segments that the *New York Times* released on 12 November 2018. Other initiatives include an online game, *Get Bad News* (Delfi.lt, 2020), designed and then promoted through the news portal Delfi.lt to understand the tactics of online manipulation by positioning the user in a player role who needs to make decisions about the content that can foster manipulation. There were nine stories about the disinformation game on Delfi.lt released in 2020 alone.

While these initiatives are commendable, they are primarily geared toward left-leaning audiences, and such initiatives have not been covered on *Breitbart*. Searches on *Breitbart* with the keywords such as “foreign influence” result in stories that cover attacks on George Soros’s fact-checking initiative (Hale, 2017). In other words, right-leaning users are not exposed to these educational sources about cases of misinformation and disinformation, especially if those cases are framed as blaming the left. As this study has shown, the right-leaning media in the US neither encourages nor provides access to such sources. Thus, it is unlikely that right-leaning publics have access to gain familiarity with them. For instance, since Russian trolling coverage was relatively infrequent on right-leaning spaces like *Breitbart*, the scarcity of educational material about online influence tactics in such spaces is to be expected.

Comment management by news organization staff is yet another initiative to handle internet trolling. Like the charge of news commercialization, other forms of news contestation are viewable through the user-generated content that interrogates democratic values. Although such user-generated content is crucial for democratic deliberation, today’s destabilization of democracy, due to the vulnerability of news portal comments, requires a reassessment of news organizations—how they can inform news readers and still encourage comments that fulfill the democratic premises of debate. News organizations tried different approaches throughout the past decade: By following democratic ideals of participation, they enabled user commenting. Then, some of

them disabled commenting, and others have left commenting sections open only for a portion of the stories. For example, the *New York Times* decided to address the problem of online comment management by enabling user commenting for just 10 percent of all stories. The *New York Times*' decision was made in 2016 due to the lack of a long-term cost and sustainability of human moderation of user commenting (Spayd, 2016). National Public Radio (NPR) illustrates this shift in perspectives regarding the potentials of commenting to impact communities that started with the optimism and led to the subsequent closure of commenting sections for some stories, transpiring through statement in 2008: "We are providing a forum for infinite conversations on NPR.org. Our hopes are high. We hope the conversations will be smart and generous of spirit. We hope the adventure is exciting, fun, helpful and informative. This is important for the NPR community" (NPR Editorial, NPR Launches, 2008, para. 1).

In 2016, however, NPR announced it would shut down the comment sections for stories. The announcement was made in response to user complaints, as in the following example: "A user named Mary, from Raleigh, N.C., wrote to implore: "Remove the comments section from your articles. The rude, hateful, racist, judgmental comments far outweigh those who may want to engage in some intelligent sideline conversation about the actual subject of the article. I am appalled at the amount of 'free hate' that is found on a website that represents honest and unbiased reporting such as NPR. What are you really gaining from all of these rabid comments other than proof that a sad slice of humanity that preys on the weak while spreading their hate?" (Jensen, 2016, para. 11).

Consequently, rather than completely discontinuing news story comment solicitation, NPR has outsourced it to third parties such as social media (e.g., Facebook, Twitter). NPR is not the only news organization that shifted the responsibility of user comment management to third-party providers. News organizations have, in fact, had to adopt creative solutions to the challenges that accompany such management—such as by soliciting diverse user commenter voices and addressing the problem of comment civility.

The *New York Times* increased its staff for comment moderation, notwithstanding the exorbitant costs implementing such practices. The company was able to manage budgets allocated for such online human tasks, however, by enabling commenting for just 10% of stories in 2016, to allow for thorough moderation. Then, in 2017, the company announced a sharp increase in plans to open up more stories for commenting and to use automated tools, such as the machine-learning system Moderator (Etim, 2017; Salganik & Lee, 2020). The system was designed to gauge why comments would be rejected (e.g., inflammatory, insubstantial). Additionally, the *New*

York Times partnered with Google for artificial intelligence initiatives to automate comment scanning (“Google News Initiative,” n.d.). Thus, by 2018, the *New York Times* managed to triple the number of news stories open for commenting from the mere 10% in 2016.

Similarly, there are specific circumstances, where news portals temporarily deactivated comments. One such case was of deactivation of commenting on all news portals in Lithuania on February 24, 2022, was announced as follows: “When Russia started the invasion to Ukraine, Lithuanian news portals have deactivated news commenting sections with the goal to stop potentials for disinformation spread” (BNS, 2022, para. 1). User comments have been similarly deactivated on the news portals’ social media platforms.

Although user comments are undoubtedly valuable for news organizations, they continue to present multiple challenges. These include the determination of practices for meaningful comment negotiation. Thus, while comment incivility had been one of the first challenges, it has been succeeded by the more recent problems of dark participation and automated participation, such as bots, as mentioned earlier. While one solution to such challenges has been the outsourcing of comments to third-party providers, the practice has led to the relinquishment of the responsibility for exercising control over content. However, news organizations, such as the *New York Times*, have elected to forgo this measure. Thus, despite various challenges, for example, the *New York Times* has retained its authority to moderate user comments.

When tackling Russian trolling in news portals, the problem needs to be contextualized within broader comment moderation practices and the specificity of user-generated content management. While Russian trolling is an issue that goes beyond mere incivility, news portals can engage in similar practices to manage them as they did to foster online civility such as enabling later commenting or completely disabling it for more controversial news stories, or even combining human moderation with artificial intelligence, as already implemented by the *New York Times*. While these proposed solutions can facilitate management of online incivility, they can also track down massive influxes of organized influence. Thus, they provide promise to tackle the problem of Russian trolling in news story comment spaces.

Governments have also proposed other Russian trolling management initiatives, some of which are policy driven (Iosifidis & Nicoli, 2020). For instance, by funding an agency that is tasked to combine efforts to promote fact-checking and media literacy to combat disinformation, the European Commission (2019) has unanimously acknowledged the seriousness of Russian trolling. A 2018 report addresses government funding for journalists, and other stakeholders, who help to advance information trans-

parency or media literacy initiatives (European Commission, 2018). The report also provides recommendations and guidelines for all EU member states to enable effective disinformation management. The UK launched government-based offensive cyber security initiatives (Devanny et al., 2021). However, although the report is stakeholder centered, it does not directly address how news portal comment spaces can be infiltrated by ideologically influencing trolls and bots.

Other international initiatives include governments around the world have prioritized disinformation management. For instance, Taiwan's government has launched an aggressive media literacy campaign and initiated a public service that involves the activation of fact-checking bots. And although Ukraine's government has not been as proactive as Taiwan's, Ukraine's private sectors have launched fact-checking online services through online platforms such as *youscan.io*, *SemanticForce.net*, and *InfoStream.co* app for apple products (Woolley & Howard, 2018).

Bottom-up approaches to counteracting Russian trolling, applauded for their grassroots activities, have also evolved over the past several years, such as fact-checking initiatives *Debunk.eu*, a Lithuanian initiative that partners with news organizations and citizens in response to Russian trolling, and a fact-checking project curated by the Annenberg Public Policy Center ("Fact-check, Factcheck: A project," n.d.). Additionally, UNESCO has published a handbook about how to identify and resist fake news while circulating Twitter hashtags (Ireton & Posetti, 2018). These initiatives show how institutional efforts focused on providing identification and resistance efforts involve sharing fake news experiences and ideas about how to respond to them. Thus, the handbook specifies how journalists risk disinformation charges that could negatively impact their credibility. US efforts to counteract disinformation include academic initiatives such as *Botometer* ("Botometer," n.d.), which enables users to determine whether a Twitter profile is authentic or bot-generated, and *Hoaxy*, which allows for identification of false information.

Thus, in light of new context of disinformation, online news portals are facing new challenges in their content and comment moderation management practices. However, online space moderation remains extremely challenging, yet employing AI to combat it seems still unattainable. Scholars like Gillespie (2020) argued that the cost of false positives for solutions that aim at quantifying and scaling is too high—it is an act not of classification but of social and performative assertion of something that should be treated as is and will be thus contested. And it can be exploited as an argument for disinformation. Russian trolling deniers' arguments, presented in this book,

also argue that news portal moderation is an objectionably hierarchical top-down initiative. According to this misconception, news portal moderators are the media professionals and other social elites who exclude all other users from participating in decision-making processes. This misconception can be modified, however, by invoking that news portals comments are based on the idea of user-generated content; that is, all users can contribute to online content with sociotechnical affordances such as content rating and reporting options as forms of moderation.

Similarly, misconception that user-generated content moderation is invariably hierarchical or elitist can be redressed by treating community-based online moderation as an ideal to strive for when it comes to user-generated content in news portals. And while such moderation has been implemented in some instances—for example, the comment flagging in Lithuanian news portals—it can generate anxiety that whoever puts in most effort can dictate the norms of a given online community.

Content moderation has proved a major challenge, even if media companies are putting up resources to enforce best practices, as a Facebook initiative that resulted from challenges of defining what is “right” and their subjective and objective descriptions (Newton, 2019). Yet another measure for discouraging online influence involves comment activation for news stories only after a substantial amount of time has elapsed since their initial release (Almgren and Olsson, 2015). This measure was originally proposed to deal with reactive inflammatory comments. While it can prevent foreign influence through commenting, the major downside is that it can also discourage authentic user comments. Although this initiative is less extreme than the complete disablement of comments that Russian trolling deniers have suggested, it nevertheless generates troubling implications—that the need for public discourses is not so urgent after all and that the democratic foundations for such discourses are actually quite fragile.

Grassroots Initiatives in the Fight With Russian Trolls

Regardless of the challenges of grassroots moderation, grassroots movements have been proposed as the most meaningful way to deal with Russian trolling, as argued by Szulecki (2018), who stated: “The only way to defeat civilizational and moral crisis through grassroots, organic work to overcome decay—with education in humanitarian values at the core” (p. 326).

Lithuanian elves showcase such grassroots initiatives: They organized

themselves to review news portals' comments and flag suspicious content that might have been generated through foreign influence. Lithuanian elves describe themselves as concerned citizens who monitor news portal comments and call out users whose comments suspiciously resemble Russian trolling posts ("Debunk.eu," n.d.). The media coverage of anti-Russian trolling initiatives has included interviews of some of these volunteer elves. One interviewee, who went by the pseudonym "Hawk," claimed that elves act only defensively in online news portals: They neither engage in cyberattacks nor disseminate counterpropaganda. Although the story about Lithuanian elves was released in 2019, elf operations had started earlier, with the eruption of the ongoing Russia-Ukraine conflict, which brought to light the battlefield of facts in the online sphere during this conflict and their power of creating chaos and foster disinformation. In this book, there are several examples of how Lithuanian elves have been attacked. At times, called out Russian trolls addressed their rebuttals to elves by naming them as such. These exchanges provide evidence of the perceived oppositional forces. One is acting as Russian trolls, and the other, that debunks Russian trolling, calls themselves elves.

Similarly, when treating community values in user-generated content contexts, Wikipedia can serve as a successful example for expectation building geared toward meaningful online contributions. In Wikipedia the success of the content contribution and Wikipedia engagement has been found to be dependent on the nurturing of the community, that is, involved and dedicated users who help to foster the community's values (Panciera et al., 2009). While Wikipedia and news portals seem to be very different, their shared element is the community of users who contribute and others who benefit from the shared good—that is, the value that user-generated content provides to communities. Therefore, community values should be fostered on news portals' comment sections. Such values can inform moderation as a practice. Thus, moderation that emerges from the communities enables a continuous enforcement of the community rules with the awareness of practices that are outside of those rules. Such approach could protect communities from threats of dark participation.

Even if the initiatives outlined here provide hope for a more transparent online public sphere, there are some caveats to counteracting Russian trolling. One such caveat is the effect of what Rojas (2010) referred to as corrective actions. Corrective action, can be a powerful argument to counteract Russian trolling by engaging with them and pointing out any argumentative flaws. Such corrective action in the form of counteraction assumes a noble task to correct flawed content found online, in this case, in the news portals'

comments. In the long run, however, corrective action can realize the objectives of Russian trolls: Users end up engaging in futile, self-defensive, and digressive discussions instead of focusing on the actual problem (i.e., Russian trolling) and its plausible solution. Examples of this corrective action included users' calling out Russian trolls and contesting skepticism regarding Russian trolling, illustrated in the previous chapters of this book. Thus, instead of clarifying issues, corrective action generates more online chaos—users end up in a vicious cycle of endlessly diverted arguments, whereby much energy is expended and clarity is only negligibly impacted. Such resource-consuming scenarios exemplify how loss (i.e., energy) can exceed benefit (i.e., clarity). Similarly, another challenge for grassroots activists, like the Lithuanian elves, is that they have become targets of the attacks by Russian trolling deniers, who “fight back” by accusing them as a mere opposition with an “agenda.” Thus, the rational approach—debunking facts—cannot be easily implemented in the *affect-instilled* information warfare of disinformation. Traps of corrective action can affect forms of genuine activism. For instance, Lithuanian news portals were home to an active Russian trolling opposition by volunteer elves who worked to call out Russian trolling. To combat Russian trolling, elves were explicit about using the “callout” technique, even if it might not have been sufficient to combat Russian trolling.

To sum up, comment spaces are convenient target points for the agents of dark participation. Before the challenges of such participation had been documented, the lack of consensus about how to handle online news portal comments had been singularly problematic across all platform types, as argued in recent research (e.g., Boberg et al., 2018; Ekström & Westlund, 2019). Thus, within the context of dark participation, a major question lingers regarding the best practices on how to moderate online spaces, when it is now a generally known fact that not all messages are authentic.

Roots of Russia's Victim Playing

Through new communications pathways what could be called “social technical means,” in contrast to “national technical means” such as orbital surveillance and digital espionage almost anyone can disinform almost everyone else. But while almost anyone now can play, national governments, often through their security services, are playing best. And playing to win, with evident vengeance. (Geissler & Sprinkle, 2013, p. 54)

Chaos in online spaces directly impacts democracy. When we cannot distinguish between what is real and what is not real, uncertainty can permeate our minds. Since uncertainty generates mistrust and fear of “the other,” it is useful for exercising control over people. Such public mind control has been identified as the objective of not only Cold War propagandists but also more recent information warfare that seed disinformation in the post-truth era.

While news portals and social media have been equipped with various solutions for combating automated forces, Russian trolling still presents unique challenges. Russian trolling has been alleged to influence foreign elections, as in the United States and France, through the soft influence of information warfare (Bulckaert, 2018). Thus, to understand Russian trolling, it is critical to uncover the context in which emerged. Russian trolling is contextualized here and treated as a form of government-orchestrated online influence or an astroturfing tactic, as detailed in earlier chapters. Russian trolling throughout this book has been posited as a form of influence in online spaces.

This chapter focuses on a sociopolitical projection of Russian trolling. It details how Russian trolling can be contextualized within Russia's treatment of the online sphere by analyzing media policies associated with it.

Next, this chapter showcases how information warfare has been employed by Russia, the birth of the Internet Research Agency, and the roots of the victim-playing frames where Russians are allegedly victims of Russophobia.

By tracing recent developments in Russia's information warfare through a review of its policies, this chapter outlines how, in the past several decades, Russia has approached online spaces as a matter of strategic geopolitics. Scholars like Michaelsen (2017) argued that authoritarian regimes are not delimited by geographical boundaries. Furthermore, this book argues that online spaces provide new territories for authoritarian regimes to exercise their power. Subsequent sections detail how legitimization works—its contextual treatment and specific discursive techniques.

To enable an understanding of how information warfare can be deployed in everyday life, its success can be gauged by its previous implementation. An example of such success, as it pertains to Russia, is the information streamlining that legitimized intervention in Crimea (Iasiello, 2017) as the move toward restoring Russian identity (Liñán, 2010). Influence during the Crimean conflict is presented here as one of the test cases for information warfare's legitimization of issues, the success of which depended on the approval of targeted populations (Mareš, 2021). In other words, the Crimean case is just one instance of how tactical legitimization has been constructed in the past as a form of consensus. Yet the legitimization of the occupation of Crimea becomes seamlessly embedded in the argument that the Russian government intends to convey to its citizens—a rhetorical argument used by authoritarian regimes. Thus, such legitimization is achieved by the reframing of narratives to target various audiences, which is also found in the comments analyzed that justify Russian trolls and is shown later in the chapter.

One tactic involved in the legitimization of consensus specifically detailed in this chapter is self-victimization—or, more specifically, the resituating of the self from perpetrator status to that of a victim. Such victim-playing is discernible in statements such as “Russian trolls are allegedly blamed for everything,” which supports the self-victimization through alleged “Russophobia” frame. The same “Russians are allegedly blamed for everything” frame has been projected to the Russian people as a campaign to justify Crimea's annexation. Russian trolls are similarly positioned in online news comments not as perpetrators that push their own agendas but as misunderstood victims within those same spaces. Allegedly, Russian trolls are victims because they have been unfairly blamed. In fact, they are presented as victimized scapegoats for all the surrounding world's evils.

This chapter contextualizes Russia's media landscape and its geopoliti-

cal reasoning expressed through (online) media policies. Furthermore, this chapter provides examples of the reemergence of Russophobia arguments used to justify Russian trolling in Lithuanian news portals in 2016 and its prevalence in US news portal comments in 2018. While such victimization seems to have emerged recently in online spaces (e.g., US news comments accessible to all readers), here it is traced back to earlier periods. Victimization frames were reported before the annexation of Ukraine by Russia in 2014 (Liñán, 2010). Prior to the annexation of Crimea, the same assumed Russophobia trope circulated in online spaces and dominated arguments to project Russians as victims who were treated unfairly by foreigners.

Findings about the 2016 US election infiltration reveal how information warfare, combined with technologies that have emerged within the past several years, has become a powerful mechanism for influencing public perception—Russian trolling, as defined by Robert Mueller's indictment, discussed earlier, is one of them. However, there are multiple mechanisms through which authoritarian regimes have regimented and protected their own online spaces from deliberation. Furthermore, this chapter documents how authoritarian regimes use online spaces to push ideological agendas, as through exploitation of the Russophobia frame. This chapter outlines the roots of Russophobia frames in Russia and reviews other rhetorical techniques used to control masses such as legitimization of consensus, limited pluralism, or its opposite information flooding, as typically found used by the for authoritarian regimes and treated by scholars like Roberts (2018) as vehicles of communication suppression.

Thus, this chapter overviews some typical ways to exercise influence for maintaining such an order such as the designation of constraints on technological affordances. The sociotechnical elements in question involve limiting of the creation of user-generated content, the distribution and authentication of user behaviors, and the technological properties enabling those behaviors. However, this chapter further discusses more nuanced ways of implementing control online, such as through soft propaganda techniques, by shaping views or information flood, which makes it too hard to sift through the sea of information to find the truth, thus tapping into the post-truth era.

New Media and Information Warfare in Authoritarian Regimes

Within the context of sociotechnical considerations, the sociotechnical properties of online platforms can strengthen authoritarian regimes from both within their national borders and beyond them, globally (Morozov,

2011; Pearce, 2015; Roberts, 2018), even if some of them are technologically defined and others are socially constructed. Consequently, online spaces discussed here go beyond restricting user behaviors online and as a form of surveillance. They are also used to manipulate positions and opinions, such as the emergence of the Russophobia frame that victimizes Russians and pits them against the rest of the world. These frames then are reintroduced in contexts as ways of excusing Russian trolling behavior.

Legitimization of consensus involves the projection of discourses. Limiting of communication can be also a successful strategy to achieve this goal. And new technologies can not only aid but also enable such limiting through access to technologies and content censorship. Authoritarian regimes, in particular, have employed strategies to limit communication. Technologies in authoritarian regimes have been used to maintain social order, as noted by Pearce (2015). Oates (2013) documented how online contexts have been influenced not only by regular citizens but also by some unidentifiable third parties. Similarly, online spaces have been in the spotlight as host to inauthentic user behaviors, and Russia has been specified as one of the actors involved.

Social media, along with mass media, have been appropriated for subversive purposes in authoritarian regime countries. Online tools have, in fact, been subverted to promote authoritarianism in Russia—for instance, through online voting systems, to make elections appear democratic, as argued by Toepfl (2018). Similarly, Filer and Fredheim's (2016) comparative analysis of Twitter threads concluded that the Russian Twittersphere is a hostile social media environment—one that is characterized by prodigious amounts of automated content and other forms of spam. Consequently, these characteristics have reduced the utility of Twitter for users who oppose governments that have become increasingly authoritarian. Moreover, Filer and Fredheim (2016) described social media as used to consolidate and amplifying a highly polarized and repetitive political conversation.

Furthermore, Gunitsky (2015) has observed that nondemocratic regimes are already gatekeeping online content, a computational technique among numerous others—and that, moreover, such regimes are “shifting toward proactively subverting and co-opting social media for their own purposes” (p. 42). Specifically, the analysis of deleted tweets exemplifies that progovernment forces tamper with political content through an intricate process of deletion and dilution (Filer & Fredheim, 2016).

Dukalskis (2017) discussed how autocratic regimes manipulated, through online legitimation, the ways in which their citizens talk and think about politics. Moreover, legitimation is a crucial component of consent,

according to Gerschewski (2013), who said that “legitimation seeks to guarantee active consent, compliance with the rules, passive obedience, or mere toleration within the population” (p. 18). While legitimation is crucial for securing active consent, totalitarian regimes today exploit online tools for this very purpose. However, recent evidence shows that with the rise of automation and anonymity on internet platforms, such tools are exploited not only for interpersonal gain but also for global influence (Woolley & Howard, 2018). In other words, legitimation becomes one of the pillars propping up the edifice of autocracy and guaranteeing its stability.

The other two pillars, that perform that same function of silencing for dictatorships, are repression and co-optation. Instances of these can be seen through the power-maintenance tactics that authoritarian regimes employ in the countries in which they are entrenched. Intimidation is one of the six warfighting techniques described in the coercion literature, along with denial, attrition, decapitation, punishment, and risk. Intimidation is deemed to be most successfully applied for cyberdomains (Borghard & Lonergan, 2017). Such intimidation can result in limiting activism prevalent in totalitarian regime countries, such as Belarus, Azerbaijan, and China (Bedford & Vinatier, 2018). In Azerbaijan online spaces are used to maintain political control (Pearce, 2015), also observed in Kazakhstan (Anceschi, 2015), whereas the government of China uses online media to exercise constant surveillance over its citizens (Roberts, 2018). Information control, thus, has become a power-maintenance tactic that authoritarian regimes exercise (Kargar & Rauchfleisch, 2019). This type of censorship is notorious as a silencing method that is exercised through the threat of personal harm infliction, such as incarceration, death sentence, or exile—all of which are part of the repertoire of totalitarian practices.

Other tactics involved in information warfare include disruption, espionage, and degradation (Valeriano et al., 2018). Such tactics are known to be typically grounded in coercive diplomacy and cybercoercion. Coercive tactics in the cyberspace have been reported to take new shapes. The Center for Strategic and International Studies in Washington, DC, compiled a report that documents cyberattacks around the world since 2006, showcasing diverse actors and types of attacks, including ransomware, targeting of dissidents by authoritarian regimes, hacking into the essential national security or economic infrastructure, and more recently into medical agencies to access information about COVID-19 medications or vaccines (“Significant Cyber Incidents,” n.d.). This report documented a range of actors involved and different degree in which countries around the world have been affected by it. For instance, in 2019, in the European Union there were around

4,000 cyberattacks recorded daily, with around 55,000 annual attacks in place in Lithuania (Grybauskaitė, 2019). Both countries analyzed in this book—Lithuania and the United States—were among the countries listed for Russian hacking efforts, which account for 164 cases out of around 760 reported cases (“Significant Cyber Incidents,” n.d.). Soft power breaches’ list of cases included before and after the US election breach and warnings that emerged in Lithuanian news portals indicating a range of breaches and denial where orchestrated efforts have been detected.

The Center for Strategic and International Studies, furthermore, reported that hacking is one of the types of information infrastructure breach that has taken various shapes, yet all include one common denominator—they target critical areas, be they economic, sociopolitical, or geopolitical, that are contextually relevant for a given time (“Significant Cyber Incidents,” n.d.). Similarly, approaches to breaches vary depending on the target, which typically is attacked off guard or through “the weak link”—a third-party provider or system. For example, such breaches included the following list of incidents. In 2021, suspected Russian hackers breached the US State Department server and stole emails. In 2020, Russian hackers targeted top Lithuanian officials through information technology infrastructure. In 2020, Russian hacking groups breached US state and local governments and aviation data. In 2020 Microsoft and US Cyber Command took down a Russian botnet ahead of the 2020 election. In 2020, Russian hackers targeted government agencies in NATO (North Atlantic Treaty Organization or North Atlantic Alliance) member countries. In 2017, 2018, 2019, and 2021, a hacking group with Russian ties was reported as having attempted to breach US critical infrastructure (e.g., water, nuclear, energy, aviation, manufacturing). In 2018, Russian hackers impersonating US State Department officials attempted to gain access to the computer systems. In 2018 Microsoft announced that Russian hackers targeted US senators critical of Russia and campaigns of three Democratic candidates running in the 2018 midterm election. In 2017 Russian government hackers stole National Security Agency secrets through Kaspersky antivirus software. In 2014 was the Yahoo hack by two Russian intelligence officers that compromised 500 million user accounts (“Significant Cyber Incidents,” n.d.).

In addition to hacking, social media allows for control-based power maintenance through surveillance. Kagar and Rauchfleisch (2019) analyzed how authoritarian states retaliated against citizens. Kargar and Rauchfleisch (2019) concluded that the Instagram musicians they analyzed were found to be “targeted by state-aligned hackers because of their controversial music, e.g., songs that address politically and socially sensitive topics such as censorship, theocracy, homophobia, and sexism” (p. 1508). Such online attacks were followed by other retaliatory measures. For example, the musician

Najafi's Instagram profile photo was replaced with an image of the flag of the Islamic Republic of Iran and his personal information was subsequently disclosed.

Limited pluralism, whereby information restriction is a typical example of sociotechnical constraints, is a strategy used by authoritarian regimes (Heinrich & Pleines, 2018). Limited pluralism does, indeed, provide spaces for participation but in restricted ways, such as authoritarian control that limits activism, as witnessed in Iran (Michaelsen, 2017) or Azerbaijan (Pearce et al., 2018). Furthermore, authoritarian regimes such as in Iran, were found to exercise censorship through the cyberspace control that suppresses voices of political opposition online (Rahimi, 2003, 2008). Individuals who voice dissenting political opinions are subjected to cyberattacks or other forms of intimidation. Such intimidation typically occurs during politically significant times, such as national elections (Anderson, 2013; Benner et al., 2018; Bruns & Eltham, 2009).

In other contexts, there is an even finer line between the soft and hard power exercised by authoritarian regimes. Jamal Khashoggi, a journalist who critiqued the Saudi government while living in the United States has been a victim of continuous online attacks, that ended with his death. This case exemplified how a so-called troll farm working on behalf of the Crown Prince Mohammed bin Salman was silencing voices of influential Saudis who had criticized the kingdom's leaders (Benner et al., 2018). The *New York Times* reported this case as follows: "Mr. Khashoggi's online attackers were part of a broad effort dictated by Crown Prince Mohammed bin Salman and his close advisers to silence critics both inside Saudi Arabia and abroad. Hundreds of people work at a so-called troll farm in Riyadh to smother the voices of dissidents like Mr. Khashoggi" (Benner et al., 2018, para. 4). In this case, information warfare provoked tangible outcomes that exceeded mere online incivility or disagreement—and ended this journalist's life.

While incivility is usually a problem in online spaces, authoritarian or totalitarian regimes make such spaces appear as though they were actually governed by civility—given that they employ limiting and retaliation tactics. The semblance of online civility in such instances is ominous. Such simulated civility also exemplifies that, instead of encouraging free speech, authoritarian governments promote their own agendas online.

Roots of Russia's (Information) Warfare

To contextualize Russian trolling and its operation online, it is imperative to understand the workings of Russia's media ecosystem and Russia's

approaches to online information warfare. While this book focuses primarily on the Russian trolling phenomenon in online spaces accessible outside of Russia, its objective is to contextualize mass media and social media policies enforced in Russia throughout the past two decades. For example, Putin's Russia has adopted a markedly serious approach toward all forms of mass media, including those that involve the use of online spaces. In other words, Russia has endorsed a conceptual framework that equates online spaces with information warfare zones while gradually regulating data use.

Russia's online information warfare can be traced back to the late 1990s through the early 2000s. The resurgence of information warfare goes hand in hand with the regulation of information. Such territorialization of the internet was enforced through the 2019 laws passed in Russia enabling what is known as digital sovereignty, intended to isolate Russia's on-demand internet use or to block incoming communication from outside its geopolitical boundaries (Musiani, 2019). Online spaces in Russia have gradually been treated as physical battlefields, similar to physical spaces. Thus, information online spaces have been guarded, as military war zones would be.

In other words, Russia has developed a system to protect its internal mass information flows through centralized government control. Such protective measures involve the control of Russia's incoming information—an endeavor known as digital sovereignty that has been implemented through Runet, an independent computer network that has been disconnected from the Western internet. In fact, Western media outlets such as the BBC call Runet the “unplugged internet” (Wakefield, 2019). In December 2019, Russia's announcement of the successful test of Runet signified its independence from Western information channels.

For the remainder of the Western world, however, this declaration of independence from Runet implied that Runet was actually a vehicle for exercising greater control over the information access of Russia's citizens. Yet Russia insisted that an insulated, government-controlled internet is a strategic need. Thus, Runet has been ratified by a government provision through a bill signed by Vladimir Putin (Rossokhovatsky & Khvostunova, 2019). Runet, thus, presents itself as a case of what Sivetc (2021) called infrastructure-based censorship. Infrastructure has been used to collect and track all user transactions online and obligate third-party companies to share data. Such infrastructure-based censorship has been backed by a legal system, i.e., passing data localization law that allows to surveil citizens in all spheres of their online activities.

An unplugged internet network illustrates how Russia has a clear and unified vision of the exercise of power inherent in mass media and informa-

tion systems—that is, within both mass media and online or digital media. As Maréchal (2017) observed: “Russia does not view internet governance, cybersecurity, and media policy as separate domains. Rather, all the areas covered by those disciplines fall under ‘information security’ for Russian foreign policy” (p. 29).

Russia’s internal lockdown functions like a defense mechanism during information warfare. This lockdown has, in turn, been followed by information warfare attack mechanisms geared toward influencing the information spheres of foreign governments, be it Ukraine or the US. Specifically, this section deals with the mechanisms of soft influence and strategic planning that involves information management. This strategic planning is exemplified by surveying Russia’s information landscape from a policy perspective. This section also lays the groundwork for understanding Russia’s information management mechanisms that were employed before Russian trolling accusations went public.

2000 Doctrine

Besides Runet as providing network independence, Russia’s information warfare history can be traced back to the mass information lockdown following its tightened legislation. Information control was consolidated first through Russia’s regulation of foreign agency financing of mass communication and second through its information content management practices.

When describing the facets of information warfare, it is relevant to contextualize the specificity of Russian mass communication as an area of control. Such contextualization is crucial because information control remains a prerogative of authoritarian regimes. Moreover, various perspectives purport that control is a safeguard for internal information flows. The 2000 doctrine describes the processes of Russia’s initial perception formation concerning boundaries, both physical and virtual—a perception that informs its exercise of control over foreign information access within its own boundaries and beyond. In Russia, information warfare is closely related to geopolitics, as mentioned in the case of Runet. In short, physical geopolitical control is transferred to the online sphere. Thus, it is worth emphasizing that Russia considers the virtual public sphere a physical geography, thus extending its notion of information warfare to encompass the ideal of victory over specific territories of influence.

The goal of information warfare is to seize control of the online public sphere—in this case, within the former Soviet Union (Iasiello, 2017).

As a result, in 2000 Russia's information infrastructure has been regulated through the Information Security Doctrine of the Russian Federation (Public Intelligence, 2020). According to this doctrine, the Russian Federation's national security threats reside within information communication technologies, such as computer-based internet networks. Martišius (2014) emphasized Russia's prerogative of focusing on information warfare as a critical means of securing control over a specific geographical region. To support his argument, he cited Panarin and Panarina (2003), who asserted that the expansion of Russia should occur through the proliferation and control of mass communication. Similarly, Manoilo (2003) emphasized the effectiveness of information warfare for foreign politics.

Russia's crackdown on internal information has been further detailed by Aksartova (2003), who described the effects of the 2000 doctrine and its implementation in Russia's mass information. The first step in the crackdown involved prohibiting foreign companies from contributing to Russia's mass media information and communication flows. This prohibition has also been enforced retroactively, so that only citizens of the Russian Federation can start up new media institutions that manage communication information. This restriction has been followed by the central government's consolidation of mass information. By 2018 Freedom House stated that the Russian information system is not free but is an area under Putin's direct jurisdiction ("Freedom House," n.d.).

The 2000 doctrine remains relevant for discussing Russia's information warfare today. Like other authoritarian countries, Russia emphasizes the threat of foreign influence through information. And to prevent such interference, it created laws that prohibit foreign media from entering the country. One result of the 2000 doctrine was the shutdown of Радио Свобода (Freedom Radio), a former recipient of financial support from the US that had served as an independent news source. Consequently, without foreign and alternative media sources, Russian mass media can shape the narratives involved in all issues by legitimizing the government's actions or by focusing on Russia's positive aspects while prohibiting any criticism. At the same time, Russian mass media is permitted to advance its own agenda by criticizing foreign countries.

While the 2000 doctrine marked Russia's implementation of defensive mechanisms in its information warfare campaign, Russia concurrently employed offensive or proactive information warfare tactics. As opposed to defensive mechanisms, such as infiltration and control of foreign mass information, offensive mechanisms were launched through an ad hoc information warfare media ecosystem that targets foreign governments. In some

instances, such mechanisms of influence involved circulating information about Russia from within its geopolitical boundaries to shape perceptions of Russia abroad through mass media such as Russian Voice, RTL Planeta, or TV channel Russia Today.

Offensive tactics include a range of mass information channels geared toward influencing perception abroad. For example, Голос России (Russian Voice), the radio station established in 1929, is one such cases that reorganized the “ether” in the blink of the dissolution of the Soviet Union. In 1993 it has been reorganized by the decree of Boris Yeltsin to illuminate foreign countries about cultural, political, and social life and events in Russia (Innovbusiness, 1993). This government-run station operates in 31 languages with an audience of nearly 100 million listeners worldwide in 160 countries.

In 2002, RTR Planeta (RTR Planet), a state owned broadcaster in Russia, which hosts a simultaneous online TV channel, was established to project images of Russia from the perspective of its desired perspectives (“RTR Planeta,” n.d.). This TV channel has a YouTube channel to enable further distribution of online content and purports to serve the Russian-speaking diaspora. However, strategic information warfare elements have been identified in programs aired on this TV channel (see, e.g., Martišius, 2014). In fact, there have been claims that if governments do not regulate these channels, they will be utilized to influence people who speak Russian or are ethnic Russians living abroad to retain the Russian government’s viewpoints.

Russia Today, a TV channel whose goal is to inform foreign citizens about Russian politics, has also been under fire—in this case, for resorting to tactics of propaganda deployment (Yablokov, 2015), such as conspiracy theories legitimizing Russia’s political decisions and attacks on adversaries such as Western democracies that withhold their approval of Russia’s politics. Even if Russia Today presents itself as a public diplomacy tool, this mass media broadcaster is still used to project predominant state narratives, such as “other countries have more problems than Russia,” and promote conspiracy theories, reflected in the slogan “question more” (Elswah & Howard, 2020). Moreover, content analysis of Russia Today programs revealed that rhetorical strategies propagate one-sided narratives about contentious or political issues (Borchers, 2011; Rawnsley, 2015).

Other scholars such as Pomerantsev (2014) described Russia Today’s modus operandi as a “mash-up of truths assembled and interpreted in ways that rewrite reality” (p. 43). Consequently, as Pomerantsev explained, these “mash-up” truths are geared toward generating “apathy, distrust, and a vague sense of paranoia” (p. 43). This statement, in turn, explains that the goal of

Russia Today news is not the provision of greater clarity, but the obfuscation of questions of interest—in other words, the creation of chaos in the minds of Russia Today program viewers around the world.

Furthermore, the concepts of confusing, befuddling, and distracting are all encapsulated in “question more,” the motto of the multilingual Russia Today. There are two aspects to the motto that are difficult to unpack: The first of these involves the indisputable assumption that “question more” is meant to enhance clarity. Yet when presented with tangential arguments, “question more” can become a powerful technique of whataboutism by asking questions of dubious relevance, that digress from main issues, or that divert focus to others. In other words, “question more” can become a deflection technique. Moreover, it can be used to legitimize the actions of a specific country—legitimization being a technique that authoritarian regimes use to maintain their power.

The description of Russia’s mass media information warfare through the 2000 doctrine provides an overview of the media ecosystem charged to channel consistent messaging targeting recipients outside Russia—for instance, foreign governments through Russia Today. Another element of information control was used to protect from the potential information influences from outside of geopolitical sphere of Russia. Such self-protection was implemented by regulating the internet to prevent non-Russian users from channeling their messages through online tools that are not systematically regulated. With this goal, Russia began to adopt preemptive strategies to “protect itself” from foreign influences where geographical boundaries of physical territory was applied online, given that online spaces are not uniformly regulated. Such loosely regulated spaces involve user-generated content, such as social media posts and news portal comments.

Internet Research Agency

Information influence targeting territories outside of Russia led to the birth of the Internet Research Agency, or IRA. When describing Russian automated activities by the Internet Research Agency, Howard (2020) contended that the most far-reaching IRA activity was in organic posts, not advertisements, as it is typically perceived as ways of measuring impact of campaigns (and advocated by some scholars; Jamieson, 2018). And therefore, organic content spread by IRA, according to scholars like Howard (2020), led to the greatest reach and influence, achieved through polarizing people’s opinions. Tactics of information warfare have been largely associated with the IRA.

This section describes the birth of that main actor, which is linked with the beginning of the Russian trolling phenomenon.

While Russia's information lockdown is inscribed by the 2000 doctrine described above, less is known about how influence works at the messaging level. The declaration of the 2000 doctrine and its implementation show the intent and directionality of the values behind a specific issue—in this case, information flow. Yet how the influence takes place in the everyday public sphere is less visible.

US journalists identified the IRA as the originating source for Russian trolling and held it accountable for its misinformation campaign throughout the 2016 US presidential election. Furthermore, the most recent scholarly reports that exposed the mechanisms of information warfare also detected IRA presence in the US presidential elections. Reported tactics included targeted tweeting involving IRA-controlled Twitter accounts, based on in-depth analyses of Russian troll behaviors in the presidential elections that originated in the IRA (Zannettou et al., 2018), otherwise known as the Russian troll farm (Chen, 2015). These accounts were used to infiltrate and influence online communities that endorsed both left- and right-leaning political views. Such influence was achieved by stirring discord across political spectra (Zannettou & Blackburn, 2018) and the results of tweet analysis showed that “Russian government-sponsored troll farm called the Internet Research Agency, [which] was the subject of a federal indictment issued in February, stemming from Special Counsel Robert Mueller’s investigation into Russian activities aimed at influencing the 2016 U.S. presidential election” (para. 2).

The extent of the infiltration was determined by analyzing the tweet activities of the accounts listed and later released in a congressional investigation. Zannettou et al. (2018) concluded: “Russian trolls exhibited interesting differences when compared with a set of random users, actively disseminated politics related content, adopted multiple identities during their account’s lifespan, and that they aimed to increase their impact on Twitter by increasing their followers” (p. 225). These findings of “muddying the water” confirmed the work of various scholars like Bessi and Ferrara (2016), who concluded that about 20% of tweets engaging with 2016 US presidential election candidates were posted by bots. The prevalence of bot-style communication was identified in the midterm elections on social media as well (Luceri et al., 2019). All of these facts are undeniable evidence that Russian trolling exists, proving how and the extent to which it infiltrated US online communities across the political spectrum. Yet the question lingers: How specifically did this infiltration occur in 2016?

Within the context of computational propaganda discussed earlier in this book, Russian trolling is conceivable as a form of astroturfing—a concept related to user-generated content influence and synthetic online behaviors. As a term, “astroturfing” has emerged primarily in commercial contexts. In an era when anyone can speak about brands, the reputations of branded commodities are constantly at risk. Thus, to enable their marketplace survival, companies have started to manage proactively their public relations through the falsely authentic reviews that positively skew opinion about their branded products. Thus, we might recall that the term “astroturfing” first emerged in a political context: US Senator Lloyd Bentsen of Texas coined it in 1985 to refer to companies or individuals that mask their ulterior motives and act as participants of grassroots movements (Goldschein, 2011).

Since then, corporations have adopted the term. In his overview of ten fake grassroots movements in *Business Insider* (2011), Eric Goldschein described their operations accordingly: “Grassroots movements are so powerful because they reflect the will of the people. There’s no filter, and no ulterior motive: just a natural, independent effort to force change” (Goldschein, 2011, para. 1). Yet the goal of these movements is to pay people to mask realities while promoting their altered variations. Within nonpolitical contexts, faking hype about McDonald’s burgers exemplifies a relatively minor effort to influence consumer perceptions, albeit in an ethically questionable way. However, politicians were found not to be an exception. One such notorious case regarded the creation of a fake Twitter account to support Toronto’s mayor Rob Ford and his policies.

Astroturfing and propaganda campaigns share the following approaches: They provide misleading information or pay people to spread misinformation by altering reality. For instance, McDonald’s has been known to pay people to line up in front of stores to simulate overeagerness for a newly upgraded half-pound burger. A more insidious case of consumer influence is Phillip Morris’s sponsorship of operatives who cover up health-risk warnings printed on cigarette packaging (Goldschein, 2011). More recent incidents include Yelp review fabrication and filtering to manage business reputation; around 16% of Yelp reviews are filtered (i.e., manually selected which ones stay and which ones are removed) to a certain degree (Luca & Zervas, 2016). While ethically questionable, such practices are business strategies used in good faith in a marketplace where buyers and sellers compete for best possible deals on all products—and that includes intangibles like opinions.

However, what happens when a foreign government resorts to astroturfing? Government-ordered fabricated social media posts have been empirically documented by Chinese government indicating that 2,000,000 people

have been recruited for such operations with an estimate of 448 million posts a year produced by such operations (King et al., 2017). King et al. (2017) showcased that the goal of such commenting not to engage with debate (as it is expected in the democratic ideals) but to distract and deflect attention by changing the subject. Changing the subject involved positive information about China such as praises of the Communist Party.

Russian trolls working for the IRA use this large-scale, surreptitious commercial scheme to influence public opinion. Volchek and Sindelar (2015) exposed information about payments made to the “general citizen” to write comments. Their report includes an IRA employee who described the comment production process accordingly: “It’s a real factory. There are production quotas, and for meeting your quota you get 45,000. The quota is 135 comments per 12-hour shift” (para. 9) He, then, proceeded to describe the nature of the work as follows: “The main task of the factory is to write on visitor forums, in particular forums run by Russia’s ideological enemies. Who does that? Burkhard: There’s a Ukrainian department, an English department. They bombard the websites of CNN and the BBC. They have their own type of targets—*The New York Times*, not the Samara city site. It’s a little simpler for us, of course” (Volchek & Sindelar, 2015, para. 25).

Then, he mentioned the underlying ethos of commenting, describing the unfixed, fluctuating nature of political ideologies:

Yes, there are special people working on Facebook. There are about 40 rooms with about 20 people sitting in each, and each person has their assignments. They write and write all day, and it’s no laughing matter—you can get fired for laughing. And so every day, any news does the trick—it could be Obama, could be [German Chancellor Angela] Merkel, could be Greece, North Korea. The young people doing this work are barely capable of formulating what’s important about these stories. Even a political scientist can’t be an expert about the entire world, but here people are expected to write about everything. And how you write doesn’t matter; you can praise or scold. You just have to put those keywords in. (Volchek & Sindelar, 2015, para. 28)

The paid and orchestrated aspect of Russian trolling that renders it comparable to astroturfing also raises questions about the agents of orchestration and shifts accountability from the Russian government to third-party corporations. Due to strict regulation of Russian media spaces, however, such arguments are not very credible. Interestingly, Russian trolls are frequently

referred to as “sock puppets.” According to Lee et al. (2014), ideological sock puppeteers can be government employees, regular internet users who attempt to influence discussions, or “crowdturfers” hired to fabricate reviews and post fake comments about products. While Russian trolls have been unmasked as actual operatives working on behalf of the Russian government, the focus here is on the mechanisms of Russian trolling rather than the actual user identities of Russian trolls.

In early 2013, *The Atlantic* staff writer Olga Khazan (2013) exposed in her story “Russia’s Online-Comment Propaganda Army” the paid aspect of commenting in online news portals: “At least some anti-Western comments appear to come from staffers the Russian government pays to sit in a room, surf the Internet, and leave sometimes hundreds of postings a day that criticize the country’s opposition and promote Kremlin-backed policymakers” (para. 8). In other words, Khazan described how users, who sensed the excessive hostility of online environments through antagonistic progovernment posts, have discontinued their participation. Such discontinuation revealed the suppression of spaces for free expression. Moreover, Khazan lamented: “Judging from recent events, though, open, vigorous, and untainted online discussion is something Russia badly needs” (para. 14). Yet she also suggested that internally implemented silencing of citizens had been orchestrated by the government.

In 2013, when Khazan’s article appeared in the US media, few readers would have predicted the hot topics concerning Russia that would be debated during the 2016 US presidential election year. Khazan’s article proves that online influence strategies, including posted news article comments, were orchestrated by the Russian government as early as 2013.

Information Warfare in Action by Russia

Reflexive Control as Soft Influence

Some scholars view information warfare and propaganda use as typical characteristics of political turmoil. Moreover, it has been observed that the invisibility of actors in the process of influence exemplifies that soft influence alone does not emerge during times of political turmoil (Simons, 2015). Propaganda can hide behind an innocuous presentation of alternative informational facts, but it has real-world consequences. Thus, it is crucial to understand the various ways the online public sphere remains particularly relevant for us today.

Because information warfare is typically situated within a specific framework, the identification of generalizable online tactics of influence can be a complicated process. For example, the difference between Russia's information warfare that had been codified and deployed in the former Soviet Union and its Western counterparts has been noted (e.g., Chotikul, 1986; Huhtinen et al., 2018; Mustonen-Ollila et al., 2018). Specifically, the Russian framework for information warfare is reflexive control, described as a process that "allows initiator to induce and adversary to take a decision advantageous to the initiator through information manipulation" or as "a method for achieving geopolitical superiority and as a means for arms control negotiations" (Thomas, 2015, p. 16). Thus, reflexive control is closely related to the concept of influence—more specifically, the kind of influence based on the decision-making that affects a selected target group and shapes its information environment. It can be argued that the principles of Reflexive Theory in a form of cyberwar or information war had been successfully implemented to maintain control in the former Soviet Union where the information superiority is gained by applying pressure, providing false information, confusing the decision-making by the adversary and by manipulating timeliness of events by starting unexpected operations (Jaitner & Kantola, 2016).

Iasiello (2017) described Russian information warfare as "influencing agents [rather] than as destructive actions" (p. 51). This assumption treats information warfare as an invisible process, rather than as a conflict that involves physical, or tangible, elements. Iasiello further elaborated: "The information space lends information resources, including 'weapons' or other informational means, to affect both internal and external audiences through tailored messaging, disinformation, and propaganda campaigns" (p. 51). And then concluded that "the essence of information confrontation focuses on this constant information struggle between adversaries" (p. 52).

Several tactics are commonly deployed in the information battleground, as discernible through Iasiello's (2017) citation of Igor Panarin, a Russian information warfare expert, to outline propaganda techniques. These are divided into the following macro levels or structures, or into what Iasiello (2017) called instruments, including propaganda (black, gray, and white), intelligence (specific information collection), analysis (media monitoring and situation analysis), organization (coordinating and steering channels, influencing media to impact the opinions of politicians and mass media), and other combined channels. Furthermore, information warfare vehicles include social control, social maneuvering, information manipulation, disinformation, purposeful fabrication of information, as well as lobbying, blackmail, and extortion (Darczewska, 2014).

Reinstating National Pride

While authoritarian regimes censor and manipulate information, they also use other historically relevant and context-specific instruments to maintain their power (Kargar & Rauchfleisch, 2019). Thus, Russian trolling requires historical and geopolitical contextualization. Specifically, the underlying assumption of the phenomenon is that Russian trolls emerge from either a tradition of propaganda crafting or a process of geopolitical media evolution. To evaluate this assumption, it is crucial to examine the historical circumstances that contour the current Russian media landscape and its media politics. This examination enables us to identify mechanisms of propaganda that have been formerly used together with an overview of the evolution of Russia's media ecosystem. Thus, a discussion can be initiated regarding the agents embedded in the current information battlefield of Russian trolling. Moreover, detailing propaganda mechanisms of the past can serve as a baseline for propaganda today. We can answer questions such as How are they reflected and to which degree they reemerge in the current social media landscape and in news portal comments?

Information manipulation techniques considered here reflect a periodization that is temporally and spatially based—that is, techniques that were crafted and perfected in the former Soviet Union and have continued to be deployed throughout the decades since its dissolution. The recent ubiquity of information communication technologies and their continuous use for political purposes need also to be taken into consideration. The relevance of Russia within the context of these concerns is eloquently described by Masha Gessen (2017), on the totalitarianism that has been reclaimed in Russia since 2012. Gessen argued that since that year, Putin's administration initiated a complete political crackdown that resulted in a war within Russia and involved that nation in hostilities against its neighbors, including physical invasion of Ukraine on February 24, 2022. This crackdown began with the invasion of Georgia in 2008, and it continued in 2014, with Ukrainian information warfare. All are presented here as a context that preceded Russian trolling in the 2016 US election.

Cases of the information “maintenance” summarize the steps that Russia took since the Soviet Union's collapse. The first of these addresses the problem of national identity, and the second involves the expansion of national identity-based propaganda mechanisms to justify the invasion of a country already saddled with questions about its own sociocultural identity, concluding with the concerns expressed for the geographically unlimited post-TV era information “maintenance” of online spaces that transcends national

borders. These cases illustrate the source of the Russian troll justification frames and the context of such victimization.

The first one is reinstating national pride. A major rationale for the relevance of the information maintenance in the case of Russia is the drive to reinstate national identity and generate national pride. Reinstating the national pride constitute efforts of the propaganda “at home” geared toward Russia’s citizens. Through its evocation and revision, history has been actively converted into a powerful propaganda tool for weaving persuasive narratives that conform with the agendas of Putin’s Russia. National pride is projected through visions of Russian greatness, packaged by the movement of Eurasianism led by Ivan Ilyin and Alexander Dugin (Orenstein, 2019).

Dugin has assumed roles not only in Russia’s political life; he also has written extensively on the topic of Eurasianism or neo-Eurasianism by opposing Eurasianism to Atlanticism framed through geopolitical spheres of influence (see Dugin, 2015). Geopolitical emphasis is further presented by Dugin through aforementioned ideologies and is also clearly engraved in the naming of these two powers. In a nutshell, Eurasianism ideology, postulated by Dugin, envisions an emergence of a new power that does not include the West and that projects Russia as great again after the defeat brought by the collapse of the Soviet Union, while Atlanticism represents the West. Dugin, described by writers such as Heiser (2014) as “Putin’s brain,” is deemed to be a “father of . . . Eurasianism.” However, Eastern European scholars like Orenstein (2019) are less subtle about the role of Ivan Ilyin and Alexander Dugin in the forming the Eurasianism ideologies by positioning them as fascist thinkers aiming at restoring the national pride through geopolitical determinism.

Reinstating the national pride is considered by scholars like Liñán (2010) as a rhetorical devise behind Putin’s propaganda, stating that the ideals embedded in the narratives evoke the bygone historical grandeur of the Soviet Union to redefine the Russia’s present. The past can be appropriated conveniently: It cannot be reliably supported or contested because there are no witnesses. At the same time, it can be amplified and embellished according to specific needs. Such perception-shaping techniques were deployed as national identity-framing mechanisms that primarily targeted the Russian people.

According to Liñán (2010), more specifically textbooks and movies are two predigital age media forms that mass propaganda could appropriate. Thus, the project of consolidating national identity is historically based—one that uses facts, allegedly rooted in a historical past, to project aspirations for a “bright” national future. Liñán’s (2010) concluding statements articu-

lated this phenomenon of historical myth making: “The apparent success achieved in building a “positive” view of history of which Russians can feel proud could be a mirage that dissipates with the same speed with which it was created. In spite of the efforts, the historical message transmitted over this period is “on the defensive.” It is propaganda discourse that rather than shedding light on the past, accuses those who question Russia’s greatness of lying” (p. 177). Such a positive national identity reinstates national pride but also repositions a nation in contrast to others.

In the case of Russia, national pride has been equated to notions such as geopolitical superiority. Thus, geopolitical superiority has been promoted through post-Soviet information warfare. It is further reflected in Martišius’s (2014) claim that Russia’s information warfare objective is its maintenance of control over former Soviet territories. Ultimately, the goal was to produce a geopolitical vision that supports the Russian Federation’s nationalistic agenda.

Efforts to advance geopolitical superiority agenda can be traced in Russia’s treatment of the Baltic states. Since the Baltic states seceded from the former Soviet Union, the tension between Russia and the Baltic states has remained. Lithuania, which was the first to declare independence from the Soviet Union, has been vigilant about information warfare breaches. In the past decade, Lithuania’s government routinely informed and warned its citizens about not only cyberwar attempts through internet server breaches of the government’s online infrastructure, i.e., soft influence, but also provocations in the air force, with continuous breaches of airspace regulations by Russian fighter jets, i.e., hard influence. Such warnings have been delivered through news stories, and multiple reports have been released concerning the incursion of Russian fighter jets into Baltic airspace. More specifically, it has been reported that they frequently breached NATO airspace regulations in the Baltics—sometimes, several times per week, as documented in the news stories (Alkas.lt, 2014; BNS, 2017, 2018a, 2018b, 2018c, 2019; Ekspertai.eu, 2015; Elta, 2017).

Moreover, it was discovered that Russia had mobilized through soft influence Russian-speaking communities outside its current geopolitical boundaries, such as those within its former Soviet regions—specifically, the Baltic states (Helmus et al., 2018; Karpan, 2018; Simons, 2015). When considering Russia’s media development, it is evident that over the past two decades, Russia has prepared its media landscape for the exercise of foreign influence. And opportune moments have emerged within recent years for testing the effectiveness of such influence.

Hard influence, or physical intervention, has been also used by Russia in

combination with soft influence. A combination of these powers, resulting in the hybrid information warfare tactics that were deployed in the 2008 invasion of Georgia and in Ukraine's Crimea in 2014 and in 2022. While Georgia's conflict exemplifies the problem of access to physical territories, the one involving Ukraine represents hybridity of physical combat and information warfare (Iasiello, 2017).

Russian Trolling and Ukraine

While propaganda techniques used for internal purposes (within Russia) are contextually relevant to understand the effectiveness of post-Soviet propaganda, the contexts in which it has been used that go beyond the national spectrum, must be reviewed. The second period can be considered a test case for the manual manipulation of the public through social media employed by Russia. A specific instance of this period involves the information warfare deployed against Ukraine. Since Russia's annexation of Crimea in March 2014, Crimea has become a test case for manual control of the public sphere by the Russian government—one that exemplifies the resurgence of post-Soviet propaganda (Helmus et al., 2018). Specifically, the German newspaper *Spiegel* reported in 2014: “Moscow's independent business daily *Vedomosti* reported recently that, since the start of the Ukraine crisis, the presidential administration in Moscow has been testing how public opinion in the United States and Europe can be manipulated using the Internet and social networks” (Spiegel, How Putin, 2014, para. 14).

Thus, questions arise: What techniques were utilized in Ukraine? What specific topics were pertinent to the Ukrainian case that enabled its success? Martišius (2014) outlined tactics deployed in the 2014 Ukrainian conflict accordingly: The first step involved protests against the government that led to administrative reform. Because Russia had been dissatisfied with that reform, it has occupied Crimea since the reforms became effective and has supported separatists by supplying them with firearms. The second step involved information warfare whereby the Russian media was used to justify aggression against Crimea. Martišius (2014), then, concluded that the goal of information warfare was influencing of a country's public opinion from both within and outside its geographical boundaries by systematically tailoring media messages.

Sanger and Erlanger (2014) claimed that the Russian government has deliberately used social media to wage information warfare. Moreover, they have identified several crucial preexisting contextual conditions, or what

they call historical conditions. The first of these is the infiltration of Russian secret services to governmental information and communication networks. This infiltration has been possible since 2013, when the Ukrainian government was based on the pro-Russian government majority led by Viktor Fedorovych Yanukovych, Putin's incumbent ally (Sanger & Erlanger, 2014). Yanukovych and Putin drafted a contingency plan that involved the destabilization of Crimea and other territories in southeastern Ukraine that were densely inhabited by a Russian-speaking population (UNIAN Information Agency, 2015).

Destabilization, in turn, involved reclaiming the Russian identity of local supporting groups while indoctrinating them with the belief that hatred toward Russians is a global phenomenon. Russians were prepared to embrace the so-called Russophobia campaign that projected Russians as victims of such hatred, particularly the animosity harbored by foreign nationals residing outside Russia. To lay the groundwork for this destabilization, a massive disinformation campaign was launched—a combination of physical warfare and cyber and informational attacks (Pasitselska, 2017; Snegovaya, 2015).

To uncover and prove the presence of information warfare, multiple pieces of evidence are needed to triangulate this complex phenomenon (Lysenko & Brooks, 2018). Such data triangulation provided evidence of physical entry points of covert Russian military operatives and the information centers in smaller Russian towns from which the massive flows of tailored messages were sent to the web—that is, by tracing the web brigades involved in information warfare. Specific information-driven warfare forms involved not only informational attacks but also media disinformation campaigns that replicated historical persuasion efforts to alter public perception. However, these campaigns relied heavily on new media outlets or large news operations. Iasiello (2017) described the tangible evidence of the cyberattack against Crimea accordingly: “[Russia] shut down the telecommunications, infrastructure, disabled major Ukrainian websites, and jammed the mobile phones of key Ukrainian officials before Russian forces entered the peninsula on March 2, 2014” (p. 54).

Crimea's case exemplifies, how Russia capitalized on Russophobia frame and the need to celebrate the resurgence of national identity. In fact, its preannexation, “state” propaganda is “a form of planned and long-term special operation, that employs techniques of manipulating information and elements of ‘manually controlling’ the general public” (Darczewska & Żochowski, 2015, p. 7). The chosen narrative purported that Russophobia victimizes Russians (who potentially lived in Ukraine) who were projected as victims—a powerful frame invoking the minority-majority issue that posi-

tions Russians as alleged minorities. The frame contrasts Russian dominance in the Soviet era with post-Soviet Russian marginalization, and it evokes nostalgia for Moscow, once the headquarters of the Soviet political apparatus. Thus, by minoritizing Russians, nostalgia for the former Soviet Union is evoked and Russia's loss of dominance over the Soviet republics becomes a point of historical emphasis.

Russophobia-based self-victimization frame exposed by Darczewska and Żochowski (2015) is interpreted to elicit from the receiver a categorical response (being a perceived victim of Russophobia); moreover, it is deemed to be accompanied by emotionally stimulating context that should make Russians feel like the world is against them. Such a Russophobia narrative was found to be wrapped around conspiracy theories. Thus, the Ukrainian propaganda campaign for spreading Russophobia was based on the conspiracy theories that exemplified the classical propaganda repurposed in the new media era. Darczewska and Żochowski (2015) described the phenomenon accordingly:

Russia's information campaigns are turning into battles waged with the language of aggression, excluding any possibility of dialogue or compromise. The arguments they present, which justify Russia's right to shape the international order, are intended to strengthen the belief within Russia itself that there can be no alternative to the measures the authorities are taking. The repertoire of actions taken is not sophisticated and is reminiscent of the methods used during the Cold War. According to Russian propaganda theorists, the key to success lies in the use of a few basic principles: large-scale and long-term operations; the repetition of simplified information which pushes the recipient into an "us and them" response; arousing the recipients' emotions; and alleging a certain "obviousness," referring to the Russian cultural code, an inseparable part of which involves clinging to the idea of empire. (p. 13)

Essentially, these propagandistic campaigns involved the repetition of easily digestible information. Such repetition recalls Darczewska and Żochowski's (2015) assessment of the construction and circulation of politico-historical narratives:

The conviction that the "Russian world" beyond Russia's borders has specific rights; that the rights of this Russian-speaking population are at stake; that there has been a "Russian spring," i.e. a patriotic

awakening of the nation; that “Banderites” (identified with fascists) are threatening the Russians and their neighbors; that the so-called ‘colour revolutions’ are the result of a conspiracy by the West against Russia, whereas Russian conservatism is a response to Western liberalism. According to the logic of “us and them,” this technique requires the construction of an image of the enemy (both external and internal). For example, these “enemies” include Poland—as “the US’s Trojan horse in the EU,” but also as supporters of Westernism in Russia—a fifth column, or extremists, which includes any and all critics of the authorities. The arsenal of slogans and stereotypes used is constantly being supplemented and updated, as are the methods of disseminating them. (p. 14)

When propagandistic narratives are constructed, they are deployed through various media forms and reinforced by the language used by official sources. In the case of Ukraine, Russia had to scale down the radicalism of the Russophobia frame to react to Kiev’s resistance. Thus, Ukraine has been represented in this propagandistic narrative as a Russophobic country. Politicians such as Putin have also reinforced the Russophobia narrative. In a 2014 interview covered in the story “Vladimir Putin: Support of Russophobia in Ukraine will lead to a catastrophe” (Вести Калмыкия, 2014), Putin himself emphasized that the West’s stoking of Russophobic sentiment in Ukraine could lead to disaster. The interview uses a discursive maneuver that becomes more fine-tuned when Ukraine is framed as part of Russia. An important element of this information strategy is expanding the notion of “domestic Russophobia” to Ukraine by insisting that Ukraine is and will remain a part of the “Russian world.”

Martišius (2014) summarized Russia’s propagandistic information control tactics during the 2014 Ukrainian crisis where the Russophobia self-victimization was exploited through false claims that were typically difficult to check and repeated in different forms. Examples of such false claims were that Kiev’s government had been taken over by *chunta*, the pro-fascist government, *benderovci*, who in eastern Ukraine kill Russian-speaking citizens. In addition, it claimed that these atrocious killings were orchestrated by the US and NATO member countries. No alternative positions were provided. The result of this campaign culminated in 2014, when Putin awarded 300 journalists for “the objective coverage of the events in the Kremlin” (Камышев & Болецкая, 2014, para. 1), even if those journalists reinforced the false sentiments of victimization and Russophobia. The report about the “awarded journalists” is covered in the Russian media—Vedomosti (Камышев & Болецкая, 2014).

Another way to create influence was by further exploiting mass media sources abroad. To deploy propaganda-based narratives, the Russian media were found to provide their version of the story to foreign correspondents, as reported by the German newspaper *Spiegel* in 2015. When considering news comments as sources of influence, a 2014 story in *The Guardian* reported complications involved in moderating news comment sections. Specifically, moderation was complicated by the discovery of orchestrated foreign pro-Russia campaigns behind stories covering the conflict in Ukraine (Elliott, 2014). The Polish government expressed similar concerns in the Polish edition of a *Newsweek* article by stating that pro-Russian sentiment was “heard” in stories regarding Ukraine in the Polish media (Olwert, 2014). These news stories prove that the targeted management of opinion and its widespread reach exceeds a single region and have expanded to influence outside Russia. Furthermore, these stories exemplify how Russian trolling—which can be considered a “rehearsal” for the Kremlin’s internal propaganda orchestration—resonated directly with the foreign press as well.

The resurgence of information warfare in Russia can be considered attempts to influence Western nations, in addition to Ukraine. The third period discussed here includes the territories that have been designated as Western democracies. The 30 May 2014 *Spiegel* article “How Is Russia Winning the Propaganda War” underscored the significance of Russia’s information warfare campaigns by quoting these numbers: “The Kremlin invests around €100 million (\$136 million) a year in Russian media abroad in order to influence public opinion in the West” (para. 9).

Moreover, Szulecki (2018) claimed: “While old propaganda was merely about crudely promoting the Kremlin’s agenda, the new ‘information warfare’ is ‘calibrated to confuse, befuddle, and distract” (p. 324). According to this assertion, current Russian propaganda tactics attempt to subvert rather than clarify. The physical power demonstration has been coupled with soft power.

Victim-Playing Russian Trolls in the News Comments

How are Russophobia frames reflected in comments responding to US news stories related in any way to Russian trolling? The complete absence of such frames is expected, since there is no real urgency to defend Russians in US media sources. By logical extension, there is no need for US comments justifying Russian trolls in the US. Yet the Russophobia frame, claiming Russian trolls as an alleged victims, was present in all three analyzed US media sources and in one Lithuanian case. Specifically, these US sources are the

politically conservative *Breitbart* and Gab, and the comparatively liberal *New York Times*. Forms and uses for these argument frames having been identified in the news comments, and the frames can be categorized according to these three terms: mockery, provocation, and deflection.

Russian Trolls as Treated Unfairly

According to the freedom-of-speech argument, Russian trolls are perpetually being subjected to unfair treatment. On *Breitbart*, other users contributed to the discourse of Russian trolling denial by insisting that Russian trolls be protected by the First Amendment.

Breitbart Story 9, Example 1

So no 1st amendment for Russian trolls but ok for fake news?

This rhetorical question constructs an unbalanced equation between two things: Russian trolls and fake news. Others evoked alleged free speech rights of Russian trolls:

Breitbart Story 6, Example 1

Indicted yes . . . convicted No..... Even Russians have free speech in America. I haven;t heard of any real crimes other than being internet trolls. Most companies do media monitoring and use fake Facebook and disquis commentators to advance marketing to advance sales. This is smoke and mirrors. If they were Soros financed superpacs then it would all be legal..... Propaganda is LEGAL in America . . . Just look at CNN, MSNBC, and WAPO.

This comment also exemplifies false equivalence to justify Russian trolls. In this instance, the commenter compares them to US residents in general, including those who staff left-leaning media outlets. Through such false equivalence, the commenter attempts to establish a rapport or affiliation with *Breitbart* readers, who are already predisposed to be critical of the left-leaning media. Such rapport is projected through the commenter's invitation to endorse the idea that Russian trolls deserve the right of free speech in the US. Yet another comment called such a demand of freedom of speech for Russian trolls.

In fact, several Gab users insinuate that the Russian trolling narrative is used to censor the online public sphere:

Gab Example 1

User Jon: Better reject social media censorship with extreme prejudice. The “Russian meddling” bs is nothing but an excuse to censor Americans. Russians have been meddling in elections for decades. So has America. Obama blatantly interfered in Israel & Ukraine’s elections. The “Arab Spring” was pretty much caused 100% by Facebook & Twitter trolls. Stop tolerating the fascist double standards of liberals.

Others expressed being unfairly victimized:

Breitbart Story 11, Example 1

One of my friends got banned for re-posting a “Bad lip reading” from Hillary Clinton during the debates.

Apparently one-sided comedy will get you banned too?

This comment is based on the argument that freedom of speech is denied to Russian trolls and conservatives. Thus, the commenter insinuates that these social groups are subjected to similar forms of oppression.

Russian Trolls as an Authentic Opposition

According to “authentic opposition” arguments, all controversial posts are genuine and are not textual indicators of Russian trolling at work. Claims that Russian trolls are merely opposition members proliferated throughout online spaces. Specifically, *Breitbart* commenters provided personal stories of being censored in online spaces, despite their claims to user authenticity. Thus, through such personal accounts, they demonstrated their support for Russian trolls.

On Gab, the “treated unfairly” argument was implied by comments complaining that anyone can be falsely accused of being a Russian troll. Such complainants resort to mockery when they propose a Russian troll “test.”

Gab Example 2

Gab example: Self Test yourself to see if you're #Russian Troll (/hash/RussianTroll) and didn't know it! 🤪🤪🤪🤪 (https://www.zerohedge.com/news/2018-02-26/are-you-russian-troll) SCORING: Give yourself one point for each (a), two points for each (b), three points for each (c), and four points for each (d). 7-10 points: America. Love it or leave it. 11-15 points: Both sides were equally to blame for the Cold War.

This comment justifies Russian trolls, or at least shows solidarity with them through the mockery that diminishes the seriousness of the trolling issue. Additionally, even if the link is not accessible, the comment's frivolous game proposal is positioned to delegitimize Russian trolling investigations.

Similarly, Russian trolls were also positioned as victims by claiming that those with oppositional opinions are accused of being Russian trolls:

Gab Example 3

Gab example: #NeoconDon (/hash/NeoconDon) has effectively made US Air Force wings of ISIS / Al Qaeda. If you oppose bombing people who are fighting terrorism, you are Russian troll / Anti-semitic. Burger "nationalists" have drowned in swamp. You know it is so when Chuck Schumer praises Drumpf for attack on #Syria (/hash/Syria). #GoodGoyTrump (/hash/GoodGoyTrump)

This comment provoked the following responses that call out such comments as being written by Russian trolls:

Gab Example 4

Response Didmos: I am surprised how many people are finding excuses to defend this event. It seems like any reasonable person would have to admit the obvious.

Response Xazzy: I suppose.....it sounds more mach. . . . to say: We're fighting the Russians. . . . than it does to say: We just smacked a tiny, poor country, desperately fighting ISIS rebels. . . . Rebels who started all of this BS in the first place . . .

Response Wyatt: Russian Troll Alert!

While the second comment in the series refers to the Islamic State and Syria, the third exemplifies a Russian troll callout.

Gab Example 5

Gab user /pol/: Automatically assuming that anyone calling you an NPC is just a Russian troll is probably one of the most NPC responses you can have. Way to prove the point.

Gab user /pol/ lamented that Russian trolling has been used to describe mere opposition. By refuting the conservative accusation that only Russian trolls could possibly object to non-politically-correct language and making reference to /pol/, a politically incorrect thread on 4chan, this commenter insinuates that Russian trolls are perpetually being stigmatized.

The *New York Times* comments also endorse the authentic opposition argument as follows:

New York Times Story 5, Example 1



New York September 21, 2018

So anyone who disagrees with your views or uses an argument which you don't want to hear is a troll? Let's hope the real troll spotters do better than that.

The comment alludes to the fact that disagreement does not necessarily indicate the presence of Russian trolls. At the same time, it also implies that it is difficult to confirm their presence. Another user posted a similar argument:

New York Times Story 1, example 1



New York Aug. 24

Suppose the Russians start to post pro and con messages on e cigarettes, seatbelts, home schooling, school admissions tests, low income multifamily housing, or about a million other things? All they are doing is joining a million other voices on every possible side of every argument. Every time we react as if these messages are "tearing us apart." As if the same messages from Indiana or Texas or Canada or India for that matter are ho hum who cares. But if they're traced to some Russian, it's hair on fire time. Can we please just accept that messages we like or don't like / agree or disagree with can come from anywhere in the planet and stop letting them drive us crazy?

Other users responded to the comment accordingly:

██████████

Novosibirsk, Russia Aug. 24

You probably did not read the writings of Dr. Goebbels. In his books it is proved that the Russians are guilty of all the woes of mankind for the last thousand years. The first thing that should be instilled in every child in a civilized country is the Russian enemies of civilization. Russia - Mordor. I hope that you will read *The New York Times* more, and your doubts will disappear.

Similarly, another user added:

██████████

Toronto Aug. 24

██████████ completely missing the point; it's like watching an argument and then saying "hey you two should start fighting"—then imagine feeling the need to say that from the other side of the planet . . .

Implicit in these comments is the assumption that the practice of online commenting differs from foreign influence. Similar arguments against suppressed authentic opposition appeared in Delfi.lt, where the democratic premises of news portals were questioned. The following commenter resorted to victimization, of being wrongly accused as a Russian troll, despite innocent attempts to express "authentic opinions."

Delfi.lt Example by Registered Users 1

Headline: Dictatorship established?

Comment: If you try to say something negative about immigrants, then you will be called a troll? I cannot believe that the Finnish government has sunk so low.

The user lamented that the suppression of "authentic opinions" is a form of dictatorship, implying that the premises of democratic inclusion are absent in Lithuania. Moreover, the reference to Finland alludes to the article to which the comment was first appended. That article reports the Finnish government's initiation of a court case against pro-Russian trolls who had persecuted a reporter. The comment also refers to immigration as a sensitive issue in Lithuania, or the "crack in the society." The reference here is loaded, considering that throughout the previous several years, numerous citizens

have emigrated from Lithuania and specific immigration patterns are identifiable for Lithuania, as well as for other European countries, particularly in the wake of the Syrian crisis. Thus, this loaded reference can be read as a rhetorical strategy for refuting the rationale behind trolling accusations—in this case, specifically, the user's "legitimate critique" of important Lithuanian sociopolitical issues that threaten to expose the cracks in Lithuania's social edifice.

Yet other users argued that their opinions about "pro-Russian" issues should be respected as mere democratic expressions—the argument's rationale being that freedom of speech is prohibited in Russia.

Delfi.lt Example by Anonymous Users 1

Headline: Wow

Comment: This is an example of censorship in a so-called democracy, these are the first political victims. This is what you call freedom of speech in the western world.

Response Headline: A pig

Response Comment: How can you, Russians, be not ashamed to speak about freedom of speech?;D When in Russia there is only one truth, either you suck to putler [Author's note: reference to the president of Russia Putin] or you are the enemy of the government;D

Headline: To the Savushkin office [Author's note: reference to the Russian troll farm that had been uncovered in St. Petersburg on Savushkin Street reported by Chen (2015).]

Comment: What will respond to that, cotton [Author's note: cotton is reference to the cotton coats used by pro-Russian militants.]

This thread exemplifies a pro-Russia stance through the implication that trolling is a form of free speech requiring protection. Additionally, the thread alludes to the failed promise of Western democracies to protect free speech.

Other users responded to the arguments that Russian trolls should be granted the freedom of speech by providing a rebuttal. This rebuttal states that Russian trolls' comments are orchestrated by Russia rather than mere opinions:

Delfi.lt Example by Anonymous Users 2

Headline: A pig

Comment: Opinion, what kind of opinion is that when Russia lies 24 hours a day?;D Here trolls simply repeat this kremlin's "truth" and they call this opinion freedom of speech, this is a complete nonsense;D

Delegitimization Rhetoric

Another set of arguments deriving from Russophobia frames are aimed at delegitimizing Russian trolling as an issue. The rhetorical act of delegitimizing here show how Russian trolling as a topic was being nullified. These arguments included denial of Russian trolling as an actual phenomenon. Such forms of denial, whether or not they were accompanied by supporting statements, were found across news portal comment spaces. They involved the following frames: “It could not have happened” frame used at face value; “it could not have happened” frame used for mockery of investigation; “Russian trolls are merely internet trolls”; “Russian trolls did not affect results”; “There is no evidence”; “It is legal to troll”; “Russian trolls do not exist”; and “Nobody even reads these posts.”

As mentioned earlier, such delegitimization techniques are typically deployed by authoritarian regimes to secure information control. Yet they had been successfully implemented in the media in the US and in Lithuania—not in the mass media stories themselves, but within their peripheral spaces, specifically in the comment sections that publicize a general readership’s bona fide opinions.

Disbelief

The disbelief argument exemplifies denial of the Russian trolling phenomenon. This argument supports all other frames because it is prototypical: It resorts to denial while attempting to divert attention from Russian trolling as a potential subject of contention. Specific statements to advance the argument employ the “it could not have happened” frame, appropriated at face value or to mock Russian trolling investigations.

The following *Breitbart* comment exemplifies the justification of Russian trolls.

Breitbart Story 9, Example 2

Apparently trolling social media and fake news is fine as long as it’s done by anyone except Russians. Where’s the evidence that anyone was influenced by these Russians? There is none. We were being bombarded by this same kind of stuff by American trolls and U.S. media every single day but we’re suppose to believe 13 Russians were more influential than the many millions of Americans on social media and our multi-billion dollar media industry? I don’t think any sane person is buying that.

This example, like many others, implies that Russian trolls have the right to free speech, and that they are being treated unfairly by being denied that right. Additionally, this comment denies the possibility of foreign influence.

Several Gab commenters mocked the idea of the existence of Russian trolling by implying that Russian trolling is a mere hoax sprung upon gullible users.

Gab Example 6

Maga news user: LOL! Russian troll! FaReal!

You have reached the Russian embassy. To arrange a call from a Russian diplomat to your political opponents, press one. <https://www.yiannopoulos.net/2017/04/russian-voicemail/> #MAGA

The Gab example above implies that Russian trolls are simply a hoax. However, it links to an inaccessible link. Yet another user defended Russian trolls by quipping that scientists cannot determine who is a troll online by citing Russia Today, Russia's state affiliated media source:

Gab Example 7

So what scientific criteria did NBC employ to find these "Russian" bots? Did they look for specific terms or references to vodka or Borscht? Nope Here's one that tipped them off "Donald Trump has huge support from women" but "the media will never show this." Clearly Russian #FAKEnews #NBC #NationallyBroadcastCommunism <https://www.rt.com/news/418828-nbc-russian-trolls-tweets/>

This comment defends Russian trolls by questioning scientific approach by attacking news outlets that report on Russian trolling, despite the absence of supporting evidence for the phenomenon.

New York Times commenters also resorted to "no evidence" arguments or to the "it could not have happened" denial frame to justify Russian trolling.

New York Times Story 7, Example 1

██████████ Philadelphia, PA Feb. 21, 2018

Douthat is assuming that those 78,000 swing voters in the Midwest were too sophisticated and nuanced to be swayed by the Russian trollings. There is no evidence presented here by him to justify such an assumption. Thus the invalidity of his argument here. We see this time and again from GOP apologists, the logical fallacy that the majority of Republican voters and

congressmen are really decent people-- they are not, nor should they be considered as such, most especially in the current incarnation of the Trump criminalized GOP.

Similar arguments based upon the premise that Russian trolling could not have influenced elections were found on Gab. While some users have accepted the idea that Russian trolls exist, they were unable to provoke controversy on Gab because they are greatly outnumbered by opponents of that belief.

Gab Example 8

User Longy: It was the Russians tho <https://order-order.com/2018/02/08/just-49-russian-twitter-trolls-sent-only-942-tweets-during-referendum/>

Response: Happy: Igor made me vote leave.

User Deep: Imagine my shock the commie bastards blame anyone but them selfs. Muh Russia

This comment implies that Russian trolls are victims of scapegoating. It also argues that hostility toward an entire nation is absurd in instances where only a negligible minority of individuals are found to have acted on behalf of their government, thus the evidence is not worthy.

An example of a no-evidence argument, attempting to deflect attention from Russian trolling to “it is us” introspection, has also been identified in the *New York Times*.

New York Times Story 6, Example 1

■ Cincinnati Nov. 13

Let’s put this in perspective to the disinformation campaign promulgated on the American electorate by the billions of dollars spent by our political organizations, PACS, SuperPACS, something ominously called “dark money” and of course don’t forget our oligarchs and corporations. And let’s not forget the free air time, billions of dollars worth, that the media companies gave to Trump. It is well documented that the media companies ignored the Sanders campaign and instead showed empty podiums of Trump. Did the Russians do all this? Did the Russians cancel Hillary Clinton’s flight to Wisconsin? Do the Russians try to mess with elections around the world? Oh course, just like WE do. Polls show that this whole Russian thing is a joke with less than 1% of the American public who care less about it. Why? Because they know full well that compared to what Citizen’s United has done to our election system, the Russians are rank amateurs compared to our oligarchs and corporations.

Partial Dismissal

Russian trolls were further justified through arguments starting with the conditional clause “if they exist,” and concluding with these statements of dismissal through arguments such as “Russian trolls are merely internet trolls,” “Russian trolls did not affect results,” “It is legal to troll,” and “Nobody even reads these posts.”

The goal of dismissal is to generate the conviction that Russian trolls are unworthy of public notice, even if they actually exist. Thus, while the outlined statements of dismissal acknowledge the possibility that Russian trolls exist, they diminish the gravity of the Russian trolling problem itself. The following comments exemplify the first dismissive rationale: “They are merely internet trolls.” In fact, one user defended the Russian trolling phenomenon by dismissively stating, “It is just trolling.”

Breitbart Story 6, Example 2

So, they were basically doing what any internet troll does on a daily basis, except “THEY WERE RUSSIANS”!! Hey, what about Hillary’s favorite villains, the “Macedonian Content Farmers”? And, those devious RUSSIANS, were supporting Trump AND Sanders! sheesh! To use a very well worn phrase - BIGGEST NOTHING-BURGER EVER!!!

Other *Breitbart* commenters denied the existence of Russian trolls.

Breitbart Story 11, Example 2

Yeah, a bunch of Russian trolls posting borrrish stuff on FaceBook “are responsible for Trump winning the election”! Seems you are not quite bright! LOL

Yet others argued that because there are only “a few” Russian trolls, the amount of influence they could possibly exercise is insignificant.

Breitbart Story 6, Example 3

So basically Mueller found a few Russian trolls. LOL

Russian trolling denial also assumed the form of mockery while implying that Russian trolls do not exist.

Breitbart Story 15, Example 1

They “meddled” lol. 13 Russian trolls. I mean seriously, who would have ever guessed the existence of Internet trolls.

The internet trolling indicator “lol” in all three comments mocks the seriousness of Russian trolling investigations.

Other users posted comments that discredited the possibility of Russian influence.

Breitbart Story 8, Example 1

WHAT?! THESE are the type of tweets that supposedly reek of Russian POLITICAL influence? Is this a sick joke? Or something far more sinister.....

Yet others attempted to instill doubt by claiming that anyone could have financed Russian trolling operations.

Breitbart Story 8, Example 3

Putin’s right. The 13 trolls aren’t connected to the Russian govt, and they could have been paid for by anyone, including the DNC.

Other comments defended Russian trolling through the implication that lack of accountability invalidates it as a legitimate concern.

Breitbart Story 7, Example 1

Russia is a very large country with way over a 100 mil population, could you be a bit more specific? was it Putin, a Russian government agency, or Russian individuals that the 18 US agencies beyond doubt knew were interfering. Please don’t say Putin knows everything that happens in Russia that’s so old and stupid.

Others cited lack of evidence for Russian trolling.

Breitbart Story 12, Example 1

Has there been any proof released to the public that the 13 Russian trolls on twitter were in any way connected to the Kremlin?

Yet others argued that Russian trolling does not qualify as criminal activity.

Breitbart Story 9, Example 3

If being a troll is a crime their a lot of people in trouble. If you try to dissuade your spouse from voting for an idiot is that a crime too? There are a lot of political meddlers in a lot of trouble now aren't there? I think Bob needs to start arresting politicians for political advertisements trying to interfere with the vote.

Others trivialized Russian trolling as yet another variation of internet trolling.

Breitbart Story 9, Example 4

Ludicrous. . . . how many international Trolls are on Facebook or other Social Media? Millions i would have to assume. Are they all going to be indicted for buying ads on FB? Mueller is setting up his 2nd Retirement plan. "Infinite Indictments."

Gab users resorted to face-value denial of Russian trolling ("Since I do not see them, they do not exist"). Furthermore, the user implies that Russian trolling is an excuse for government surveillance:

Gab Example 9

Jam: Where are the "online Russian trolls" we keep hearing so much about from the Dems?? I'm always online, I've never seen them?! Yet, Obama & FBI now say that was an excuse to spy on our social media accounts on election night?! We have a right to know who they spied on! "Big" DM friends get us [detective head emoji]?? BS!

A *New York Times* user resorting to the "no evidence" argument that in turn promotes the idea that Russian trolling could not have occurred.

New York Times Story 6, Example 2

■ NYC Nov. 13

**But as of Nov. 13th 2018, we've never seen any proof of these claims that Russia interfered in the US2016 election.
It's always half truths and conflation.**

The same user repeated this claim in different terms in a later post.

New York Times Story 6, Example 1

■ NYC Nov. 13

Sorry, there's no evidence the Russian state funds the Internet Research Agency.

So more fake news in this video.

By degrading social media as providers of not serious media outlets, several users diminished the gravity of potential consequences of interference.

New York Times Story 1, Example 2

■ ma Dec. 18, 2017

We're supposed to be worried about how Russia monitors social media? Good grief. As if we don't have enough problems within our own country these days. What about all of the IS propaganda videos and memes and recruitment websites? Now there's a real worry. Can those be taken down as well?

Several users posted comments that underestimated the persuasive impact of online messages to claim that Russian trolls could not have influenced elections.

New York Times Story 1, Example 3

■ House Aug. 24

It's an interesting approach by the Russians to use views toward Vaccines to sway the election. Yet, I'm curious, did anyone ever actually read these tweets?

Another user also expressed skepticism about Russian trolling in response to a different *New York Times* story. In fact, some users went to great lengths to legitimize foreign interference to imply that public focus should be deflected from the Russian trolling debate.

New York Times Story 4, Example 1

■ United States Nov. 7

The Federal Election Campaign Act allow foreign nationals to participate in U.S. political campaigns as long as they are not paid and don't make illegal campaign donations. They can, and do, work as campaign volunteers. They can organize campaign rallies make campaign speeches and post opinions on social media without violating federal election campaign laws. It is not

unlawful for foreign governments to attempted to influence U.S. election. Most countries that feel they are affected by U.S. foreign policy, which is to say most countries, attempt to influence U.S. election. During the 2016 election, Putin said complimentary things about Trump, but the president of Mexico compared Trump to Hitler. Both were attempts to influence the election. It's legal as long as the methods are legal.

Yet other users argued that Russian trolling should not be the focus of public attention any more than it had been in the past. Thus, the seriousness of the issue was diminished.

New York Times Story 6, Example 3

██████ Beloit WI Nov. 13

Russians/Soviets did and do what they do. There is nothing new in that. The Left urged us for decades to be forgiving and understanding of Moscow's work. What changed to suddenly be so shocked about something that has been going on for almost a hundred years.

News portal comments throughout 2018 in the US media and in Lithuanian media comments throughout 2016 demonstrate that the Russophobia frame proliferates. Victim playing is part of that frame—a rhetorical maneuver in which the speaker asserts that “Russians are blamed for everything,” “Russian trolling does not exist,” or “Russian trolling did not influence the election.” Other arguments suggested that Russian trolls are blamed unfairly since they merely represent an authentic opposition. Specifically, Russian trolls were portrayed as victims who are deprived of access to an online public sphere, which allegedly constitutes an infringement of free speech, and Russian trolls are treated unfairly. Some users expressed solidarity with Russian trolls (when users include themselves in the “deprived of a public sphere unfairly” category: “we have all been unfairly treated”). Other arguments included claims that Russian trolls were not actually Russian trolls but represent an authentic opposition. Russian trolls have been victimized; they are “blamed for everything.” Finally, victim-playing arguments included claims that censoring Russian trolls is an attack on democracy.

Zero-Sum Game

Zero-sum game can be illustrated with the quote “bad people are on both sides,” used to justify Russian trolling. In multiple instances users justified Russian trolls by arguing that there are also others who may be held account-

able for negative behaviors. This argument is similar to the complaint “Russians are faulted for everything.” The rhetorical maneuver of blaming “both sides” is also viewable as a zero-sum game involving the false equivalence of two things that cannot be compared. Within Lithuanian rhetorical contexts, the zero-sum game was identified in a discussion thread that constructed a false equivalence between trolls and elves (elves here referred to a grassroots initiative in Lithuania where online users expose Russian trolls, discussed in Chapter 3). Specifically, the negative traits of Russian trolls have also been ascribed to elves, whose objective is to counteract those very trolls. In Delfi.lt, for instance, the zero-sum game lumped Russian trolls and Lithuanian elves in the same category of cyberoffenders.

Delfi.lt Example by Registered Users 2

Headline: Ace

Comment: They deserve it. The time will come when we will put trolls and elves into jail. There is no difference between them. They use swear words, they threaten, and accuse each other. That’s the level that we have reached.

This commenter applied the same judgment lens to both Russian trolls and elves, and in so doing, trivialized both as “impolite” users, who are merely expressing “personal opinions.” Thus, online incivility is their sole offense. Furthermore, by dismissing the information warfare frame, the commenter represents a set of users who downplay the relevance of online discourse.

Both the “zero-sum” and “mirroring sides” games have the propensity for advancing online chaos. Specifically, the “mirroring sides” guilt game creates a frame of attack by appropriating the very same defense mechanisms of the attacked. So, for instance, if Russian trolls are accused of being paid for exercising influence, the same mirroring argument is applied when referring to “left-wing trolls.” This opponent blame game has been played out in debates concerning partisan issues or in attacks on the media.

Russian trolls were also defended through their comparison with paid Soros trolls. User comment samples from *Breitbart* criticized political opponents by implying that, because “Soros trolls” are paid, it is not at all unusual—in fact, it is even OK for Russian trolls to serve as paid operatives. Such comments ultimately legitimize Russian trolling.

Breitbart Story 15, Example 2

Take note PAID SOROS TROLLS: you can be indicted.

Some users implied that, like Russian trolls, Soros trolls can also be called out.

Breitbart Story 15, Example 3

Great ASCII Art. I usually just post: Warning: Soros Shill Detected. Every post he/she/it creates earns 25-cents. Starve the Soros Troll®.

Yet others adopted the self-victimization frame by implying that Russian trolls are unfairly selected scapegoats.

Breitbart Story 15, Example 4

Why were Russia's trolls so much better than, say, Soros's trolls?

These comments are readable as defenses of Russian trolling. Such justifications of the phenomenon through the equation of Russian trolls with other types of oppositional trolls, in turn, imply the use of conspiracy theories to deflect attention from the Russian troll interference problem to unverifiable rumors about George Soros.

Yet other users provided a similar “shared responsibility” argument that can be encapsulated in statements, such as, “It was also Americans, not only Russians [who could have been held accountable].”

New York Times Story 7, Example 2

██████████ Feb. 22, 2018

I think any rational person would agree that the Russians alone didn't get Trump elected. Plenty of Americans arrived at the decision to vote for the former host of *The Apprentice* on their own. But what Douhat seems to be doing is making an argument against a stance that few actually hold. It isn't fake news that the Russians tried to influence the election. We just don't know how much impact, if any, their efforts had on the election.

This comment also advocates that “both sides” (Russians and Americans) are equally blameworthy and shoulder a shared responsibility. Such arguments diminish the burden of responsibility for foreign governments while obscuring the role that they play in international politics. It can also function as zero-sum game where no one is responsible.

The “bad people on both sides” argument is not unique to Russian troll denial, which makes it potentially more acceptable by the general public.

Politicians have used this argument to delegitimize or diminish the gravity of issues. For instance, former US president Trump resorted to such delegitimization when he justified the gravity of a mass shooting in El Paso, Texas, through the false equivalency underlying the “bad people on both sides” argument reported by Graham (2019). Additionally, when an interviewer asked Vladimir Putin why so many of his critics die, he attributed those deaths to Russia’s high crime rate. Putin then cited John F. Kennedy’s assassination and clashes between police and civilians to counterargue that the US is also struggling with its own high crime rates, thus evoking the idea of “bad people exist everywhere” argument (Associated Press, 2018).

Mockery

Mockery can be used to exploit classical trolling as a form of delegitimization or by attacking opponents without presenting any rational argument. Delegitimization techniques have been deployed in response to topics such as Russian trolling by diverting attention from the main subject of ongoing arguments to something else. The techniques have also been used to attack institutions that are typically considered expertise-based spaces that cannot be questioned or delegitimized. In the case of classical “trolling,” however, mockery and attack become legitimate techniques of rhetorical violence.

The subtler forms of ironic mockery were observed in sarcastic jokes that treated Russian trolling as an occasion for wordplay. This comment exemplifies that type of sarcastic wordplay:

Breitbart Story 9, Example 5

Anyway, what exactly is a “troll farm.” Is it political agriculture?;-)

Mockery was involved in arguments that are geared to discredit FBI work (e.g., in a comment that FBI agents had found “only” a handful of trolls) or to delegitimize media institution credibility. Yet another news story comment invoked “Russians trolls” to mock institutions like the FBI, geared to invalidate Russian trolling as a serious threat.

Breitbart Story 6, Example 4

The FBI’s motto should be “when in doubt.. blame the Russians” Can’t stop a school shooting despite numerous tips?? No problem! Indict some more Russian trolls!!

The idea of “blaming Russians” implies the innocence of Russian trolls and their unfair treatment.

While diminishing an overall seriousness of a message, such jokes threaten to delegitimize the issue at hand. Moreover, such mockery tactics can always be rationalized as “witty trolling.”

Provocation

The “it could not have happened” argument has been used to exploit internet trolling by challenging the validity of a given rational argument. Challenging the validity of a given issue, two rhetorical maneuvers were found in the comments. The first of these involved the use of logic, whereby conditions were posited for explaining why trolling presumably could not have happened. Yet such arguments were arbitrary and at times guilty of false equivalency in the process of justifying Russian trolling. The second maneuver involved the use of examples when there was no clear counterargument. This later approach merely challenged the validity of Russian trolling allegations. And numerous times, such a rejection of Russian trolling as something that has happened or is happening served as an alternative opinion. Russian troll justification comments with no rational explanation other than a blunt rejection of Russian trolling existence typically received some backlash or comments from other users.

Hence, such nonrational delegitimization arguments resorted to techniques typically attributed to internet trolling, whereby the rhetorical goal is to provoke strong reactions and to move conversations into vicious circles that disrupt internet communities. In other words, the goal is to introduce division within communities rather than contribute toward their growth, as observed in studies on online trolling (see Herring et al., 2002). Consequently, such instances of internet trolling functioned as provocations rather than statements. In such cases, the goal could be the implication of others or the perpetuation of the rejection of Russian trolling existence frame without any specific counterargument. This specific tactic of provocation appeals to systems of values or beliefs, as it convinces comment readers that Russian trolls never existed, without providing any supporting facts for the assertion. While some arguments can include some semblance of facts, others are entirely based on unquestioned belief systems. Thus, such belief-dependent arguments are dogmatic and target “believers”—those who would endorse a cause despite its absence of supporting logic.

Deflection

Legitimate forms of opposition were mimicked to claim that Russian trolls are victims because they are denied the right to free speech. Arguments related to their Russophobia-based unfair treatment or victimization fall under the rubric of deflection tactics that shift attention from Russian trolling to other issues. Thus, denial of Russian trolling assumes the form of deflective arguments that exploit controversial topics that typically elicit divergent partisan or individual reactions—given that such topics represent “cracks” in societies. Such topics were used as rhetorical bait to enable digression from the main issue of Russian trolling and were frequently accompanied by self-legitimization. This rhetorical process is based on the concept of authentic opposition, for which multiple examples specifying points of deflection will follow.

Authentic opposition involves agreement with the claim that Russian trolls do not exist and that other social groups, such as Republicans, have also been treated unfairly or shunned from discursive participation in specific online forums. The victimization of these groups is related to the appeal to sympathy for Russian trolls as Russophobia victims, as discussed earlier. In fact, Russophobia-based Russian trolling denial is read in victimizing statements, such as “We are falsely attacked.” Variations of this statement recur in messages claiming that Russian trolls are being “falsely” accused or blamed for “everything,” including the problem of Russian trolling itself. This frame that was identified across news portals—ranging from *Delfi.lt* to *Breitbart* and *Gab*—was couched in the language of alt-right ideology but with the intention of “defending” freedom of speech for Russians. Representations of Russian trolls as victims have been found across analyzed news stories and other analyzed media sources. In *Breitbart*, for example, Russian trolls have been represented as scapegoats.

Breitbart Story 5, Example 1

Wow Russian trolls are being blamed for everything today, I think people didn't like the movie because of it overly feminist political views.

Another Russian troll denial frame uncovered in the news comments involved the exploitation of cracks in the edifice of “democracy.” Such exploitation was based on the assertion that freedom of expression is a major tenet of democracy. However, this assertion does not consider the paradoxical possibility that Russian trolling interference in democratic debates can-

not exemplify democratic free speech because such interference is excluded from democracy's discursive parameters. In other words, Russian trolling is an influence technique that subverts democracies—a phenomenon that emerges from authoritarian regimes, such as the current one in Russia.

Other users included irony in their comments to delegitimize the seriousness of Russian trolling. This rhetorical maneuver decontextualizes Russian trolling, as the following comment exemplifies:

Breitbart Story 5, Example 2

Russian Trolls ate my PhD thesis. Ivan and Boris just laught at me.

This example illustrates the irony that is typically used in online trolling—particularly in instances when the act of trolling targets internet users who have unconditional faith in the existence of Russian trolls. In this case, trolling, in the guise of mockery, attempts to delegitimize the seriousness of the Russian trolling phenomenon and its consequences. Such efforts, in turn, validate the phenomenon.

On Gab, a comment parodying a *Star Wars* movie review implied that Russian trolls are worldwide scapegoats “blamed for everything.”

Gab Example 10:

How to hide the fact that your SJW movie was bad propaganda and bored audiences? Blame the Russians (LOL) <https://www.radiotimes.com/tv/sci-fi/russian-trolls-blamed-for-perpetuating-star-wars-the-last-jedi-abuse/>@AlaskaNews

Again, this sample comment implies that Russian trolling should not be taken seriously. The “blame it on Russians” rhetorical trope included a range of associated unrelated topics, especially on Gab. Some of them resonated with alt-right political issues, beyond the US contexts. One of these was Brexit:

Gab Example 11

Someone said #brexit was a result of Russian trolls the other day. Like, woops, PutinLover69420 made me vote to leave!!!

According to this Brexit frame, the denial of Russian trolling is an impossibility, based upon the assumption influence does not exist. Thus, a fallacy

emerges—one that purports that Russian trolls cannot make someone vote and therefore cannot be blamed. These syllogistic premises are misleading because the main issue at stake here is public influence rather than voting.

The “Russian trolls are blamed for everything” trope functioned as yet another frame of reference in the *New York Times*, as revealed in the news story comments of several users.

New York Times Story 7, Example 3

██████████

NYC Feb. 21, 2018

Russian trolls as bad as the sneak attack on Pearl Harbor? A bit of a stretch. Russia hacked the DNC? Somebody hacked the DNC. What is rarely reported was the content of what was hacked. To wit : Clinton was undermining Sanders. The leaked info would help Sanders out: Russia wouldn't benefit. Lately, the word Russia has turned into an all purpose excuse as to why the US is failing. Everything is Russia's fault. Soon our CIA may obliterate Moscow and Clinton will run again and lose. Case closed : everything is not Russia's fault.

“Everything is Russia's fault” is a refrain in this comment, which concludes with the unambiguous conclusion of the opposite—that Russia is allegedly victimized. Additionally, this comment alludes to the absence of a culprit who can be held accountable for the failures of the US. Thus, it attempts not only to discredit the existence of Russian trolling but also to project a critical view of potential domestic issues confronting the US. This implicit appeal to introspection—to “look inside” (instead of judging others), projected through such a rhetorical pathos, can be a powerful deflection strategy. Since *New York Times* readers are expected to appreciate calls to introspection, this strategy would be effective for that particular news readership.

Other comments projected political divisiveness by stating that liberals are exploiting the Russian trolling frame.

Gab Example 12

Gab example: Jam (donor): Why is it okay to hate on all Russians now just because 13 troll losers were working to help loser Hillary? Yet Islam not to blame when certain attackers keep screaming that it is? Uh..huh . . . sure.

Similarly, other users blamed on liberals for Russian trolling:

Gab Example 13

Vlad: Observe their goal: to complete the alt-right movement with Russia. From this quote: “The likely objective of these measures is increasing media coverage of the fandom conflict, thereby adding to and further propagating a narrative of widespread discord and dysfunction in American society Persuading voters of this narrative remain a strategic goal of the U.S. alt-right movement, as well as the Russian Federation.”

Gary: The Russians are convenient fodder for liberals to blame everything that doesn't go their way. Fairly predictable.

By implying that liberals have scapegoated Russians, user “Gary” delegitimizes Russian trolling as a serious issue for debate.

Other users have provided their own stories about how they had been treated poorly—for instance, how their rights had been denied.

Breitbart Story 11, Example 3

I was banned for posting a picture of my MAGA hats! Those cyber terrorists must be shut down and arrested! MAGA!!!

Examples in this section of “Russian trolls as falsely accused” reflect how the Russophobia frame was found to be prevalent across news portals. It includes the rhetoric of victimization that internet users adopt in claims that Russian trolls were not actually Russian trolls but members of an authentic opposition. This frame is related to the conviction that Russian trolls are victims of unfair treatment. Such victim playing among right-wing users is discernible in statements like “We are falsely accused of being Russian trolls, but we are not.” Use of this rhetorical strategy is also implied by comments like “We are merely an authentic opposition,” or “Russian trolls are treated unfairly. As victims of censorship, they are denied freedom of speech (or access to other rights that democracy guarantees).” Moreover, self-victimization rhetoric is evident in “zero-sum” arguments between Russian trolls and their opponents (e.g., Lithuanian elves).

Within the Russophobia frame in such comments, it has been argued that the right to freedom of speech should be extended to include Russian trolls. Yet another argument emerged from claims that Russian trolls have been denied freedom of speech and was prevalent in *Breitbart* stories on Russian trolling topics. According to this argument, conservatives (Republicans) are treated with the same unfairness to which Russian trolls are constantly subjected. Variations of the argument emerged when conservatives com-

pared themselves to minoritized Russian trolls. Such strategies to downplay the seriousness of Russian trolling, identified across news sources, can be categorized under these rubrics: denying freedom of speech is unfair treatment and an authentic opposition argument.

Summary

The Russophobia frames can function as a face-value delegitimization technique for discrediting the significance of the Russian trolling as an issue. Justification through rhetorical techniques of mocking and degrading represents an outgrowth of classical trolling, where discursive maneuvers such as deflection or face-value ridicule are intended to delegitimize presented facts. And whoever opposes such a stance becomes a victim of circular reasoning. And while it is unexpected to find a persistent justification of Russian trolling in US news story comments, justifications were presented in multiple forms, as exemplified above.

The difficulty with counteracting the Russophobia frame of victimization and delegitimization is that delegitimization is an aggressive technique that does not permit rational argument to counteract face-value ridicule. Such ridicule automatically relegates confrontations to disbeliever status—in other words, the center of ridicule-based attacks.

Victim playing is another prominent discursive frame, discussed earlier as a typical propagandistic technique that shifts blame from the perpetrator to the victim. Complaints such as “They are falsely accused” or “They are blamed for everything” exemplify such victimization. Additionally, downplaying the seriousness of Russian trolling is yet another delegitimization tactic for justifying the phenomenon. This list summarizes statements found in news portal comments that were intended to achieve the discursive objective of downplaying seriousness of Russian trolling: “it could not have happened” frame used at face value; “it could not have happened” frame used by mocking investigations; Russian trolls are merely internet trolls; Russian trolls did not affect results; there is no evidence for Russian trolling; it is legal to troll; Russian trolls do not exist; and nobody even reads these posts.

Delegitimization was not based on facts—it is not a logos-based information battlefield, thus fact-checking can be hardly effective in debunking it. Because these delegitimizing statements are based on the irrationality of belief systems, they recall the post-positivist paradigm that invites multiple interpretations of reality. They are guided by pathos or affect. Yet the post-positivist interpretation of reality reflected in analyzed news story comments

is intended to create online chaos rather than clarity. Thus, one can say that chaos creation can exploit the post-positivist paradigm, which is evident through the use of arguments such as those advocating freedom of speech. In other words, Russian trolling justification should be de facto invited and accepted in these online forums. The projection of Russian trolls as merely “authentic” oppositional commenters further pushes for the narrative of lack of free speech.

Cited examples of face-value justification of Russian trolling is identifiable in absolutist claims, such as “Russian trolls don’t exist” or “it could not have happened.” At times, the irrationality of arguments can be “covered over” with a veneer of rationality. For instance, some arguments insist “there is no proof,” despite the Mueller report’s substantial provision of evidence for Russian trolling. Yet others trivialize Russian trolling as another form of online incivility, claiming that “it is legal to troll.” Other comments insisted that “Russian trolls could not have affected election results,” showcasing a general statement that lacks supporting evidence. Finally, the seriousness of Russian trolling was downplayed through the dismissive statement “nobody reads these comments.” Such dismissive statements imply that Russian trolling can be easily justified through these discursive strategies.

Examples in this chapter showcase how users claimed to be victimized to be mistaken Russian for trolls and were inclined to denounce antitrolling moderation practices as rationales for exercising undemocratic censorship online. However, the flaw in this undemocratic censorship argument is that it assumes that Russian trolls act within the democratic premises. Yet Russian trolling does not subsume democratic values. Thus, this makes the argument of censorship nonapplicable.

This chapter has overviewed the examples of Russian propaganda development and their historical contexts. While Russia has become a central player in the aftermath of the 2016 US presidential election, it had assumed a significant international role throughout the past two decades by using information to influence its neighboring countries—the post-Soviet territories in particular. Post-Soviet countries have, in fact, experienced the effects of the continuous hard and soft forms of influence described earlier. Such effects include the constant breaching of airspace by Russian military fighter jets and Russian interference through cyberattacks. While cyberattacks exemplify warfare’s soft influence, hard influence has characterized its war tactics in other instances.

Deny and Conquer

Fears of Looking like a “Pussy State”

Denial, along with attack and defense strategies, contribute to chaos regarding the Russian trolling phenomenon. Denialism is defined as “the employment of rhetorical arguments to give the appearance of legitimate debate where there is none” (Diethelm & McKee, 2009, p. 2). While denialism may sound not grounded in legitimacy, there are long-term consequences to denialism and a price to be paid for it. For instance, Moses (1989) stated: “By the time denial has become a significant factor in political process, efficiency has already been considerably impaired” (p. 294). To bypass rationality, denial is typically accompanied by deception. However, the two differ. Denial focuses on blocking the relevant information, while deception aims to make the adversary believe something that is not true (Godson & Wirtz, 2000). Furthermore, rationality is subverted by blaming social problems and conspiracy theories to divert attention from given uncomfortable or inconvenient truths (e.g., Jolley et al., 2018). In other words, a long process of denial creates an insurmountable damage that escalates the problem.

This book documented how chaos online was reflected through different rhetorical and argumentative shapes. In addition to summarizing and explaining this chaos-instilling rhetoric related to Russian trolling justification, this chapter is set to provide a list of “tools” to cope with its destabilizing effects. The first set of tools is a list of discursive mechanisms to recognize denialism as a tactic of justification. Next, there is an explanation of the psychology of denial. Then, an outline of denial justification argumentative traps. Finally, media literacy tips are included to provide long-term guidance.

Implications of the Denialism Discourse Regarding Russian Trolling

Denialism is a powerful strategy that can create chaos online. Thus, it is critical to recognize denialism discourse tactics, especially since the discursive mechanisms outlined here can be extended beyond Russian trolling to a denial or deflection of any controversial phenomena. This chapter summarizes the complexity of Russian troll denialism and its relationship to multiple tropes: denialism as created by using propaganda and disinformation tactics through deflection and whataboutism, as well as cracks in society such as attacks on immigrants. Finally, the expression of denialism was at times found to employ the tone typically attributed to internet trolling—dismissal, mockery, and delegitimization—which makes it conflated with subculture rather than an information warfare.

Furthermore, the notion of “question more,” ironically being the motto of Russia Today, that is, Russia’s state-run TV station evokes the need to complicate issues in question, rather than trying to resolve them. In some ways it resembles the dilemmas that post-truth era brings. And, given that reliable information to answer the quest of questioning more, the use of conspiracy theories accompanies the very ethos of “question more.” One of the dangerous aspects inherent in the idea of “question more” is the simulated endorsement of the principles of democratic debate, where understanding emerges through the multiple ideas. However, the deviance of “question more,” is in that it diverts the focus of the debate. As a result, it can lead to a distorted view of reality. Szulecki (2018) observed: “[Question more] arguably takes the Enlightenment ideal of a critical and sharp reason beyond the frontier of relativism and into nihilism, aiming at provoking doubt and amplifying disagreement” (p. 324). Whataboutism is set to create chaos based on the Russia Today slogan “question more” without implying an answer, but by instilling more doubt.

Antipublic sentiments that questioned legitimacy of institutions and radicalized political polarization, which Davis (2020) called discourse of *antipublics*, were found to be mixed in with disinformation efforts. Antipublic discourse was used to justify Russian trolling—as a technique to divert attention and provide recommendations or themes that are already familiar to the far-right readers, since those recommendations most frequently appeared in right-leaning media comments—in *Breitbart* and Gab.

A mix of these three rhetorical tactics with affect result in a rather cacophonous but unified front of what can be seen as an authentic and genuine denialism. Regardless of the actual identities of users who deploy provocative rhetorical tactics in news portal comment spaces, in all instances, Russian

trolling denial, summarized in this book, was found to be based on either argument, constructed in a generic manner to fit anywhere.

Such arguments, through which Russian trolling was justified, was found across platforms and news portals regardless of news source. Even if they were topic specific and found across multiple platforms and two countries, these arguments were based on affect or belief system rather than logic. Such denial is reified through what I conceptualize as generic denial construction—a rhetorical process that perpetuates explanatory frames by repeating them multiple times across platforms over an extended period to validate them instead of providing proof. These universal denial techniques and their rhetorical variations can be outlined accordingly:

- Whataboutism is attention deflection technique (“Do not look here but look there instead”) or digression introduced in a given message. Diverting attention to a peripheral aspect of an issue (e.g., the costliness of Russian trolling investigations) is accomplished by shifting the attention from the main issue. That is, instead of arguing against that issue (e.g., Russian trolling) the goal is to downplay its seriousness; using false equivalency or diversion of attention to “cracks in society” (e.g., illegal voting, immigrants).
- A recommender affiliation type of argument uses an agreed-upon truth to validate other arguments (e.g., “If you hate Hillary Clinton, you should also deny Russian trolling”).
- The victimization rhetorical strategy is based on self-victimizing statements (e.g., “We are falsely accused of Russian trolling,” “The enemy is someone else”).
- Shifting blame (e.g., “The real culprit is the political opposition”).
- Self-blame (e.g., of Russian trolling denial). This rhetorical maneuver is based on providing additional support for scapegoating (“we are duped”), spreading conspiracy theories.
- Delegitimization of institutions (e.g., news organizations, the FBI), attacked because of their role in the ongoing investigation of or exposure of the Russian trolling as a phenomenon.
- Face-value dismissals (e.g., Russian trolling simply does not exist).
- Dismissal through mocking, provocation through implicature denials. Denial has been found to be constructed through the tone of expression.

Whataboutism emerged as one of the most prolifically used techniques in news portal comments. Whataboutism departs from a set of contested facts

that are elaborated not for clarification but for distraction. Whataboutism functions like magician's trick that invites the audience to look in a different direction and focus on something else while the magician performs the trick. Such misdirection that is at a core of the whataboutism is created through allusive subliminality. And even if whataboutism is openly stated in the message, it functions like subliminal advertisement designed for people not to see the targeted content but to subconsciously memorize the advertised item (Theus, 1994). The power of redirecting attention of such an allusive subliminality of messaging can relate to the findings of the subliminal advertisement where affected populations develop even stronger opinions (e.g., Ruggieri & Boca, 2013).

As mentioned above, the whataboutist strategy of attention diversion can effectively exploit the inclination to validate preexisting beliefs by endorsing particular viewpoints or by accepting specific types of information, as argued by the theory of social comparison processes (Festinger, 1954). Because such exploitation can be extremely predictable where partisan issues are concerned, whataboutism can specifically target the psychological loopholes of polarized issues. Moreover, because whataboutism can create vicious circles of argumentation, these techniques can be used to ignite a perpetual interaction that leads to nowhere but distracts from the real issue. Such engagement could involve a simple defense of an individual position on an issue that itself seems to be fulfilling the promises of online spaces of public deliberation, yet it leads to perpetual argumentation that disrupts online discussion spaces, as seen in typical online trolling behaviors (Herring et al., 2002).

The recommender affiliation is found in the news portal comments as yet another resource-consuming measure to push arguments claiming that Russian trolling does not exist. To maximize denial, one needs to predict how the target will react to it (Godson & Wirtz, 2000). Thus, recommender affiliation can be used to ensure success of the denial. The recommender affiliation capitalizes on reinforcing of the pre-existing beliefs. In other words, recommender affiliation is supported by the findings of confirmation bias, in psychology research is described as "interpreting of evidence in ways that are partial to existing beliefs, expectations, or a hypothesis in hand" (Nickerson, 1998, p. 175). Such a recommender affiliation is based on two distinct items that are juxtaposed within a single message. For instance, if the first item is introduced as an agreed-upon truth, and the second is juxtaposed alongside it, typically ideologically-fitting to the preexisting beliefs, and the message reader will be very likely to endorse the suggestion. Moreover, such juxtaposition increases the likelihood that the reader should automatically agree with any new information, even if encountering the message's content

for the very first time. Thus, the recommendation technique involves a two-part message: The first part is the promoter that has been already accepted as true; the second is the promoted message component that needs to be remembered and accepted as true. In Russian trolling denial arguments, this technique appears as an illogical alignment of values (e.g., “If you are against Hilary Clinton, then you will believe that Russian trolling didn’t happen”). Thus, the promoter (i.e., established consensus) and the promoted (i.e., new targeted message part) work in tandem.

Recommender systems are widely exploited as an online marketing technique. Specifically, after a product has been launched, others that share similar features can be recommended in its wake (e.g., “If you like this product, you will also like this one, which is similar”). Such product recommendations can reflect consumer taste even while influencing purchasing decisions. However, the caution is that while similarity as a metric to measure taste in marketing can rely on any manifest conjectures—such as previous purchases or demographic variables, in online persuasion, similarity is more nuanced and relies on latent variables such as political affiliation or values. Recommender affiliation technique is similar to what Herring et al. (2002) identified as a trolling technique, in this case, based on ideological manipulation of the audience, which capitalizes on exploiting the existing agreed-upon points to stir discord.

Russian trolling denial was also found to have denial arguments embedded within a partisan argument. Such construction generates what Koopmans and Olzak (2004) called discursive opportunities of influence, which have been employed and relevant for persuasion typically in mass media messages, even before social media spaces were acknowledged as public spheres. Typically, discursive opportunities of influence operate best on messages that are contentious. Three elements create conditions conducive for such discursive opportunities: Visibility, or the extent to which a message is escalated (i.e., known to the general public); resonance, or the extent to which message recipients react to a message (e.g., allies, opponents, authority figures); and legitimacy, or the degree to which such messages are supported. Visibility, resonance, and legitimacy determine message reception—a message’s potential to proliferate or acquire memorability.

Moreover, denialism served as a divisive partisan issue. While blaming the “others” of being “duped” by Russian trolls, frequently found in the comments explains, in part, any partisan justification embedded in online news portal comments that justify Russian trolling, however, such partisan denial was unequivocally strong among Gab users who, by scapegoating the political opposition, whether the left generally, or Barack Obama and Hill-

ary Clinton specifically, in their posts dismissed the Russian trolling phenomenon as an absurdity. It is not surprising to find a partisan explanation to the phenomenon. The same claims of “Russian trolls do not exist” have been repeated by government officials. For instance, on multiple occasions, a former US president Trump publicly insisted there was “no collusion,” “no obstruction of justice,” and “no Russian interference,” as reported by Nussbaum (2018).

Russian trolling denialism was found to go beyond partisan divisions, even if partisan accusations have been found to be part of instilling chaos, in line with previous research on partisan vulnerabilities of media ecosystems (Benkler et al., 2018). However, political division has been found to be exploited on contentious issues by creating “paranoid arguments” that are typically based on mere accusations rather than logic (Hofstadter, 2012). This style of American politics was chiefly documented back in 1966, in discussions about gun control. Hofstadter (2012) described the rhetorical construction of the paranoid style involving self-positioning within the “us” versus “them” opposition (we are the good guys; they are the bad guys, the enemy we need to vanquish). In such rhetorical instances, the “enemy” needs to be identified and then confronted. Thus, Russian trolling denial can exemplify paranoid argumentation—one that is primarily defensive and that resorts to whataboutist attacks on opponents.

Similarly, whataboutism techniques found in this book used to justify Russian trolls are similar to grooming trolling technique defined as a psychological manipulation of the target to align with certain beliefs or ideologies, as described by Berghel and Berleant (2018). The mocking tone found in this book can be related to false-flag trolling, where the troll purports to hold a specific belief that they are actually in conflict with (Sun & Fichman, 2019). Similarly, given that in this book Russian troll justification was used through political polarization frames, such frames relate to what Fichman and Sanfilippo (2016) called as political trolling. Similarly, scholars like Anderson et al. (2014) found the polarizing effect of incivility online. Finally, the concept of baiting—inherent in what constitutes trolling for some leading trolling scholars like Phillips (2015) and Fichman and Sanfilippo (2016)—can be applicable to many Russian troll justifications referenced in this book, making it harder to separate Russian trolling as political trolling, from an internet online trolling, which is already part of the online fabric.

Denialism functioned also as conversational digression—as the rhetorical process of redirecting public attention from Russian trolls and cyberoffenses to other possible scapegoats for unrelated social problems. Interestingly, in

multiple instances, all categories of people were denounced as “trolls,” with the single exception of Russians. For instance, media institutions have been targeted for particularly vitriolic attacks while the focus of discussions was frequently shifted from Russian trolls to US immigrants. Such rhetorical maneuvers are consistent with Polletta and Callahan’s (2019) assessment of Donald Trump’s remarks about “fake news media” intended to delegitimize media institutions that critique his presidency.

Blaming rhetoric was also geared toward media institutions, legislative institutions, politicians, and immigrants. This blaming construction through the lens of the opposition has been attributed to a populist rhetoric, found to be prevalent in the far-right discourse, for example Bobba’s (2019) analysis of Italian *Lega Nord*—right conservative political party’s—rhetoric online. As noted in earlier chapters, blaming both sides was a variation of blaming rhetorical maneuver that had been recurrently identified in analyzed comments. In such zero-sum instances, denial of Russian trolling paradoxically coexisted with its acknowledgment. However, such acknowledgment also accompanied the whataboutist comments accusing Democrats of attempting to profit through the use of Russian trolls.

However, rhetorical maneuvers of denialism are complex: It is not only about the content of the message but also about the tone (Schmuck & Hameleers, 2020). Yet, message and tone are geared to create perceptions of authenticity. Populist discourse typically relies on denigration of the enemies—the elites (political, media, financial, judicial, and intellectual) and others as defined by sociopolitical context. Blaming has been found to comprise the “othering” of various groups of people (e.g., “cracks” in society), which in Bobba’s (2019) analyzed Italian case were immigrants, Roma people, LGBTQ individuals, and welfare recipients, similar to the US cases, where immigrants were a particular target as well. And Bobba (2019) argued that these frames were found to work best when coupled with affect.

The affect was traced in the tone and the manner of denial frames. Denial arguments have been found to be vested in the tone of dismissal and mockery, typically in trolling discourses (Clarke, 2018). In international politics, cynical mimicking is the concept that captures the essence of mockery (Magun, 2016). Magun (2016) argued that the “cynical” does not mean “coldly rational” but rather “provokingly insolent.” Such a cynical tone was found in the Russian troll justification comments described in numerous examples of this book.

Repetition of identical messages and frequent posting by a given user were posting traits found in news portal comment analysis on *Breitbart*. These repeated messages signal an automated nature of message dispatch.

The automated nature of repetition is particularly plausible, considering that the same messages were found across news portals and news stories. Such repetition foremost can enhance the memorability of a given message. However, repetition can also lend it a semblance of accuracy, given that the same information is repropounded on multiple platforms and news portals. Thus, this entire rhetorical process extends the original notion of the illusory truth effect, an expression coined in the late 1970s. The concept of illusory truth effect postulates that repeated statements are easier to process and subsequently perceived to be more truthful than new statements (Fazio et al., 2015).

Repeated frames that delegitimize Russian trolling also create the information flooding effect. When describing censorship styles, Roberts (2018) distinguished between information deprivation and information flooding. In contrast to information deprivation, whataboutism is based on the flood of information, where the nature of information is intentionally unrelated to the goal of distraction. While Roberts focused on information flooding as a macrotechnique, in this book I have exemplified how it works on a micro level, through specific utterance-based constructions, and how those constructions are exploited to circulate across media platforms through the adoption in the user-generated content spaces.

Psychology of Denialism

Gab Example 1

Marcus: I talked to Vlad for a few minutes over Skype today, and he promised me that my check would be mailed in 7-10 American business days. Excited. <https://occidentaldissent.com/2018/04/14/pentagon-scrambles-to-cover-syrian-humiliation-brings-out-russian-troll-narrative/>

Link to a story “Pentagon Scrambles To Cover Syrian Humiliation, Brings Out “Russian Troll” Narrative.”

[image: an army of soldiers with the masks of trolls instead of faces]

Fuhrer: The idiotic move by the Jews combined with making US look like a total “pussy state,” because it painstakingly avoided harming even one hair of “Russian bear’s” head, make’s Trump look like more of laughingstock than Niggerbama.

While comments like these include racial slurs and anti-Semitism to reallocate blame, they also suggest an answer to the question: What are some

psychological explanations of denial and why someone would choose to propagate such denialism? Such comments imply that Russian trolling investigators were restrained by collective anxiety—the fear of being perceived as a “pussy state,” that is, by exposing the vulnerability of the United States and of making the US president “look bad.” Thus, the rhetorical motif of Russian trolling denial that recurs within conservative circles derives from the fear that the US would “look like a pussy state.”

“Pussy state” is an idiomatic reference to the condition of being subjugated and defeated. Such vulnerability demanded concealment, followed by disavowal. The comment posted by this Gab user provokes further discussion about the significance of “pussy state” and the context in which the term emerged. Can such anxiety-driven rhetoric provoke the collective denial of Russian trolling and foreign interference? This chapter outlines how denial as a discursive tactic worked to sustain the justification of Russian trolling.

Fear of looking like a “pussy state” exemplifies the denial-driven self-defensive impulse that Moses (1989) identified as a survival mechanism: “The usage of denial can be found anywhere in the world—more particularly, more strongly so when and where there is acute conflict. We, most of us, push out of awareness whichever warning signal is presented to us” (p. 294). Furthermore, fears of looking like a “pussy state” address the following questions: Why would online comment writers across news portals want to generate the illusory truth effects? What vested interest is there for users located within the US to repeat Russian trolling denial messages online? Such user behaviors provoke the suspicion that there are specific individuals who, for whatever reason, deem it an urgent necessity to persuade news portal comment readers that Russian trolling does not exist. The current media allows for a repeated exposure to information across multiple sources, which, in turn, as argued by Hasher et al. (1977), can enhance one’s perception of the accuracy and veracity of those facts.

Thus, denial in the broadest sense can operate as an unconscious mechanism and has been documented and justified as a psychological condition that healthy adults normally inhabit. Where individual psychology is concerned, Moses (1989) argued that the strength of denial is proportional to the perceived threat to one’s physical or psychological existence. Comments that deny Russian trolling as ways to justify it are wrapped in an aura of projected authenticity, especially since they included familiar tropes. Familiar tropes here refer to the frames that have already proliferated in polarized, affective framings and what Nadler (2020) called countercultural conservatism. Nadler (2020) furthermore stated that conservative media superstars utilized populist discourse of visceral politics. Then, these constructed

frames that constituted “preconceived notions” regarding immigration or other sensitive social and political issues have been found to be reposed in the comments along Russian troll justifications. Such an exploitation of preconceived notions generates the illusory truth effect.

Mitigation is yet another denial strategy that uses euphemism to downplay the seriousness of issues. These strategies have been identified across all analyzed news portals and platforms throughout this study. According to van Dijk (1992), denial discourse included mitigation through euphemism, excuses, and disclaimers; blaming the victim; reversal and defensive maneuvers of face saving, and self-presentation during discussions about controversial topics—all of which function as modes of justification. Van Dijk (1992) also discussed the subtler forms of denial that he calls presupposing doubt, or distancing, here conceptualized as creating chaos.

Moreover, while this study endorses van Dijk’s (1992) observations about denial-based attack and defense strategies, it identified specific cases of blame shifting presented in various forms of denial. Denial as modes of justification have been extensively reported in the academic literature (Brint, 2019; Mason, 2012; Milburn & Conrad, 1998; Priestly, 1996). For instance, while Dedaić (2005) claimed that denial can assume the form of dismissive irony, Furko (2017) treated denial as a form of manipulation to achieve communicative goals such as diversion or whataboutism. According to Jolley et. al (2018), “By blaming tragedies, disasters, and social problems on the actions of a malign few, conspiracy theories can divert attention from the inherent limitations of social systems” (p. 465). Such a dismissive irony and content diversion had been identified in multiple instances throughout this study. For instance, while some users resorted to ironic parody when they called themselves “Russian trolls” to downplay the seriousness of Russian trolling, others complained that “Russian trolls are blamed for everything.”

Yet the power of denial is indisputable. In some form, denial can be rooted in the denier’s sincere belief (in the value of denial). In others, denial can assume the form of outright lying in the convoluted process of withholding or avoiding to admit the truth. Yet in others, it can appear as selective interpretation of truth, or as misrepresentation of reality. Denial can also be the outcome to find comfort in beliefs contradicted by evidence (Bardon, 2019). It can even escalate into a denial syndrome that enables the denier to manage guilt while asserting superiority over others, including those who accuse that denier of wrongdoing (Ramet, 2007). In fact, according to Chandler (2006), denial and lack of accountability are related.

Denial can also be a powerful procrastination strategy. For instance, *Operation InfeKtion* (2018), while discussing the propaganda playbook,

stated that playing a long game allows to perpetuate denial of facts. This propaganda tactic can also be deployed to make targeted message recipients forget about a specific issue or to redirect their attention to other concerns. Throughout preceding chapters, Russian trolling was identified as the primary justification object in online news story comments. As such, public attention was deflected from Russian trolling to other issues. Thus, justification of Russian trolling paradoxically assumed the projection of a collective denial. Such denial is, in fact, viewable as a convenient procrastination tactic—for instance, during the 2018 investigation into the Russian influence of the 2016 US presidential election. Given that the investigation took a long time, news portal comments could speculate on outcomes by introducing and reasserting the justification of Russian trolling.

Denial can be a useful procrastination strategy in many other contexts, especially when immediate action or a clear plan is required. Moreover, denial can be particularly useful before any further evidence is presented. When a given phenomenon (e.g., Russian trolling, taking place online) is new, it can be time consuming to collect substantial evidence to support claims of its contested existence. During such ongoing contestation, denial can be a useful strategy for dismissing the seriousness of that phenomenon for the general public, even if the final outcome of the investigation finds supporting evidence of its existence. Or at the very least, it can buy time for devising an alternate explanation for the contested phenomenon. Typically, denying a crisis before it is obvious, is a convenient tactic. When the crisis is imminent, the focus is on solutions rather than questioning the denial. Prolifically used in political processes, denial has been deployed as a tactic in a range of circumstances that include propaganda orchestration and avoidance of issues, such as climate change (Antonio & Brulle, 2011) and Russian trolling.

Furthermore, denialism is a form of misdirection that is geared to disinform. Disinformation differs from lying, yet they share a doubt-instilling element. Carson (2010) argued that lying and deception can promote one's personal interests when used in public sphere. Deception not only can manipulate public opinion but also be used to avoid consequences for one's actions. While typically public statements are official types of communication, in information warfare, Russian troll justification frames occur covertly, through user-generated content (e.g., news portal comments, social media posts). And, finally, denial amplified online can gain traction. Where Russian trolling is concerned, denial as justification was detected in news stories on the topic throughout 2018, even in the wake of Mueller's evidence. Russian trolling, in fact, was a convenient object of denial due to

its ambiguous visibility, which complicated efforts to identify its specific instances and support them with unequivocal evidence.

Denial and Conspiracy Theories

Russian trolling justification in this book was also found to be convoluted in conspiracy-based explanations. The proliferation of conspiracy theories is analogous to the circulation of rumors with tailored content. And messages that are viral typically include content that is most likely to stimulate interest or provoke controversy (Nahon & Hemsley, 2013). As noted in previous chapters, e.g., in Chapter 2 and Chapter 3, in particular, conspiracy theories were used as justification frames. This section proposes conspiracy theories as another set of discursive tactics that divert attention from Russian trolling. Conspiracy theories are known as ways to explain events by evoking unverifiable sources of invisible but powerful groups that allegedly plot against the government. By this virtue, conspiracy theories have been argued to violate norms of the democratic discourse (see Baden & Sharon, 2021). Conspiracy theories as a framework here is set to demonstrate chaos-instilling efforts, i.e., how conspiracy theories can diminish the seriousness of arguments about the damage Russian trolling causes to the democratic processes. Moreover, it illustrates how such theories are particularly exploitable for advancing Russian trolling denial arguments.

According to conspiracy theories premises, the truth is somewhere out there, and it is attainable through the act of seeking. Thus, for conspiracy theories to function, one needs to access to “the ultimate truth.” Such an “ultimate truth” then is repropounded through multiple “explanations” or “theories” of the “invisible” phenomenon, despite the implausibility of embedded premises. Thus, there is always an available “alternative theory” proposed by conspiracy theories to explain or justify anything. Ideally, an informed citizenship can foster such individual truth seeking. While individual truth seeking approach can be viewed as preferred in media literacy education, some scholars have critiqued this information sense making as an individual responsibility (see boyd, 2017). This ideal encourages conspiracy theories, that are likely to thrive in discursive contexts that popularize the “find the truth yourself” directive. In other words, alternative arguments constructed from the subjective perspective of truth-seeking individuals can provide the bases for conspiracy theories. The unverifiability of such argument premises increases the likelihood that they become appropriated as rhetorical scaffolding for conspiracy theories.

Since denial does not take place in a vacuum, certain conditions are required for its proliferation. First, denial needs believers. In fact, denial usually involves groups of followers who can sustain seeded ideas and, in some cases, transform them into movements. Such movements of denial can be rather prolific. Movements can be based on seeded ideas, rumors, or even conspiracy theories. For instance, Oliver and Wood (2014) found that 50% of Americans endorsed at least one conspiracy theory. Moreover, Oliver and Wood (2014) observed that beliefs in supernatural or paranormal phenomena could be predicted by the conspiracy theory endorsement. Thus, conspiracy theories underlying comments that justify Russian trolling provide latent but powerful organizing principles for American mass opinion. Invoking conspiracy theories to deflect attention from Russian trolling is a logical tactic to achieve such beliefs.

Second, the effectiveness of denial depends on its ability to function as a system of unified messaging across platforms and news stories. For instance, some of the best-known conspiracy theories are used by the climate change denial movement. Such movements were found to be mutually enforcing organized initiatives, or components of what Dunlap and McCright (2011) called a denial machine. Such mutual enforcement attacks various facets of the same content. Attacks involving institutions are intended to undermine policy-making processes. Thus, denial movements are subversive and rooted in collective disbelief in proposed, typically empirical, evidence.

Denial movement followers are interconnected through multiple online platforms and face-to-face networks. For instance, antivaccination and flat-earth followers were found to engage with other deniers through online network clusters on platforms like YouTube (Paolillo, 2018) or other social media platforms. Such movements provided and proliferated their own self-explanatory narratives through online spaces and networks. More specifically, Russian trolling deniers in this book were found to adopt the rhetorical maneuvers of denial that recur across analyzed news portals comments, despite variations in political affiliation and geographic distribution of analyzed news sources.

Other movements, such as Holocaust denial, justified their disbelief through alternative rationalizations and explanations of historically documented facts (Fraser, 2009; Moses, 1989). If we accept the premise that conspiracy theories justify or at least divert attention from the inherent limitations of social systems, we might understand why they appeared in the Russian trolling denial comments identified primarily on Gab. While the writers of these comments and their intentions remain unknown, clearly such comments have some kind of social value

for online community members, who could at times be disillusioned by governing structures.

The mechanisms of influence based on conspiracy theories can be described accordingly: Such influence can be introduced through an initial set of values and ideologies. Then, a counternarrative can be drafted—one that presents main ideas within a framework of doubt and uncertainty. Such presentation also introduces new premises for deliberation. Although such premises can be irrational, inclusion of plausible elements can generate a sense of credibility. Thus, recipients of messages, based on conspiracy theories, are duped into explanations to draw connections where there are none, between main ideas and digressive or irrelevant points.

Disinformation and conspiracy theories benefit from the unverifiability of the claims where rhetorical moves use affect or *pathos* rules over reason or *logos*. In that, conspiracy theories can be prolific in post-truth segments of society. Conspiracy theories, Russian trolls, and disinformation all share different degrees of invisibility that justify their existence—whether through unverifiability of a source, anonymity, or a mere camouflage. Moreover, conspiracy theories can successfully coexist with other factual information in the postmodernist era when a single truth can solicit multiple interpretations. Thus, they are convenient mechanisms for covering up truths or distorting them—or ambiguously multiplying them. Conspiracy theories, as such alternative points of view, have been prolifically used to justify Russian trolling.

Ironically, however, conspiracy theories purport to reveal truths. And the assumption underlying conspiracy theories is that the truth is not what it seems but is “out there.” Yet the possibility that “the truth is out there” enables the subversion of conspiracy theories in favor of Russian trolling justification. Such subversion is urgent because the conspiracy theories that are amplified and proliferated exemplify alternative modes of thinking behind the justification of Russian trolling.

Yet we might ask why conspiracy theories are even considered when discussing Russian trolling. We can address this question by acknowledging that Russian trolling’s intangibility begs for alternative explanations that allow for the justification of its denial. In other words, although Russian trolling exists, there is an alternate explanation for why it does not exist. Similarly, conspiracy theories are convenient, given that it is a highly accepted subculture in the US, as noted by Oliver and Wood (2014). Thus, if there is an ongoing interest to obstruct evidence for Russian trolling existence, alternative conspiracy-based explanations can be substituted for that evidence. Such alternative explanations then advance subversive agendas.

Consequently, with Russian trolling being an invisible and easily intangible online phenomenon, it is a perfect target to be exploited by conspiracy theorists. Some comment writers in the analyzed news stories projected Russian trolling itself as conspiracy. Treated this way, Russian trolling can be trivialized as a phenomenon that falls into a category of hysterical questioning. “Hysterical questioning,” coined by Hofstadter (2012), can be described as a form of a paranoid style of communication. Such a paranoid style provided American politics with its rhetorical subtext and created a new level of chaos in which all information streams are suspect. Thus, the online invisibility of trolls can justify their denial by conspiracy theorists and paralyze any efforts to make rational sense of it. This leaves us with a question of what can be done to avoid argumentative traps of denialism.

Denial Normalization Traps to Avoid

While distinguishing rhetorical tactics of denial and its psychological origins is critical, Russian troll justification arguments are listed here as traps to be avoided. There are several Russian trolling denialism traps that can be grouped under an umbrella of normalization. The first such normalization trap to avoid is its habituation and a treatment of it as everyday persuasion—as when repeated frequently that Russian trolls do not exist or when Russian trolling is treated as yet another form of persuasion. The second facet of normalization is exploited through definitional ambiguity, that is, by justifying it as yet another uncivil behavior or grouping Russian trolling on par with any other subcultural phenomena, addressed here as trolling or conspiracy theories that are used to justify it. The third relates to definitional ambiguity, and the fourth set of arguments attribute Russian trolling to partisan turfs. Finally, the discussion, is opened regarding the treatment of foreign influence in the ecosystem of online (democratic) participation. The argument is that even if we live in an era when information warfare rages on, the subversion of online comments by unauthentic actors should not be normalized as democratic. Instead, democratic debate needs to remain unhindered by encouraging the participation of bona fide internet users.

Habituation

This section outlines several caveats for Russian troll normalization traps. One of the caveats of treating Russian trolling beyond incivility or online subculture stems from denial construction through tactics such as mock-

ery or deflection, typically used in internet trolling. In other words, Russian trolling denial techniques recall internet trolling characteristics more generally. It is worth noting that deflection and mockery are also used in propagandistic rhetoric (Choukas, 1965). Thus, due to similarities between denial arguments and trolling techniques, Russian trolling can be viewed as a mere outgrowth of popular cultures. More specifically, it lends itself to trivialization as a mere variation of trolling, a major subcultural practice, and despite its propagandistic rhetorical qualities. Thus, it is uniquely challenging for Russian trolling to be recognized as such. Moreover, the treatment of Russian trolling as a subcategory within the more general cybercultural phenomenon of trolling suggests that “we are the ones engaging in Russian trolling.” In other words, American internet users morph into the actual cyberoffenders as the co-conspirators of Russian trolling.

When normalized, Russian trolling becomes an inseparable part of the online social fabric. Specifically, if masks are worn on a regular or even frequent basis, trolling becomes another self-masking behavior in online spaces. Thus, the first trap not to fall in when dealing with denialism is by avoiding arguments that normalize the issue at stake.

Previous chapters discussed how Russian trolling denial had been identified in specific rhetorical maneuvers. Collectively, such maneuvers project efforts geared to normalize Russian trolling denial. More specifically, normalization presents Russian trolling as just another regular online activity that is neither unique nor effective. In fact, as evident from the comments presented in this book, some deniers themselves argued that Russian trolling is a form of persuasion that is not new to the media landscape. While this argument can be interpreted as partially trueful, it is untenable when we consider the parties who might have vested interests in exercising online influence. Where Russian trolling is concerned, such parties are foreign operatives (i.e., Russian trolls).

Russian trolling, for example, has been repeatedly trivialized in the deniers’ arguments as just another innocuous online identity charade. Trolling habituation, however, does not diminish the gravity of paid operative influence. Thus, in instances when influence is funded, the mask is a means to what Choukas (1965) called conceal distortion. Ultimately, Russian trolls can hide behind various masks, and masks in themselves are ambivalent: On the one hand, the mask can enable innocuously playful user identity performances (e.g., in chatrooms); on the other hand, it can be exploited to conceal cyberoffenses (e.g., stalking) or disrupting online communities, as in the online trolling phenomenon (Herring et al., 2002). Such polarization is further complicated by positioning Russian trolling as yet another habitual online behavior (e.g., in the news comments covered in this book). Thus,

this potential for dual interpretation of the mask can become a trap, which Russian trolling deniers have exploited in their arguments.

Multiple comments that challenged Russian trolling by using the argument of insufficient evidence exemplify paradoxical efforts to deny Russian trolling through its normalization. Such arguments, founded on the empiricist claim “If we could not see it, it did not happen,” are rhetorical maneuvers to generate doubt. The condition of not knowing the unknowable poses an insurmountable epistemological (and existential) challenge. Thus, by extension, Russian trolling, treated as normalized practice, is destined to continue to provoke skepticism, even if evidence deemed sufficient were to be provided to confirm the instances of its occurrence. Why would that be? Such skepticism is destined to linger because we are dealing with invisible masks that conceal the actual identities of Russian trolls, and that skepticism is rooted in the condition of not knowing (what is not known).

This epistemological condition of not knowing generates a lingering, deep-seated anxiety because we are constantly being reminded that we are confronted with an unsolvable obscurity. That obscurity is deemed “unsolvable” because it involves intangibles such as “invisible” trolls. In other words, we can see only the disembodied online traces that trolls leave behind—not virtual images of their actual faces or bodies, especially when they adopt anonymous user masks. Thus, the anxiety of not knowing, provoked by unsolvable mysteries or intangibles behind Russian trolling, is exploited to construct the persuasive denial arguments embedded in online news comments.

Habituation as a form of everyday persuasion is another argument that has been used by Russian troll deniers to normalize Russian trolling. The pervasiveness of everyday persuasion in the advertising industry has contributed significantly to American consciousness formation since the 1970s (Ewen, 1996). Yet everyday persuasion in advertising taught us a lesson: Everyone becomes habituated to the fact that influence is part of American life—whether that influence is exercised through advertisements or other even more subliminal online messages (e.g., “foreign influence should be accepted”). However, when it comes to Russian trolling, everyday persuasion goes beyond typical when foreign operatives are involved. Such habituation can, in turn, normalize any signs of foreign political influence.

Ambiguity of Incivility Online

Another caveat of Russian troll normalization is the ambiguity resulting in lack of seriousness toward Russian trolling. Russian trolling often was found

to be justified as *mere* trolling. Such trivial treatment is exacerbated when Russian trolling is buried beneath imbricated layers of popular cultural rhetoric and complicated by the controversiality of conspiracy theories. Thus, the invocation of popular culture or conspiracy theories can be uniquely complicating. Such invocation is a rhetorical trap that reduces the urgency of resolving the Russian trolling problem—first, by neutralizing it within the discursive context of popular culture and, second, by complicating it by rhetorically enmeshing it within conspiracy theories. At the same time, the most complicating factor for Russian trolling acknowledgment is (online) invisibility. This factor can also be invoked to rationalize the prevailing apathy toward Russian trolling and its impact on Western democracy.

While Russian trolling denial might be expressed in a civil way, it still is a form of justification. Not to fall into the incivility justification trap, democratic incivility today should be concerned with issues beyond incivility of nondemocratic efforts to interfere with democratic deliberation. The provocative tone of Russian trolling justification can easily be mistaken as a hate speech characteristic prevalent in online internet trolling. And even if construction of Russian troll denial messages is not forwardly uncivil or impolite; nevertheless, they can still pose threats to the democracy. Nevertheless, hate speech is a specific form of online behavior that can be used in Russian trolling but is not equal to it, as it has been projected through the arguments justifying Russian trolling. In other words, while hate speech as a rhetorical strategy can be used in Russian trolling discourse, Russian trolling cannot be reduced to hate speech, given that other discursive tactics that do not involve hate speech (e.g., whataboutism) are part of Russian trolling as well.

Civility has long been considered a valued indicator of a functioning democratic society. Regardless of disagreements, previous studies argued that there is a certain level of civility through which disagreements take place online, thus providing a hopeful projection of the future of online public sphere, as postulated, for example, by Papacharissi (2004). Yet visions of democratic deliberation have become more pessimistic. I argue that information warfare complicates the democratic part of democratic deliberation. Thus, while the debates might be civil, they might threaten democracy, even if civility or lack of it has been the primary focus regarding the challenges of online deliberation. Based on that, Su et al. (2018) argued about the facets of what constitutes democratic deliberation online: Disagreements should be respectful and polite for inclusion within deliberative processes. Public expressions should be high quality and present rational arguments to be considered “democratic” (e.g., Herbst, 2010; Stromer-Galley, 2007).

Thus, the disagreement that characterizes political deliberation is distin-

guishable from toxic or unproductive forms of incivility. Definitions and indicators have been used to formulate such distinctions. For instance, incivility has been primarily defined as an absence of courtesy that is betrayed through three major expressive forms: insulting language, dramatic language, and emotional display (Coe et al., 2014; Gervais, 2014; Rowe, 2014). Moreover, Su et al. (2018) specified conversation etiquette norms in their discussion of online civility. They observed that rude and extremely uncivil comments included the use of profanity or the threat of aggression. Other scholars have approached incivility as a phenomenon that is psychologically based and has ethical repercussions. For instance, Andersson and Pearson (1999) defined incivility as “deviant behavior with ambiguous intent to harm the target, in violation of workplace norms for mutual respect” (p. 457).

Thus, contentious online behaviors have been equated primarily with forms of discursive incivility. Within the context of such incivility, online spaces can enable the negativity inherent in disagreement. However, disagreement is inevitable in political deliberation. In fact, it is even welcomed, given that the discursive spectrum can be diversified by the inclusion of negative perspectives, as argued by Stromer-Galley (2007). Thus, although discursive negativity provokes negative emotions while threatening to incite negative actions, its proponents argue that it is a major characteristic of democratic debate.

Solving issues of incivility focuses on solving the trolling rather than foreign interference. Yet based on the notions of information warfare, the conditions of democratic deliberation should account for the genuine participation, as the examples in this book showed how Russian trolling justification aimed at eliciting an emotional response, a provocation technique, typical for online trolling discourse (Greenfield, 2011). As a result, mocking tone that has been found to be used in some of the justification frames adheres to this definition.

There are more reasons Russian trolling cannot be reduced to mere online incivility. Typically, in political communication, incivility online has been analyzed in democratic debates. Even if democratic deliberation is not always civil, it is at least not programmed by foreign influence, as Russian trolling is. Thus, such an uncivil debate can be exploited with the goal of blending in. Thus, online incivility in democratic debates can generate a rhetorical paradox or a crack that enables the infiltration of trolls. This paradox allows for Russian trolling to be justified as yet another opinion.

The trivialization of Russian trolling as yet another uncivil online behavior threatens to underestimate it as an orchestrated influence. In other words, encouraging the conflation of orchestrated influence with mere impoliteness

can be a useful strategy for exercising the influence that can disrupt democratic processes. Efforts to push an ideology can be disguised as gestures of mere impoliteness—as such, they can be justified by Russian trolls themselves as aspects of online subculture. Yet, notion of computational propaganda challenges the dominant conceptualizations of incivility that are based on the assumption that all online spaces are produced by authentic users, who are ordinary citizens or opinionated online news readers. Thus, while genuine participation is considered as dominant, yet, inauthentic content production is reality and online spaces can be produced, inhabited, or managed by an orchestrated group, such as an office in St. Petersburg, Russia, online.

Definitional Trap

Another type of Russian troll normalization can be attributed to the definition-based ambiguity, echoed in the media. Emma Grey Ellis's (2019) article in *Wired* magazine is headlined “Nobody Knows What ‘Troll’ Means Anymore—Least of All Mueller.” The headline implies the following narrative: Formerly, there was certainty and consensus about the definition of “troll” or “trolling.” Today, that can be declared “lost” (“Where is the good ol’ trolling of the past? The kind we used to find in the uncivil news comment threads on Yahoo!”). The headline also justifies the “authenticity of trolls,” who mirror recent cultural phenomena. Ellis (2019) wrote: “If trolls are good at anything, it’s reflecting a culture’s contentions and confusions back at it” (para. 4).

While Ellis (2019) recognized that trolls capitalize on the contentions, for her, the definitional ambiguity persists. However, Mueller (2019) clearly defined trolls: “[Trolls are] internet users—in this context, paid operatives—who post inflammatory or otherwise disruptive content on social media or other websites” (p. 23). Thus, Ellis’s (2019) headline suggests the triumph of post-truth, and the beginning of the post-troll era, when discourses concerning what or who “trolls” provoke further questions that increase our doubts about our ability to distinguish between authentic and paid troll agendas. Ellis suggested some common perceptions about trolling when she described trolls as “people who go against the norm” or “who post just for reaction.” Such descriptions could have inspired a user who proudly claimed to be a troll to boast, “I do not apply labels to myself” (para. 3). By doing so, Ellis perhaps involuntarily normalized trolling as a “part of internet culture” by claiming that trolls “bring internetty ‘irony’ to mainstream politics; they

game the attention economy; they weaponize dog whistles and identity politics. Most of all, they're cacophony with quirky usernames" (para. 5).

There is no doubt that online trolling in academic scholarship has been treated as a form of subculture. For example, Whitney Phillips (2015) claimed that trolls constitute facets of internet culture or subculture. More specifically, she detailed the development and proliferation of internet trolling over the years—how it has spread to various online communities. Hodge and Hallgrimsdottir (2019), even if rather critical toward foreign interference, also used the term “subculture” when interrelating Russian trolling and alt-right efforts to create activist spaces online: “Indeed, alt-right communities are examples of how space becomes place in (sub)cultural imaginaries” (p. 10). Moreover, they also refer to alt-right online activism as a “culture-escape.” This term encourages to justify alt-right members as mere trolls while legitimizing the alt-right as a powerful new sociocultural movement. Thus, Russian trolling, when operating in such online spaces, also qualifies as another form of subcultural practice rather than foreign influence.

To a certain degree, the idea of subculture legitimizes trolling as part of the media ecosystem—even if it is ideologically charged or possibly orchestrated by a foreign government as a form of information warfare. At the very least, the invocation of subculture justifies the entitlement of Russian trolls to occupy online spaces. However, when discussed in the context of trolling, Russian trolls are automatically normalized—possibly even glamorized (in certain circles)—as subcultural phenomena. Moreover, the risk involved in including Russian trolling in extant subcultures is the legitimization of foreign government interference. Such interference enables foreign governments to exploit mass media—particularly user comment spaces—to create their own narratives and thus push their own agendas.

On a surface level, it is easy to dismiss the Russian trolling phenomenon as a mere subcultural practice: Its emergence coincided with the global resurgence of hate groups and the hate speech they have spawned online. For instance, the alt-right (or alternative right) has unleashed ideological momentum for “virulent racism, misogyny, homophobia, transphobia, and xenophobia” (Hodge & Hallgrimsdottir, 2019, p. 563). It has been documented that, since 2016, alt-right groups have emerged from sociopolitical peripheries to occupy more central and more visible public spaces in the US. Lyons (2017) detailed the ideological elements that have resurged in alt-right messaging since the 2016 US presidential election. Moreover, Hodge and Hallgrimsdottir (2019) claimed that Steve Bannon appropriated the discursive authority with which *Breitbart* is invested to enable alt-right ideologies to proliferate throughout online spaces. Thus, finding reflection

of alt-right ideologies in the news comments on Breitbart is not surprising, whether those comments are genuine or not.

As a result, the fact that the allusive treatment of Russian trolls can be equated with the fact that they have coincided with the resurgence of hate speech and alt-right movements in Western democracies. These movements legitimize hate speech by rhetorically camouflaging it in narratives promoted by the ideology behind Russian trolling. Hate speech can be employed in Russian trolling, thus making these interlinked. Because hate speech can be found in Russian trolling justification (e.g., use of anti-Semitic rhetoric), it can be challenging to distinguish Russian trolling from more general forms of internet trolling in which hate speech is rhetorically embedded.

Lyons (2017) specified alt-right activities as efforts to establish an independent online forum to define the movement's scope. For instance, alt-right white nationalism is the main ideological focus of *AlternativeRight.com*. From that ideological perspective, it has approached wars on terrorism and issues of race. Similarly, unfiltered alt-right rhetoric is accessible on the white supremacist website the *Daily Stormer*, where, for instance, Andrew Anglin (2016), has described the movement as a counter culture that is anti-Semitic, anti-feminist, anti-multiculturalism, anti-postmodernism, anti-political correctness, anti-Afrocentrism, pro-white, pro-Europe, pro-traditional families, pro-scientific racism, pro-free speech, and anti-SJW (social justice warrior). In practice, alt-right rhetoric opposes progressive activist agenda items, such as immigration reform and gender equality (Lyons, 2017). To further describe the alt-right movement, Lyons quoted a prominent member of the alt-right white nationalist movement, Greg Johnson, at *Counter-Currents Publishing*: "The survival of whites in North America and around the world is threatened by a host of bad ideas and policies: egalitarianism, the denial of biological race and sex differences, feminism, emasculation, racial altruism, ethnomasochism and xenophilia, multiculturalism, liberalism, capitalism, non-white immigration, individualism, consumerism, materialism, hedonism, anti-natalism, etc." (p. 5).

The practices of some online subgroups generally resemble activities that are typically classified as trolling. Hodge and Hallgrimsdottir (2019), in fact, ascribed alt-right activities to a collection of disgruntled individuals (or trolls). Lyons (2017) described alt-right discursive practices accordingly: "The *Right Stuff* website uses a mocking, ironic tone, with rotating tag lines such as 'Your rational world is a circle jerk'; 'Non-aggression is the triumph of weakness'; 'Democracy is an interracial porno'; 'Obedience to lawful authority is the foundation of manly character'; and 'Life isn't fair. Sucks for you, but I don't care'" (p. 5). Russian trolling, when treated as a sub-

cultural alt-right phenomenon, can be hidden behind rhetorical masks that hate speech communities provide. Such groups can also serve as endorsement mechanisms that enable the amplification of ideas promoted through Russian trolling.

Targeted trolling has been discussed in the scholarly community as a form of ideological trolling that emerges in unexpected contexts, such as popular culture spaces or fandom discussion forums, where users experience the ideological allure of issues that are frequently unrelated to the designated fandom topic. For example, Bay (2018) detailed how haters were instrumentalized through debate about the controversial *The Last Jedi* film in the *Star Wars* series. Controversy derived from the film's celebration of values that alt-right haters typically oppose. Thus, in this instance, alt-right "hater" propagandists could infiltrate *Last Jedi* fandom discussion forums, where they would form alliances with other alt-right users to amplify their messages.

Thus, alt-right movements and internet trolling in general can conveniently mask or at least be conflated with the more specific Russian trolling phenomenon. Alt-right groups engage in the same tactics of ideological influence as documented here by Russian trolling: they exploit pre-existing beliefs to impose new interpretations, as noted by Heikkilä (2017). To be subverted, online spaces must be unregulated, and neither global nor anonymous, while catering to specific niche groups. Consequently, subversive hate groups can occupy online spaces that are considered peripheral or underground. In fact, it can be argued that such groups do exist, and have done so—and without necessarily depending on foreign government support or incentives. Hate groups feed on the trolling discourses that permeate toxic discourse spaces, such as 4chan (Oboler et al., 2019; Zelenkauskaite et al., 2020).

Gab, as an alt-right social networking site, provoked controversy that started with the hate speech and eventually translated in the act of violence. The case refers to a Gab user who had been posting antisemitic remarks on Gab was eventually charged with the 2018 Pittsburgh synagogue shooting (Kottasová & O'Brien, 2018; Matsakis, 2018). In that specific case, discourse charged with violence has moved into an act of violence. Consequently, Gab was investigated and eventually deactivated. While investigation was ongoing, Andrew Torba, Gab's chief executive officer and founder, invoked freedom of speech to defend his social networking site by making a statement published temporarily on the site: "Gab isn't going anywhere. You can't stop an idea." Thus, while Torba pleaded that the synagogue shooter was an isolated instance among numerous other Gab users citing the need for freedom of speech for all types of content.

However, radicalized online spaces have been found to be particularly vulnerable to the infiltration of foreign influence. Specifically, the Russian government has been identified as an active participant in social media spaces populated by alt-right followers (Hatmaker, 2018; Olin, 2016; Shane, 2017). Russia-backed groups also were found to spread content across platforms and modalities beyond text-based social media to amplify its reach across internet communities (Hoffman, 2017; Zakem et al., 2018). Additionally, Hodge and Hallgrimsdottir (2019) addressed the connection between Russian trolling and the alt-right: “Between 2016 and 2018, news reports began to illustrate that a significant portion of the political and social images—or “memes”—that were used in various alt-right spaces were not the work of amoral internet trolls operating from sites like 4chan, but rather the work of coordinated external actors with deep ties to states hostile to the United States” (p. 572). Hodge and Hallgrimsdottir (2019) observed that the rhetorical maneuvers of alt-right groups include opposition and rejection of the “dominant” narrative, and attacks on progressive activists.

Russian trolls, due to their affiliation with the hate groups that Russia supports, when uncovered, can be thus challenged on the grounds of this intricate overlap. News reports provide further evidence that Russia-backed groups had invested heavily in partisan debates on platforms like Twitter and Facebook, where they used automated posting services (or bots) and targeted advertisements to influence the 2016 US presidential election (Timberg, 2017). The question lingers: To what extent are radicalized platforms exploited by orchestrated influence to tap on the groups’ ideologies and channel them for different goals? As previous chapters suggest, targeted messages can be crafted and deployed more easily by groups in the networked online spaces.

Exploited Partisan Division

Analysis of the comments and social media posts that justified Russian trolling used arguments that normalized Russian trolling’s impact through the status quo treatment of partisan division in American politics. Examples found in the news portal comments and Gab betray such normalization through two partisan-specific attitudes toward Russian trolling through these two oppositional statements: “We’re *not* a ‘pussy state’” and “We have been duped.” While variations of the former statement were primarily found in the right-leaning media that *Breitbart* or Gab exemplify, variations of the latter recurred in left-leaning media, such as the *New York Times*. Although

these statements can furnish the premises for two fundamentally different arguments, they can serve the same purpose—that is, shifting the blame from Russian trolls to some other convenient scapegoat for social evils. Gab users had frequently adopted denial rhetoric by complaining that it was hard to be denigrated as a “pussy state.” Thus, such complaints suggest that even in the aftermath of Russian trolling interference in the 2016 US presidential election, denial remained a persistent rhetorical subtext of user comments.

As expected through partisan division of the treatment of Russian trolling, the *New York Times* was found to be the only analyzed American media source whose user comments acknowledge the existence of Russian trolls. By contrast, *Breitbart* and Gab did not contain clear-cut “Russian trolling exists” frames, it was only subtly implied that Russian trolling could have existed. These findings reflect the ethos of the current information landscape. Since 2016, numerous popular presses in the US have released books that treat Russian trolling as a partisan issue, rather than as a form of foreign interference (see for example, Abramson, 2019). In other words, when Russian interference is accepted, it becomes the mechanism for allegedly justifying Hillary Clinton’s loss. Denial of such interference, however, legitimizes the outcome of the 2016 US presidential election: Trump presidency and inauguration.

However, such politicization of Russian trolling suggests that denialism of Russian trolling is normalized and even acceptable. Consequently, it lends itself to the possibility of Russian trolling denialism is a mere matter of public opinion. Such possibilities recall the dichotomy between the polarities that can be introduced by the post-truth paradigm: a relativist approach which parallels the notion of truth to a matter of beliefs. Such projection of truth as a belonging to a sphere of beliefs, strips it from the necessity of being grounded in evidence. Consequently, as suggested throughout previous chapters, public mistrust and online chaos can be seeded when the existence of Russian trolls is questioned without considering its supporting evidence. Thus, when Russian trolling is trivialized as the object of subjective perception, it falls into the realm of post-truth. In other words, it works in tandem with post-positivist premises, according to which it is a phenomenon that is determined by belief systems rather than facts. In short, everyone has the freedom to endorse the belief system of their choice. Thus, Russian trolling as an object of subjective perception is rendered even more subliminal.

Furthermore, because a large part of Russian trolling denial is deeply rooted in partisan logic, its acknowledgment within right-wing political contexts translates into admission that the US is a “pussy state”—a nation that is vulnerable to foreign influence. According to such logic, Russian trolling did

not happen as long as evidence of it is not accepted. Thus, denial becomes the long game—an avoidance tactic that is deployed until the media spotlight on the object of denial finally fades out. Russian trolls deniers throughout this book blamed the American people for falling for Russian trolling, further stirring discord online.

Dangers of Russian trolling stem from persuasion as normalized but also legitimized. With legitimization, general concerns about partisanship and public trust emerge, together with more specific questions, such as “Are there really external operatives that can influence US presidential elections and internal politics?” This question implies an uncomfortable truth: the possibility that, the American people need to “deal with Russian trolling.” This especially hits the conservative voters who have been ideologically positioning their values along the lines with the Cold War rhetoric—being against the Soviet Union and everything associated with Russians. Currently, American voters are confronted with the anxiety-inducing possibility that, not only that a foreign government could have influenced their presidential elections, but that more specifically, such foreign influence was orchestrated by Putin’s Russia, and yet, on *Breitbart*, an example of the right-leaning analyzed source, comments were found to justify Russian trolling more frequently, compared to the *New York Times*. This contrast illustrates the divergent ideological values and identities that continue to polarize political parties in the US (Mooney, 2012) and how they can be exploited.

Discussion

Traps of Russian troll normalization provoke a rhetorical question: Can democracy survive this online chaos? After all, through denialism, trust in information has been compromised and the risk is to face all-prevailing skepticism, or what Choukas (1965) called the propaganda addiction, when someone is prone to bipolarize all issues in oversimplifying pro and con terms. For Choukas (1965), in such a view, nothing is innocent anymore. Thus, although we need to take everything with a grain of salt, there is no need to make that grain into a mountain. In other words, taking everything with a many grains of salt can generate lasting social effects: Disbelief and skepticism can escalate into paralyzing collective anxiety and lead to chaos.

The challenges we face today, recall the American 1960s and Choukas’s (1965) discussion of the need to develop curricula in media and visual literacy. When he wrote about mass persuasion, he claimed that citizens at the time were seeking an “all-inclusive formula by means of which one can

comprehend an incredible era we live in” (Choukas, 1965, p. 1). He also claimed that there were dangers looming in the shadows of mass persuasion. One of them is the dismissal of ideas and perspectives contrary to a doctrine we choose to endorse. Such dismissal, Choukas (1965) stated, can invite us “take shelter in a conforming but dangerous cynicism and proclaim everything as polluted with propaganda” (p. 1). Additionally, he warned us that this paranoid fixation on the omnipresence of propaganda can incapacitate us as citizens in a democracy, where pundits such as Ewen (1996) have identified an ongoing tension between democratic ideals and persuasion.

It is challenging to refrain from projecting a dystopian view of the future of democracy due to the new conditions of automation and anonymity that enable foreign government interference and the treatment of Russian trolls as authentic discussants in public online spaces. Moreover, it is challenging to refrain from adopting a similarly dystopic view of the new platforms and persuasion mechanisms that are geared toward the subversion of ideologies. The challenge can be exacerbated by the technological nihilism underlying Woolley’s (2020) cautioning that grassroots politics will be taken over by phenomena such as astroturfing.

Technopopulism furthermore contributes to creating chaos online and challenging democracy. As Bloom and Sancino (2019) argued, technopopulism generates conflicting ideas about technology. Although politicians constantly exploit technology to promote their populist agendas, their rhetoric is primarily antitechnocratic, as discernible from their refusal to believe that technology enabled Russian interference. As illustrated by Bloom and Sancino (2019) in the use of Twitter by Trump’s tweets as president and Jair Bolsonaro’s use of WhatsApp to advance their agendas, technopopulism thrives in the globalized world. Both examples show how social media is exploited for populist mobilization. Furthermore, while Trump used Twitter for mass persuasion, he has repeatedly denied Russian trolling and its intervention in the 2016 US presidential election. Thus, ironically, while he has disavowed technology as a medium of influence, he has used it for that very purpose.

Thus, online spaces are paradoxically unified by a shared predicament: They constitute an information landscape where it is increasingly harder to distinguish what is true. Such obfuscation, enabled through algorithms and bots, and geared toward exercising foreign influence, has provoked opposition to the increasing convenience of technology. Such opposition through the abovementioned technopopulism, which poses its own dangers of lingering doubt of what constitutes the authentic participation.

While the American public is still debating the scope and effectiveness of

Russian interference in the 2016 US presidential election, online messages and offline small talk continue to shape public perceptions in significant ways. For instance, just a handful of ideological trolling references can be more detrimental than might be speculated, because they seed uncertainty that can escalate into social panic. Even more specifically, by provoking the mistrust in information sources that can lead to online chaos, Russian trolling denial can initiate major structural changes in societies. Robert Lane (1962) specified the forces that can affect such changes. By focusing on the opinions of “typical” American citizens, he argued that the forces of change include objective and subjective components. Objective ones include existential bases, and subjective ones are common experiences. Other determinants for social change include cultural premises, personal qualities, political ideologies, and social conflicts.

Where Russian trolling is concerned—and particularly in far-right online news spaces, social conflict is necessary for enabling competing user voices to be heard, if they are authentic. Lane (1962) observed that social conflicts are typically muted through cultural emphases on classlessness, tolerance, assimilation, unity, public interest, and compromise. Consequently, conflicts are atomized and individualized. However, Lane (1962) warned us that even if social conflict is temporarily muted, it can be easily reactivated. By extension, Russian trolling denial frames can reactivate conflicts—and not only those that are based on partisan affiliation but also those that derive from specific social problems, such as racial discrimination, and other forms of otherization. Moreover, due to anonymity and automation, such frames online can more easily become vehicles of hate in online spaces than elsewhere. And conflict can be suddenly unleashed through the fabrication of just one rumor about the unjust treatment of any category of people.

This book, furthermore, showcases how arguments that are rooted in antipublics frames that use such a polarizing rhetoric of hatred in message frames to justify Russian trolling. This exemplifies how Russian troll justification was used along with arguments familiar to readers who are more likely to circulate messaging that contains anti-immigrant, anti-left-wing content, accompanying Russian troll justification.

This polarization has been seen in this book as ways in which Russian troll justification was used by capitalizing on various types of hate or rage (Orenstein, 2019). Davis (2020) similarly argued that antipublic discourses are based on rage. Antipublic discourse in Russian troll denial taps into the sentiment of hate regardless who is posting—be it a Russian troll or anyone who intends to create chaos. It is impossible to disagree with Orenstein’s (2019) insightful analysis of Russia’s strategic information warfare today:

He claimed that Russia did not create populism in the West, xenophobic nationalism, or anti-immigrant sentiment but inflamed divisions, and the effect of that hybrid war is polarization of politics. Similarly, Benkler et al. (2018) identified that white supremacists, far-right believers, and neo-Nazis in decentralized online spaces ranging from 4chan (Zelenkauskaite et al., 2020) to Reddit engaged in a memetic mobilization that allowed deployment of disinformation memes. Similarly, traits of antipublics have been found in Islamophobic rhetoric on Gab (Woolley et al., 2019).

The evidence in this book shows how rage has been used to divert attention from Russian trolling. Such rage has been found through antipublic discourses channeled toward anyone else—illegal immigrants, anti-Semitic conspiracy theories, institutions and political opponents—but Russian trolls. Russian troll justification includes themes typically ideologically familiar to far-right readers.

The sentiment of hate is powerful. The Icelandic band Hatari, formed in response to the worldwide rise of populism, conveyed this in its song “Hate Will Prevail” (Van Gorkum, 2019). The message behind these lyrics concerned hatred as a powerful response to the propaganda of hate, if no counter perspectives are provided—the oppositional or alternative ideas that are the objects of study for propaganda historians. Similarly, Pratkanis and Aronson (1992) acknowledged propaganda’s dark side by citing the Third Reich’s propaganda of hate: “In the hands of a demagogue, persuasion can be full of treachery and trickery, appealing primarily to our irrational impulses” (p. 259).

Thus, to resist such “irrational impulses,” we should engage critically with the content we are exposed to. Ewen (1996) emphasized the need to foster critical thinking as follows: “For the greater good to prevail, we need to imagine ourselves as a greater public” (p. 414). Yet others argued that marginalized groups have produced enough traction to increase political polarization and chaos (McVeigh et al., 2014).

Pratkanis and Aronson (1992), in a reflection about propaganda as persuasion, concluded: “We have seen how information in our world can be selectively edited . . . or managed by experienced political consultants . . . to play with our emotions” (p. 258). Thus, they proposed some initial steps in the process of developing critical-thinking skills. Undoubtedly, it remains extremely challenging to make sense of the current media landscape in which multiple actors compete for influence. Moreover, that challenge is exacerbated by our inability to determine the actual identities of such (online) actors. Thus, Russian trolling denial can be counteracted by various initiatives for managing ideological trolling. Thus far, such initiatives have

been developed by news media organizations and engaged citizens who have succeeded in soliciting government involvement.

Summary

New York Times Story 1, Example 1

████ California Dec. 18, 2017

Professional muckrakers from a foreign government intentionally targeting our country and the fabric of our society are not protected by our First Amendment.

████ Los Angeles Dec. 18, 2017

Free speech for whom, a Russian troll acting on behalf of his country's intelligence service? This type of speech is akin to yelling "FIRE!" in a crowded theatre.

New York Times Story 1, Example 2

████ California Dec. 18, 2017

Like it or not, this is free speech. Suppressing it to avoid offending people will not change what people think. Only more speech can do that.

These *New York Times* user comments expose another element of creating chaos online—the boundaries of free speech. In the era of automation and anonymity is everyone equally entitled to free speech? Before the public sphere had been expanded to include online spaces, scholars treated free speech as a concept that has an enduring but troubled relationship with democracy (see Hare & Weinstein, 2010). Past treatments of denialism can provide a lens for how Russian trolling denial should be treated online.

History deniers, in particular Holocaust deniers, is a topic that provoked a discussion between free speech and the treatment of such deniers. Denial's impact has been typically measured through the "proliferation of denial materials" or propaganda, as in the case of Holocaust denial (Fraser, 2009). Fraser (2009) used the phrase "proliferation of denial materials" to refer to the effect size or the impact of access to such denial materials. Fraser furthermore argued that changing the societal perception is the first step to combat denialism. In the case of Holocaust denial, he argued that, because it is embedded in the collective psyche, such denial impulses cannot be further threatened by technology through which such denial proliferates. Thus, he proposed to change societal perception by using legal means to restrict

exploitation of hate through the controversial topics that incite radicalized groups to emerge into online visibility. Today, such topics of denialism can include the divisive coronavirus pandemic, the qualifications of 2020 US presidential candidates, or Russian interference in previous US elections.

While Fraser (2009) invited us not to put the blame on the technology, he did caution that the sociotechnical context needs to be adjusted to new circumstances of influence. And while user-generated content (e.g., comments), by virtue of access, extends the right to free speech to all users, with the rise of phenomena such as Russian trolling and online hate groups, now more than ever we have to foster media literacy skills (Winter, 2019).

Russian troll denial frames found in the news portals comments, illustrated in this book, evoked the First Amendment argument, claiming that Russian trolls are guaranteed their right to free speech. However, there are numerous precedents when First Amendment invocation proved problematic. When considering Russian trolls' "right" to participate in online discussion, we need to distinguish between authentic and orchestrated discourses in online spaces. Admittedly, all groups have the right to participate in debates, but government-sponsored agendas that are advanced with the intention of influencing another country's political decisions—particularly those pushed by paid trolls or automated bots—cannot qualify as authentic user participation in the online public sphere. In other words, the noxious ideological aspect of Russian trolling renders it irreducible to mere participatory politics. Thus, Russian trolling cannot be treated as an authentic form of online participation.

If Russian trolls are treated as merely internet trolls, they are entitled to inclusion among all other media ecosystem participants, even if trolling discourse typically involves hijacking conversations and amplifying divisiveness. Such behaviors can be rationalized or justified by some, claiming that there is a certain level of human authenticity behind them. This logic legitimizes their right to participation online. Thus, while Reestorff and Stage (2016) compared trolling to discursive boundary work, due to the ambiguity of trolling, together with cracks in society, online participants ultimately compete to determine who has political agency and who should be excluded from (political) participation.

There is still an ongoing debate on how to handle political or foreign interference trolls online. The mere rhetorical act of calling a user "a troll" seems to be the most obvious; however, it may automatically involve the user in the same disruptive behavior as the troll, which consequently perpetuates the circle of trolling online. Such implications derive from the assumption that the interlocutor, or the user who initiates the trolling accu-

sation, assumes the authority to deny the (alleged) troll's right to participate (Reestorff & Stage, 2016). Calling out trolling also implies that all trolls should be silenced or otherwise disempowered, thus shifting their role from the disruptor to that of a victim. Such victim vestige further blocks any solutions to trolling as a disruptive phenomenon or Russian trolling as a foreign interference phenomenon.

While such solutions seem radical for trolling as an internet phenomenon, calling out Russian trolling is the first step toward providing awareness of such phenomenon, even if, as shown in this book, it has collateral effects, such as inciting uncertainty and suspicion of who is a Russian troll, and ultimately chaos online—the ultimate goal of information warfare.

Despite mechanisms already in place for cracking down on trolls, public deliberation can lead to more online chaos rather than broadened understanding or consensus—thus inadvertently realizing the objectives of Russian trolling. Disinformation campaigns are typically characterized as having multiple goals and spread in decontextualized forms across various platforms and communicative threads (Krafft & Donovan, 2020). Coupled with ideology, trolling becomes part of a larger narrative of uncertainty that individual commenters deliberately, or unknowingly, circulate—with the ultimate effect of seeding online chaos. Thus, the victimization of internet trolls through denial resonates with other denier movements. Even in the case of foreign interference, such as Russian trolling, the act of denial dangerously positions Russian trolls as victims.

Previous chapters illustrated how some users insisted they were *not* Russian trolls when they were called out as such. Instead they were lamenting that they were “falsely accused” as such. Thus, the ambiguity of one's online identity as an authentic human user is yet another complication involved in navigating online spaces. Because individual posts are decontextualized and presumed to be authentic, they can be easily interpreted as yet another slew of opinions. Thus, we need to acknowledge that the frames replicated in the comments of multiple news stories, even in different accounts, could actually be an orchestrated online strategy to advance a particular agenda—and especially when users dispatch series of messages with similar frequency.

Russian trolling justification through denialism tactics showcases a unified projection of ideology reflected through the discourse—an ideology of denying the existence of Russian trolls or justifying them. Hall (1985) viewed ideologies as sets of discourses with their semiotic meanings, that is, the systems of representation and practices situated in specific contexts and practices. And the discursive practices traced through this book e.g., denialism and justification reflect ideological stances, when privy of evidence, or

a result of a misconception based on “incomplete knowledge” (Purvis & Hunt, 1993). Justification of Russian trolling can function as efforts to shift the image of Russian trolls by showcasing them not as actors responsible for interference in the US presidential elections but as alleged victims blamed for everything. Such shift in the narrative, Purvis and Hunt (1993) argued through the reflection on ideology through Larrain’s (1991) misrepresentation theory as entailing a “negative” conception and the notion of misperception. Russian trolling victim playing serves as an example of misconception. Specifically, Purvis and Hunt’s (1993) argued that “misconception or an ‘incomplete’ knowledge of social realities where ideologies work with the intention of directionalities—to favor some and disfavor others” (p. 478). Žižek (2012) put it more bluntly, stating that ideologies are doctrines that comprise ideas, beliefs, and concepts to convince us of “truth” in the guise of utopian narratives.

This directionality is clearly viewed through discursive frames used across media types and across national contexts that aims at *converting* of the image of the Russian trolls from negatively projected actors into neutral actors or even victims. Such a need to convert the meaning of Russian trolling into positive, can be presented by some as a subversion of such an *ideological struggle*, yet, with an opposite meaning from its typical interpretations. Hall (1985) discussed the *ideological struggle* as a battle of class, race, or gender, where the minorities are repressed by the dominant majority; as a process of restitution of the minorities. While Russian trolls are not repressed, they are projected as victims, the blamed ones, thus, needing of sympathy, with the ambition to shift the projection. At the same time, the pushed ideology is the one of the innocence of Russian trolls.

We also need to consider the challenges involved in discussing the political impact of Russian trolls, as when Reestorff and Stage (2016) argued that “the participatory politics of trolling is neither inherently democratic and emancipatory nor inherently undemocratic and oppressive” (p. 249). If Russian trolls are treated as mere trolls and not foreign interference, this argument can be easily misread as supporting other arguments that justify Russian trolling—the kind of rhetorical maneuvers that have been identified in numerous user comments. It provides doubt as to the accountability of such influences. Thus, while seeding doubt about the accountability of Russian trolls, the argument might dangerously reify the claims that have been critiqued in previous chapters that, if the impact of a phenomenon (Russian trolling) cannot be measured, we cannot conclude that it (Russian trolling) exists.

Similarly, the historical accounts of persuasion and promotion in the US pose a specific challenge to efforts to override apathy about foreign influ-

ence. Escapist invoking of freedom of speech is certainly not a new rhetorical maneuver in democratic public spheres. For instance, Stuart Ewen (1996) critiqued the legitimization of persuasion as democratic voices. The main problem relevant to this book is identifiable in “The Engineering of Consent,” an essay by Bernays (1947) that Ewen (1996) cited, which emphasizes how the Bill of Rights justifies the right to exercise persuasion. Bernays (1947) writes: “Freedom of speech and its democratic corollary, a free press, have tacitly expanded our Bill of Rights to include the right of persuasion” (p. 113). However, such textual expansion has been criticized for failing to amend the rights of freedom of expression and persuasion to “augment the public dialog” (Ewen, 1996, p. 37). In other words, as the exemplar of the “free press,” the mass media alone is guaranteed the right of persuasion. Thus, the expression “engineering of consent” resembles the manipulation of public opinion or what some pundits label “propaganda.” “Engineering consent implies the use of all the mechanisms of persuasion and communication to bend others, either with their will or against their will” (p. 398). Ewen (1996) restated the mechanisms of consent engineering accordingly: “Public must be studied and analyzed prior to the manufacturing process (taking public temperature). To be successful, themes must appeal to the motives of the public” (p. 380). Moreover, Ewen (1996) articulated the fine line between democratic values and propaganda by contrasting it with a *disdainful manipulation*. These questions remain relevant in the context of foreign automated influence.

As mentioned in previous chapters, modes of persuasion today range from mass media to social media that is accessible through online spaces. In other words, these modes are no longer restricted to traditional mass media forms, such as television, radio, and print newspapers. In fact, persuasion modes now involve a much more complex media ecosystem—one that sprawls across multiple convergent technological platforms and applications, involving mobile networks and also mass media. Moreover, media ecosystem stakeholders are not only professionals and experts but also ordinary users. In fact, the media ecosystem has expanded to include automated systems involving bots and AI agents that share online space with human users. Consequently, the ambiguous distinction between authentic and synthetic online space inhabitants, especially AI applications, has become problematic. This troubling ambiguity relates to Bernays’s (1947) concern that the right to persuasion could be exploited by those who threaten possible evil. Thus, there is always the troubling possibility that such exploitation could serve antidemocratic purposes. Therefore, we might conclude that in several decades since the publication of “The Engineering of Consent,” Ber-

nays's (1947) claims remain valid for today's complex media environment.

The question that remains unanswered is this: How should the engineering of consent be treated in the social media era, when consent can be engineered by foreign governments? Moreover, Ewen (1996) contextualized the engineering of consent in American politics when he invoked Ronald Reagan as the product of the cultural practices of manufacturing public appeal. Specifically, Ewen (1996) observed that Reagan had played a critical "translational" role that appealed to ordinary people. In fact, he had enacted "ordinariness" as "an ideal cover for conservative political motives" (Ewen, 1996, p. 395). Currently, such ideals are evoked by protecting us from looking like a "pussy state."

Discussions about the challenges of practicing the democratic ideal of free speech in the online public sphere can also justify the lack of urgency in addressing the Russian trolling problem. Specifically, while critiquing Bulgarian news portals, Bakardjieva (2008) observed that online news story comments are "carnavalesque" rather than "consensus building." In other words, online spaces are platforms for the exchange of free speech, where "nonserious" cacophonous shouts compete to be heard. Such spaces are the antithesis of moderated discursive forums, where serious harmonious remarks coexist for further deliberation. American online user behaviors modify claims that discursive cacophony in news portals is characteristic of the comparatively newer democracies that Bulgaria and Lithuania exemplify. Specifically, *Breitbart*, *Gab*, and *New York Times* user comments prove that discursive cacophony also characterizes the more established democracies that the US exemplifies—that such democracies can be infiltrated by the divisive practices of not only trolling but Russian trolling.

Vulnerabilities of deliberative spaces in this chapter have been contextualized within discussions of Russian trolling—a phenomenon that has been treated as a form of foreign influence. The susceptibility of news portal comment spaces to orchestrated ideological influence complicates today's online deliberations among well-meaning citizens. In the current media landscape, vulnerability to such influences provokes a crucial question: Can democracy survive in the midst of new forms of information influence? When addressing such questions—including general speculations about whether technology is ultimately good or bad—social media has been the main focus, particularly in authoritarian regimes and as to how they use social media to maintain geopolitical power. What is evident that in uncoded network-based online spaces that have been designed for decentralized information dispatch, centralized social control can be exercised.

Epilogue

Now What?

Imperviousness to Chaos

This book has showcased how information battlegrounds have fluid boundaries. Yet there is a need to identify these spaces and to reconcile their inconsistencies within constantly shifting contexts. This need stimulates these concluding questions: How can news organizations and readers, together with social media platforms, manage the vulnerabilities of online spaces? And, how can news organizations expose the interplay of online incivility and inauthentic, or dark, participation?

This book documents not only the denial of Russian trolling but also comments that called out Russian trolls so that they could be unmasked. Such unmasking does not fully render Russian trolls visible, but it disrupts their front-end self-presentation management. As Goffman (1959) stated, “Disruptions discredit or contract the definition of the situation that is being maintained” (p. 239). The coexistence of Russian trolling denial and its acceptance suggests the subliminal quality of online influence. Far from providing clarity, such influence generates confusion about the authenticity of online phenomena. Thus, instead of opening up spaces for healthy democratic debate, the sublime quality of influence generates ambivalence about Russian trolling—and more importantly, it provokes questions about whether Russian trolls actually exist.

While it is possible to dismiss Russian troll denialism as indicators of a mere opinion or a sign of a healthy democracy in which issues are being constantly debated, their rhetorical similarity across news portals and across countries based on a repeated urge to profess the innocence of Russian trolls, indicates that these arguments have been constructed and possibly centrally dispatched—thus providing a basis for skepticism about their authenticity. As a result, affect-instilled arguments used in public

deliberation in times of uncertainty, along with whataboutism, constitute a playbook for chaos online.

Fattal (2018) argued that we live in a world where there is no distinction between war and nonwar. Similarly, we live in a world of clashing possibilities of influence, where efforts to distinguish between authentic and inauthentic online participation are perpetually challenged. Such participation includes activist efforts in the online Habermasian public sphere and the constantly contested, organized cyberefforts of orchestrated influences. This online discursive opposition creates conditions that are conducive for trolling (and nontrolling)—to extend Fattal's (2018) war-nonwar polarity to describe today's online political landscape. Yet the difference between Habermasian activist and foreign government efforts (i.e., organic versus orchestrated) becomes visible through the respective ideologies behind them. Previous chapters have discussed these ideological positions by demonstrating the repetition of the same Russian trolling denial arguments across news story comments in various media sources, amplified not only necessarily by automated bots but also by other targeted online audiences.

The problem of online circulation of ideologies brings us back to the question of propaganda models. Formerly, propaganda was orchestrated through a centralized mass media that enabled top-down message dissemination. Such messages had been officially released by leading governments—and where propaganda was concerned, such governments had been led by war propaganda, such as Nazi Germany and the Soviet Union during World War II. Since then, propaganda flows have become more complicated. For example, propaganda can be orchestrated not only top-down but also as *bottom-up*, through online user-generated content. Such bottom-up propaganda flow involves messages distributed through the social media content that all users can create and amplify, such as social media and news portal comments.

Thus, the bottom-up message flow intersects with activism and enables the voices of ordinary people to blend with orchestrated messages. The bottom-up approaches can be also exploited by orchestrated forms of influence, as discussed, through dark participation, where audiences can be exploited to participate in the dissemination of messages. Despite any surface simplicity, interactions between agents of influence and regular social media users are actually quite complex. As is the intersection between the forces of genuine activism and dark participation where the audience, knowingly or unknowingly, becomes and amplifier of genuine and orchestrated messages, as argued by Wanless and Berk (2019). The opaque language of denialism geared to justify Russian trolls further complicates the treatment of Russian

trolls. Denialism functions as a form of soft power which is based on affect, or the expectation that the audiences, the readers of the messages, join in the belief that Russian troll did not or could not have acted in online spaces.

Publics and Post-Publics

Public sphere is not static but constantly in flux. Such flux inevitably shapes the concept of publics that constitute public sphere where publics can be defined as groups of informed people about issues with a good understanding of it (Asen & Brouwer, 2001). I introduce the notion of post-publics as yet another facet of the publics. It counters the concept of informed publics that are tainted by misinformation, and particularly by the chaos creating-disinformation, or merely by post-truth.

Post-publics represent a state of confusion induced during times when a contested but impactful high-stakes issue is being discussed and cannot be based on unequivocal evidence. Such issues might be a foreign interference in the presidential election or vaccination during pandemics, or an onset of war. Publics are then reshaped into post-publics, where contestation becomes a tool not for democratic clarity but to instill chaos and confusion. As such, online publics, without a critical perspective, are presented with vulnerabilities that weaken the deliberative premises, as argued by Fenton (2018).

Post-publics is a concept that departs from the notion of publics, the publics that in part deal with the online spaces shaped by post-truth, and consequences of misinformation and disinformation. The prefix “post” relates to the state of post-communication, which Macnamara (2020) defined as “a deterioration or even a collapse of public communication from its normative purpose of informing, meaning making, and creating understanding to disinformation, deception, and exploitive manipulation” (p. 9). Post-publics are living in the information chaos defined by post-communication.

Post-publics can be shaped and amplified by antipublics. Antipublics have been defined through ideologies that are “against,” and they fixate on rhetorical grievance of antiestablishment, antiliberal ideologies, anti-Semitism to create a terrain for skepticism and relativism and suspicion. In the broadest sense, post-publics is not about utopias or dystopias of the public sphere as argued by anti-publics discourse (Davis, 2020).

Other derivations of the publics that define social movements gave birth to notions such as counterpublics (Warner, 2002). These notions exhibit the empowerment of the publics pushing boundaries beyond the expected democratic premises. While the antipublics was proposed as to describe the

radicalized groups that engage in the discourses with the values that are disjoined from the expected democratic norms and expectation, they are disruptive in the opposite direction from the counterpublics. Counterpublics are publics where a dominant group aspires to re-create itself as a public (Warner, 2002). Counterpublics are typically born of the need to apply scrutiny to the current established structures. When questioning of the established structures, counterpublics adopts “anti” discourses and providing less clarity. Thus, discourse framing becomes critical, its framing needs to shield from chaos and division, but not to amplify it.

Post-publics shape what encompasses the concept of publics. Publics typically are associated with the public sphere and democratic practices. It is about the contexts in which publics are positioned with the sociotechnical contexts facing them—automation and an intentional cross-platform push for content. Post-publics distinguish themselves by being detached from the valence associated with discourse to focus on the recipient’s perception and involvement. Rather, as the term itself denotes, it describes publics that have undergone the burden of chaos with the truth being relative and fragile. Post-publics are conditioned to emerge in the spaces governed by authentic and nonauthentic voices that create cacophony on polarized topics, typically marked by affect and left to witness unresolved chaos.

Disinformation messages, infused by affect, for post-publics can function as a form of soft power. The idea of affect mediating soft power is not new. Solomon (2014) described soft power as a form of the affective investment that audiences partake in when creating ideologies as a social construct. Post-publics, therefore, have to constantly engage in the emotional labor that is not related to the information per se that they are exposed to, but the manner in which they are presented to them.

In addition to the manner of content presentation, another challenge is the disinformation floods that take place, especially, in times of uncertainty that post-publics need to handle (e.g., Krafft & Donovan, 2020). Post-publics that are debilitated not only by affect but also by the *infoglut* articulated by Andrejevic (2013). Similarly, Andrejevic (2013) warned us about the issue of information abundance, referring it to as *infoglut*, a paradox that we currently face: the illusion that we have a sea of information available to us but also the impossibility of being fully informed.

Andrejevic’s (2013) notion of *infoglut* partly describes the state of post-publics, since they are conditioned to be intentionally flooded with a lot of contradictory information that is pushed by human and nonhuman actors—genuine and constructed ones. *Infoglut* exhausts readers or

informed citizens and leads them into more uncertainty and distrust in the value of the democratic deliberation.

In authoritarian regimes, information flooding has been identified as one of the modern types of information censorships (Roberts, 2018). Furthermore, as argued by Roberts (2018) such information flooding has been weaponized as an information diversion technique in authoritarian propaganda, as discussed in Chapter 2. Such a flood of information typically seeks to deflect attention from the issue at stake toward something else. Deflection, combined with information overload and emotional appeal, is the new form of mind control that replaces the silencing methods of authoritarian regimes. In the democratic contexts where debate is the opposite of silence, how can more information create more chaos rather than greater clarity? This book has conceptualized information flooding in the discourse, where denial is justified through deflection or whataboutism.

Publics in democratic contexts are particularly vulnerable during times of uncertainty. Discursive cacophony geared to justify Russian trolls creates a perception of online publics as post-publics where the prefix “post-” entails the general movement of postmodernism defined by skepticism, subjectivism, or relativism, with a general suspicion of reason and an acute sensibility to the role of ideologies (Duignan, 2020). Such a sentiment prescribed to the post-publics contrasts the notions of publics, counterpublics, while is fueled by antipublics.

Furthermore, while previous approaches to the online public sphere, based on Habermasian expectations, considered only human actors in the context of online public deliberation, post-publics consider a mix of potential actors—be they content created or distributed in an automated manner or manufactured by bots. As a result, if content is purposefully flooded with information, it can lead readers into a rabbit hole reasonings rather than create clarity, given that typically users deal with the unverifiability of information at hand.

With the birth of Web 2.0, online public forums have gone through stages of conceptualizations for its potentials for the deliberation of the public sphere. While started with the utopian potentials of online as an equalizer and inclusivity, in mid-2000, online public sphere was found to be spaces for echo chambers where users enforce their points of view and seek for information that is consistent with their beliefs, as suggested by Sunstein (2007); and the rise of social networking sites has been seen as new opportunities for participatory culture (Papacharissi, 2010). This trend has been followed by a more optimistic view regarding online public sphere where

the “online,” when treated as multiple-platform space where users can find various points of view and create media repertoires or collages from them, have provided hopes for the future survival of democracy and trust in user abilities to make sense of online (Semaan et al., 2014).

Throughout this book, the arguments leading to chaos ultimately form the post-publics that are pulled into aimless discussions that do not necessarily clarify. As a result, the goal of chaos is to eliminate the debate. In the rhetorical argument theory, arguments are based on *mythos*, *logos*, or *pathos*. If arguments and counterarguments are typically constructed through *mythos* and *pathos*, then the soft power reaches its goal and leads to chaos. Chaos is not persuasion. Chaos is a type of tactic that brings the masses not to the promised land of the truth but to a cul-de-sac—or more bluntly, a dead end. And post-publics are condemned to be entrenched in chaos.

What Solutions Are There for Russian Trolling?

New York Times Story 6, Example 1

■ Singapore Nov. 13

**Make information literacy a key component in the school curriculum.
Teach kids how to review sources, analyse content and look for additional
material to evaluate information in a balanced way. Start early!**

This *New York Times* comment exemplifies how online news readers take the initiative to provide suggestions for developing the information literacy skills to counteract Russian trolling. Such comments encourage us to ask: What has been done so far to resolve Russian trolling? Additionally, since Russian trolling denial frames are present across media sources and platforms, what can we do to protect ourselves from the harmful effects of trolling that create chaos online? While there are multiple technological solutions to combat disinformation, technological solutions alone remain limiting.

Besides technological solutions, current successful initiatives geared to combating disinformation can provide some insight, as can learning from the past. For instance, digital resilience is one of the frameworks that have been developed by learning from Finland’s efforts of disinformation (Bjola & Papadakis, 2020). Digital resilience builds on cognitive and physical resilience to shield from various forms of digital threats with the goal to undermine public sphere (Bjola & Papadakis, 2020).

Chouka’s (1965) distinction between propaganda and education in

postwar America provided the following insight: “The educator teaches us *how* to think but the propagandist teaches us *what* to think” (p. 5). The purpose of education is to encourage the development of independent thinking. Thus, Choukas distinguished instruction from propaganda: “The educator fails unless they achieve an open mind; the propagandist unless he achieves a closed mind” (p. 145). His assertion about close-mindedness was elaborated in his ideas about the role of ideology in propaganda. He contended that ideology is typically based on specific set of values that are clearly identifiable. Propagandists can use those values to persuade. Open-mindedness, fostered in educational settings, sets foundations for independent thinking. However, we can no longer naïvely assume that increasing access to online information automatically enables all internet users to develop critical-thinking skills. The goal is to enable publics to handle the *infoglut*, i.e., to foster the ability to evaluate information. More information should not atrophy into self-debilitating cynicism.

The need for media literacy can be described through what theorists like Anthony Giddens (1991) called reflexive modernization. Specifically, we need a heightened self-reflexivity when confronted with new threats. Such forms of self-reflexivity are necessary as a form of self-examination in the technology-saturated society in which we live. Media platforms we use are not only increasingly reflecting our lives; they are part of our lives. Self-reflexivity can be practiced by consulting the critical-thinking checklist that historical propaganda studies provide. In addition to self-reflexivity, Zabarskaitė (2019) argued for semantic media literacy where the meaning of a given message should be highlighted and evaluated in its context.

Pratkanis and Aronson (1992) claimed: “We are not only the recipients of persuasive communication, we are also the sources of such messages” (p. 259). This claim describes the current media landscape, while reminding us that we are complicit in the processes of persuasion communication through the new media technologies that provide affordances, such as automation and redistribution, where we as online users choose what to distribute. While new technologies might seem empowering, they can also involve us in the advancement of agendas other than our own. For instance, if we share or like social media messages posted by foreign government operatives that intend to exercise online influence, we become their accomplices. Yet such online complicity traps should not deter us from participation in debates within the public sphere and nonparticipation is not a solution to the Russian trolling problem. The rhetorical option of nonparticipation to resolve that problem has been proposed in Russian trolling denial comments. Thus, it is all the more urgent to develop critical-thinking skills in the changing media

landscape that could prevent Russian trolls from achieving their objectives of obstructing democratic deliberations and of subverting democracies.

Similarly, scholars such as Jankovicz (2020) urged us to overcome our own political polarization as a recipe to successfully combat information warfare. And lessons of a such practice can be learned from the propaganda studies. While analyzing propaganda, Pratkanis and Aronson (1992) generated the following critical-thinking checklist: “Judge the ethics of a persuasive attempt by assessing its goals; the extreme statement of this viewpoint would be that the ends justify the means; When the goals of a persuasive attempt are not so easily defensible, the ethical issues become more problematic; Judge actions according to the means employed by the source of information: one should avoid dispensing false information, hiding facts, using specious reasoning, or falsely playing on the emotions; Consider both the content and the goals of the message” (p. 261).

In addition, when it comes to overcoming polarization, it is not only our individual responsibility but a responsibility of media ecosystems to constantly engage the public in debates about major issues and their broader contexts and ramifications. We might ask, “What is the debate about, and who is behind it?” Such questions are necessary in today’s media landscape, where there is extensive evidence that alt-right groups launch disinformation campaigns (Bevensee & Ross, 2018). Thus, previous chapters have provided numerous illustrations of Russian trolling denial frames on *Breitbart* and Gab. Due to the absence of other positions on Russian trolling Gab can be used to perpetuate Russian troll denial.

The paradigm-based approach to critical reading can supplement this list. This approach includes the concept of what I refer to as broad ideologies—that is, the mechanisms that enable the identification of messages in question and which side those messages support. Broad ideologies as a framework encompass various facets that should allow for fighting misinformation and disinformation—as a framework it is geared as a preemptive measurement of media literacy. While typically misinformation focuses on message source and content, disinformation frameworks beyond message source and content should include a paradigmatic treatment of a message, by uncovering the implied message and the author’s framing of it. Thus, instead of verifying content factuality, this approach enables message readers to determine the objects of advocacy from the outset.

And while content and source verification are important for testing the message’s veracity, we also need to consider that it can, at times, lure us into the post-truth trap, according to which there are multiple facets of an

argument—all of which are equally tenable. Moreover, by deciphering message objectives, we can determine ideological aspects of message content. Thus, the broad ideologies' approach to critical reading focuses on what Kuhn (2012) referred to as paradigms—here specifically the overarching paradigms, rather than specific truths, are guiding principles. Additionally, this approach enables message readers to identify individual positions on issues and determine who advocates for them and why.

These broad ideologies can be illustrated by the case of Russian trolling denial mechanisms. Denial frames for Russian trolling are driven by two oppositional needs: the need for visibility and the need for obscurity. On the one hand, Russian trolls beg to be noticed to get their messages visible and thus to be able to sway opinions. On the other hand, where message content is concerned, they depend on the obfuscation of issues to achieve their rhetorical objectives. Such dependence on logical obfuscation was discernible in the Russian trolling denial frames underlying analyzed user comments. The goals of these messages are to instill doubt about the existence of Russian trolls and to provoke doubts about agreed-upon issues—whether these are endorsed by a right-leaning or left-leaning readership. Regardless of readers' position along the political spectrum, as long as the comments are divisive, the Russian trolling objective is achieved. These mechanisms of relating to ideologies (whether right-leaning or left-leaning) allow for specific information to be tailored to these values.

While building communities in online spaces is the first and foremost goal for any healthy democratic debate, from the information infrastructure perspective, information communication technologies should strive to further develop technologies that foster network-based trust. Online trust can be achieved based on Donath's (2007) proposed online signaling concept to deal with challenges of online trust. Donath (2007) proposed that signaling comprises assessment, and conventional signals; and they remain relevant in the current media landscape. Assessment signals are the ones that we can evaluate, while conventional signals we take at face value. Most communication online is based on conventional signaling as assessment is not readily available. Regardless of signals' reliability, however, the evaluation of signals can be time consuming. Additionally, such evaluation is complicated in online spaces. Thus, in her discussion of spam as an impediment to online trust, Donath (2007) argued that any malicious actors persist as long as their benefits exceed the costs. Online, such signaling, due to the lack of the direct assessment, is considered a threat to trust in online spaces. Such a lack of direct assessments has translated to genres of online communication that are

based on impostors: email and deceptive spammers—how they could compromise interpersonal trust online or masked foreign agents who pretend to be someone else. Today, trolling and orchestrated influence threaten to subvert the online public sphere. This threat raises some serious questions about the public sphere and information credibility.

Donath's (2007) suggestions can be used to make sense of Russian trolling, especially the creation of more reliable signaling systems. Donath's theory of signaling in social networks has provided a framework for creating checks and balances in network-based online spaces. Moreover, she claimed that receiver costs must be reduced when verifying information. Such measures are intended to create trust among users. In other words, to prevent phenomena such as Russian trolling, online networked structures need to be examined. Such examination enables users to determine how they are interconnected in online spaces. In short, verification systems are needed to maintain trust between users. Thus, trolls use signaling systems while masking their online identities. Since such online masks need to be credible, Russian trolls, in particular, have at their disposal the technological tools for crafting them in multiple ways. The vulnerability of online spaces permits such performative masquerades. And such online vulnerability is addressed through Donath's (2007) concept of the conventional signaling system that permits user self-representation without any trustworthy identity verification system in place. Thus, the goal is to develop the ability to recognize troll masks and to take action accordingly.

Signaling verification, through content, remains challenging due to the prevalence and acceptability of conspiracy theories in our society. Furthermore, this book began with the assertion regarding the covertness of Russian trolling through masking. Such covertness inevitably attracts conspiracy-based narratives about Russian trolling that exploit such online invisibility and masking. Similarly, conditions for launching propaganda about trolling are very favorable due to the preconception that conspiracy theories are self-taught. Thus, as Pipes (1999) argued, conspiracy theory endorses mirror the world of conspiracies, where creators are autodidacts, stigmatized by exclusion from established institutions of learning. Such is the case, even if journalists have consistently exposed Russian trolls through interviews with former IRA employees in St. Petersburg. Although conspiracy theory statements such as "Russian trolls are invented by Democrats" or "Russian trolls are invented by the FBI" is not grounded in supporting evidence, they can still significantly impact public perception on a phenomenon.

Web as a Zero Institution

Stephen O’Leary (2002) lamented that the affective side of news contributes to rumors and disinformation: “It hardly matters how strongly we resist to being drawn into dissemination of propaganda and rumor; in a context so laden by emotion, our work must inevitably contribute to the evolving of cultural myths” (para. 28). This idea can be applied to online comments. By extension, user-generated comments “laden by emotion,” and whose content resemble rumor, contribute toward disinformation and online chaos. It is our role not to become vehicles of the dissemination of disinformation in online spaces.

Similarly, Pratkanis and Aronson (1992) predicted a dark path for democracy. Ojala et al. (2018) continued to warn us regarding the potentials of online media based on enabling unprecedented forms not only of control but also of deception and offense. Today we have become post-publics that are facing what can be called *affective* propaganda, where affective politics play an important role. Yet the goal is to learn how to detect and resist some of the more obvious forms of trickery and demagoguery used in persuasion and to develop an awareness of their consequences. Although many socio-political aspects of the 1960s, in which Choukas (1965) had formulated his observations, have passed into historical archives, such observations remain relevant for us today. Where persuasion politics are concerned, it becomes urgent to recontextualize propaganda within a networked globalized world. As Pratkanis and Aronson (1992) suggested, propaganda models have been appropriated to hone effective persuasion techniques for commercial purposes in democratic contexts. Furthermore, other challenges to combat propaganda effects lie in what Choukas (1965) has cautioned us regarding the propaganda within—anyone can become victims of amplification of information that is not always based on evidence but merely affect.

Can the web function as a zero institution? Will democracy survive in the current online media landscape, where mistrust and the threat of chaos prevail? Scholars like Jodi Dean (2003) said yes, asserting that we are currently inhabiting “neo-democratic” networks. She provided a quasi-utopian vision of the future: “These networks accept that democracy is animated by split: they thrive on it rather than suppress it as a secret. By focusing on contestation instead of legitimation, then neo-democracy acknowledges the unavoidable antagonism of political life” (Dean, 2003, p. 109).

Nevertheless, the consequences of such projections to vouch for the survival of democracy can seem foreboding—particularly when informa-

tion can be manipulating and where chaos is the point, as Rosenberg et al. (2020) argued. While Semaan et al. (2014) were hopeful in seeing how online users took advantage of cross-platform media information providing diverse points of views, this book has made evident that Russian trolling was justified using ideologically charged narratives that emerged as a pattern across news stories and comments and social media posts, which makes the future of online publics uncertain. To combat chaos online, based on the findings of this book, readers are provided with a toolkit to make sense of controversial hardly verifiable positions that are pushed through the same frames across (sociopolitically contrasting) platforms and sources; that should serve as a guide to navigate complex online ecosystems. Regardless of the uncertainties looming before us, it is worth remembering that the future lies in our hands.

Appendix

Four types of data sets were collected for this book. *Breitbart* data included publicly accessible news stories referencing Russian trolling, their publication date, category in which they were placed, and the amount of comments and coding of the amount of Russian troll denial frames found in comments. User names in this study were concealed or changed to preserve user anonymity.

The *New York Times* data included publicly accessible news stories referencing Russian trolling, their publication date, category in which they were placed, and the amount of comments and coding of the amount of Russian troll denial frames found in comments. User names in this study were concealed or changed to preserve user anonymity.

Posts from Gab were collected using keywords “Russian troll” from “top results” and “latest” (Gab allows to sort content based on these categories). This search resulted in approximately 1,500 posts for the “top results” category and for “latest” approximately 240 posts that are publicly accessible without registration. User names in this study were concealed or changed to preserve user anonymity.

Data for Delfi.lt included 787 publicly available comments by registered and anonymous users on a story covering Russian trolling. User names in this study were concealed or changed to preserve user anonymity.

The quantitative coding procedure included binary coding if Russian trolling justification was present or absent. The qualitative coding procedure included subsequent analysis of comments that were labeled as “present” in the quantitative coding to trace Russian troll justification. Iterative coding of the Russian troll denial themes was conducted with new categories added as they emerged from data. Themes were refined by observing the procedure of saturation for each given category.

Duplicate analysis involved automated duplicate identification.

Table 2. Breitbart stories and the proportion of comments with denial frames.

Date	Story	Category	Total comments	Russian troll denial	Denial frames (%)
15 February 2018	Senate Intel Committee Chairman: No Conclusions Yet on Russia Collusion	Politics	119	9	7.6
16 February 2018	Watch: DOJ Announces Indictment of 13 Russians, 3 Russian Entities for Election Interference	Politics	104	94	90.4
16 February 2018	13 Russians Indicted for 2016 Election Interference	Politics	216	112	51.9
19 February 2018	World View: Special Prosecutor Robert Mueller Issues Farcical Indictment of Russian Trolls	National Security	115	38	33.0
20 February 2018	Russian Husband and Wife 'Troll Team' Indicted by FBI for Fake Political Posts	Tech	14	5	35.7
25 February 2018	Devin Nunes: 'The One Thing That's Clear in This Whole Russia Fiasco Is That the Media Is Dead'	Clips	165	130	78.8
10 March 2018	Putin 'Couldn't Care Less' About Russian Interference Claims	Politics	104	9	8.7
11 March 2018	Vladimir Putin Suggests Jews Were Behind Election Interference	Politics	104	16	15.4
20 June 2018	Twitter CEO Jack Dorsey Shared 17 Tweets from 'Russian Trolls'	Tech	554	360	65.0
16 July 2018	Trump: I Addressed 'Directly' with Putin Russian Interference in Elections	Politics	141	8	5.7
2 August 2018	Facebook Concealed Racially Charged Trolling from Foreign Influence Report	Tech	27	1	3.7
20 August 2018	Bokhari: This Is What 'Election Interference' Actually Looks Like	Tech	0	0	0.0
27 September 2018	China Rejects Trump's Allegation of Election Interference	Asia	166	7	4.2
2 October 2018	Report Blames 'Russian Trolls' for Negative Reactions to 'Star Wars: The Last Jedi'	Tech	115	13	11.3
6 November 2018	Facebook Blocks 115 Accounts for 'Coordinated Inauthentic Behavior' Ahead of Midterm Elections	Tech	144	34	23.6
	Total		2088	836	40.0

Table 3. New York Times stories and the proportion of comments with denial frames

Date	Story	Category	Total comments	Russian troll denial frame	Denial frames (%)
21 February 2018	The Trolling of the American Mind	Opinion	763	137	18.0
20 September 2018	Plot to subvert the election	Politics	453	94	20.8
12 October 2018	Operation InfeKtion: A three-part video series on Russian disinformation	Opinion	375	54	14.4
23 September 2018	Russian Trolls Used Vaccine Debate to Sow Discord, Study Finds	Health	85	9	10.6
18 August 2018	For Russian ‘Trolls,’ Instagram’s Pictures Can Spread Wider Than Words	Technology	62	11	17.7
7 November 2018	Russian Trolls Were at It Again Before Midterms, Facebook Says	Technology	40	13	32.5
8 March 2018	How Russian Trolls Crept Into the Trump Campaign’s Facebook Messages	Politics	18	2	11.1
	Total		1796	320	17.8

Bibliography

- About the ODI. (n.d.). *ODI: Open Data Institute*. <https://theodi.org/about-the-odi/>.
- Abrams, S. (2016). Beyond propaganda: Soviet active measures in Putin's Russia. *Connections*, 15(1), 5–31.
- Abramson, S. (2019). *Proof of conspiracy*. New York: Simon and Schuster.
- Adams, A. J. (2018, May). New York Times: *Using AI to host better conversations*. Google AI. <https://blog.google/technology/ai/new-york-times-using-ai-host-better-conversations/>.
- Aksartova, S. (2003). *Television in the Russian Federation: Organisational structure, programme production and audience*. A Report for the European Audiovision Observatory. http://www.infoamerica.org/documentos_pdf/rusia1.pdf.
- Aliaksandrau, A. (2014). Brave new war: The information war between Russia and Ukraine. *Index on Censorship*, 43(4), 54–60.
- Alkas.lt (2014, October). NATO naikintuvai atpažino prie NATO oro erdvės priartėjusį Rusijos karinį žvalgybinį lėktuvą. *Alkas.lt*. <http://alkas.lt/2014/10/23/nato-naikintuvai-atpazino-prie-nato-oro-erdves-priartejusi-rusijos-karini-zvalgybini-lektuva/>.
- Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 31(2), 211–236.
- Almgren, S. M., & Olsson, T. (2015). “Let’s Get Them Involved” . . . to some Extent: Analyzing online News Participation. *Social Media & Society*, 1(2). <https://doi.org/10.1177/2056305115621934>.
- Anceschi, L. (2015). The persistence of media control under consolidated authoritarianism: containing Kazakhstan’s digital media. *Demokratizatsiya: The Journal of Post-Soviet Democratization*, 23(3), 277–295.
- Anderson, A. A., Brossard, D., Scheufele, D. A., Xenos, M. A., & Ladwig, P. (2014). The “nasty effect”: Online incivility and risk perceptions of emerging technologies. *Journal of Computer-Mediated Communication*, 19(3), 373–387.
- Anderson, C. (2013). Dimming the Internet: detecting throttling as a mechanism of censorship in Iran. *Arxiv*. <https://arxiv.org/abs/1306.4361>.
- Andersson, L. M., & Pearson, C. M. (1999). Tit for tat? The spiraling effect of incivility in the workplace. *Academy of Management Review*, 24(3), 452–471.

- Andrejevic, M. (2013). *Infoglut: How too much information is changing the way we think and know*. New York: Routledge.
- Aneja, A., & Ifraimova, S. (2018, May). How to spot a Russian troll. *Time*. <http://time.com/5274785/how-to-spot-a-russian-troll/>.
- Anglin, A. (2016, August). A normie's guide to the alt-right. *Daily Stormer*. <https://web.archive.org/web/20171212095411/https://dailystormer.red/a-normies-guide-to-the-alt-right/>.
- Antonio, R. J., & Brulle, R. J. (2011). The unbearable lightness of politics: Climate change denial and political polarization. *Sociological Quarterly*, 52(2), 195–202.
- Asen, R., & Brouwer, D. C. (Eds.). (2001). *Counterpublics and the state*. New York: SUNY Press.
- Asmolov, G. (2019). The effects of participatory propaganda: From socialization to internalization of conflicts. *Journal of Design and Science* 6. <https://jods.mitpress.mit.edu/pub/jyzg7j6x/release/2>.
- Associated Press. (2018, July). Putin Again Denies Interference in US Election. *Hollywood Reporter*. <https://www.hollywoodreporter.com/news/putin-denies-us-election-interference-fox-news-interview-1127678>.
- Baden, C., & Sharon, T. (2021). Blinded by the lies? Toward an integrated definition of conspiracy theories. *Communication Theory*, 31(1), 82–106.
- Baden, C., & Springer, N. (2014). Com(ple)menting the news on the financial crisis: The contribution of news users' commentary to the diversity of viewpoints in the public debate. *European Journal of Communication*, 29(5), 529–548.
- Baden, C., & Springer, N. (2017). Conceptualizing viewpoint diversity in news discourse. *Journalism*, 18(2), 176–194.
- Bailard, C. S. (2014). *Democracy's double-edged sword: How internet use changes citizens' views of their government*. Baltimore: Johns Hopkins University Press.
- Bakardjieva, M. (2008). Bulgarian online forums as carnival: Popular political forms and new media. In F. Sudweeks, H. Hrachovec, & C. Ess (Eds.), *Proceedings: Cultural attitudes towards communication and technology 2008* (pp. 286–300). Murdoch University, Australia. http://sammelpunkt.philo.at/id/eprint/3633/1/bakardjieva_p.pdf.
- Balčytienė, A., & Juraitė, K. (2017). Media literacy and expanding public spaces: Cultures, policies and risks in the Baltic countries. In I. Wadbring & L. Pekkala (Eds.), *Citizens in a mediated world: A Nordic-Baltic perspective on media and information literacy* (pp. 45–53). Gothenburg: Nordicom.
- Bardon, A. (2019). *The truth about denial: Bias and self-deception in science, politics, and religion*. New York: Oxford University Press.
- Barnes, R. (2018). *Uncovering online commenting culture: Trolls, fanboys and lurkers*. Cham: Springer.
- Barrinha, A. (2018). Virtual neighbors: Russia and the EU in cyberspace. *Insight Turkey*, 20(3), 29–42.
- Bay, M. (2018). Weaponizing the haters: *The Last Jedi* and the strategic politicization of pop culture through social media manipulation. *First Monday*, 23(11). <https://firstmonday.org/ojs/index.php/fm/article/view/9388/7603>.
- BBC (2018, November). How President Trump took “fake news” into the mainstream. BBC. <https://www.bbc.com/news/av/world-us-canada-46175024>.

- Bedford, S., & Vinatier, L. (2018). Resisting the irresistible: “Failed opposition” in Azerbaijan and Belarus revisited. *Government and Opposition*, 54(4), 1–29.
- Bell, C. (2018, February). The people who think 9/11 may have been an “inside job.” *BBC*. <https://www.bbc.com/news/blogs-trending-42195513>.
- Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. New York: Oxford University Press.
- Benner, K., Mazzetti, M., Hubbard, B., & Isaac, M. (2018, October). Saudi’s image makers: A troll army and a Twitter insider. *New York Times Magazine*, <https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html>.
- Bennett, W. L., & Livingstone, S. (2021). A brief history of the disinformation age information wars and the decline of institutional authority. In W. L. Bennett & S. Livingstone (Eds.), *The Disinformation: Politics, Technology, and Disruptive Communication in the United States* (pp. 3–40). Cambridge: Cambridge University Press.
- Berghel, H., & Berleant, D. (2018). The online trolling ecosystem. *Computer*, 51(8), 44–51. <https://doi.org/10.1109/mc.2018.3191256>.
- Bernays, E. L. (1947). The engineering of consent. *Annals of the American Academy of Political and Social Science*, 250(1), 113–120.
- Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 US Presidential election online discussion. *First Monday*, 21(11–7). <https://firstmonday.org/ojs/index.php/fm/article/download/7090/5653>.
- Bevensee, E., & Ross, A. R. (2018, December). The Alt-Right and global information warfare. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 4393–4402). IEEE.
- Beyer, Y., Enli, G. S., Maasø, A. J., & Ytreberg, E. (2007). Small talk makes a big difference: Recent developments in interactive, SMS-based television. *Television & New Media*, 8(3), 213–234.
- Bjola, C., & Papadakis, K. (2020). Digital propaganda, counterpublics and the disruption of the public sphere: The Finnish approach to building digital resilience. *Cambridge Review of International Affairs*, 33(5), 638–666.
- Bloom, P., & Sancino, A. (2019). *Disruptive democracy: The clash between technopopulism and techno-democracy*. Thousand Oaks, CA: SAGE.
- Blumler, J., & Gurevitch, M. (2002). *The Crisis of Public Communication*. London: Routledge.
- BNS. (2017, September 18). Du rusų kariniai lėktuvai pažeidė Lietuvos oro erdvę. *Lrytas.lt*. <https://lietuvsdiena.lrytas.lt/aktualijos/2017/09/18/news/du-rusu-kariniai-lektuvai-pazeide-lietuvos-oro-erdve-2598917/>.
- BNS. (2018a, December). NATO naikintuvai lydėjo ir rusų žvalgybinį orlaivį. *Diena.lt*. <http://www.diena.lt/naujienos/lietuva/salies-pulsas/nato-naikintuvai-lydejo-ir-rusu-zvalgybini-orlaivi-894587>.
- BNS. (2018b, December). Per savaitę NATO naikintuvai keturis kartus lydėjo Rusijos karinius lėktuvus. *Delfi.lt*. <https://www.Delfi.lt/news/daily/lithuania/persavaite-nato-naikintuvai-keturis-kartus-lydejo-rusijos-karinius-lektuvus.d?id=79755565>.
- BNS. (2018c, October). NATO naikintuvai Baltijos šalyse lydėjo du rusų karinius orlaivius. *Delfi.lt*. <https://www.Delfi.lt/news/daily/lithuania/nato-naikintuvai-baltijos-salyse-lydejo-du-rusu-karinius-orlaivius.d?id=79313069>.

- BNS. (2022, February 24). *Dėl karo Ukrainoje Lietuvos naujienų portalai išjungia komentarus po publikacijomis*. Delfi.lt. <https://www.delfi.lt/news/daily/lithuania/del-karo-ukrainoje-lietuvos-naujienu-portalai-isjungia-komentarus-po-publikacijomis.d?id=89547205>.
- Bobba, G. (2019). Social media populism: Features and “likeability” of Lega Nord communication on Facebook. *European Political Science*, 18(1), 11–23.
- Boberg, S., Schatto-Eckrodt, T., Frischlich, L., & Quandt, T. (2018). The moral gatekeeper? Moderation and deletion of user-generated content in a leading news forum. *Media and Communication*, 6(4), 58–69.
- Boler, M., & Davis, E. (2020). Introduction: Propaganda by other means. In M. Boler & E. Davis (Eds.), *Affective politics of digital media: Propaganda by other means* (pp. xii–49). London: Routledge.
- Borchers, N. S. (2011). “Do you really think Russia should pay up for that?” How the Russia-based TV channel RT constructs Russian-Baltic relations. *Javnost—The Public*, 18(4), 89–106.
- Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies*, 26(3), 452–481.
- Botometer. (n.d.). *Botometer*. <https://botometer.iuni.iu.edu/#/>.
- Boutyline, A., & Willer, R. (2017). The social structure of political echo chambers: Variation in ideological homophily in online networks. *Political Psychology*, 38(3), 551–569.
- boyd, d. (2017). Did media literacy backfire? *Journal of Applied Youth Studies*, 1(4), 83–89.
- boyd, d., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230.
- Breitbart (2020). Terms of Use. *Breitbart*. <https://www.breitbart.com/terms-of-use/>.
- Brint, M. E. (2019). *Tragedy and denial: The politics of difference in Western political thought*. London: Routledge.
- Bruns, A. (2019). *Are filter bubbles real?*. Cambridge, UK: Polity Press.
- Bulckaert, N. (2018, July). How France successfully countered Russian interference during the presidential election. *Euractiv*. <https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/>.
- Bulut, E., & Yörük, E. (2017). Mediatized populisms | digital populism: Trolls and political polarization of Twitter in Turkey. *International Journal of Communication*, 11, 4093–4117. <http://ijoc.org/index.php/ijoc/article/view/6702>.
- Burns, A., & Eltham, B. (2009). Twitter free Iran: An evaluation of Twitter’s role in public diplomacy and information operations in Iran’s 2009 election crisis. *Communications Policy & Research Forum*, 322–334.
- Calabresi, M. (2017, May). Inside Russia’s social media war on America. *Time*. <http://time.com/4783932/inside-russia-social-media-war-america/>.
- Carson, T. L. (2010). *Lying and deception: Theory and practice*. New York: Oxford University Press.
- Chakars, J. (2010). Work life in the “Singing Revolution” the experience of journalism in Latvia during the struggle for independence from the Soviet Union. *Journalism History*, 36(2), 105–115.

- Chandler, D. C. (2006). *Empire in denial: The politics of state-building*. London: Pluto.
- Chen, A. (2015, June 7). The Agency. *New York Times Magazine*. http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.
- Chotikul, D. (1986). *The Soviet theory of reflexive control in historical and psychocultural perspective: A Preliminary study* (No. NPS55-86-013). Naval Postgraduate School, Monterey, CA.
- Choukas, M. (1965). *Propaganda comes of age*. Washington, DC: Public Affairs Press.
- Clarke, I. (2018). Stylistic variation in Twitter trolling. In J. Golbeck (Ed.), *Online harassment* (pp. 151–178). Cham: Springer. https://doi.org/10.1007/978-3-319-78583-7_.
- CNN. (2018, June). Russian trolls exploit Castile's death: Russian trolls organized a protest in the US. *CNN*. <https://www.cnn.com/videos/us/2018/06/25/russia-protest-philando-castile-distorting-truth-orig.cnn>.
- Coe, K., Kenski, K., & Rains, S. A. (2014). Online and uncivil? Patterns and determinants of incivility in newspaper website comments. *Journal of Communication*, 64(4), 658–679.
- Cook, J., Lewandowsky, S., & Ecker, U. K. (2017). Neutralizing misinformation through inoculation: Exposing misleading argumentation techniques reduces their influence. *PLOS One*, 12(5). <https://doi.org/10.1371/journal.pone.0175799>.
- Cushion, S. (2012). *The democratic value of news: Why public service media matter*. New York: Macmillan International Higher Education.
- Danet, B. (1998). Text as mask: Gender, play and performance. *Cybersociety*, 2, 129–158.
- Daniel, F., & Millimaggi, A. (2020). On Twitter bots behaving badly: A manual and automated analysis of Python code patterns on GitHub. https://re.public.polimi.it/retrieve/handle/11311/1133355/501163/03_Andrea_Millimaggi.pdf.
- Darczewska, J. (2014). *The anatomy of Russian information warfare. The Crimean operation, a case study*. Warsaw: Ośrodek Studiów Wschodnich im. Marka Karpia. <https://www.ceeol.com/search/book-detail?id=551340>.
- Darczewska, J., & Żochowski, P. (2015). *Russophobia in the Kremlin's strategy. A weapon of mass destruction*. Warsaw: Ośrodek Studiów Wschodnich im. Marka Karpia. <https://www.ceeol.com/search/book-detail?id=551865>.
- Davenport, T. H., & Beck, J. C. (2001). The attention economy. *Ubiquity*, 5, <https://dl.acm.org/doi/10.1145/376625.376626>.
- Davis, E. V. W. (2021). *Shadow warfare: Cyberwar policy in the United States, Russia and China*. Washington, DC: Rowman & Littlefield Publishers.
- Davis, M. (2020). The online anti-public sphere. *European Journal of Cultural Studies*, 24(1), 143–159.
- Dean, J. (2003). Why the net is not a public sphere. *Constellations*, 10(1), 95–112.
- Debunk.eu. (n.d.). About elves. *Digital News Initiative*. <https://debunk.eu/about-elves/>.
- Dedaić, M. N. (2005). Ironic denial: Tobaže in Croatian political discourse. *Journal of Pragmatics*, 37(5), 667–683.
- Degli Carpini, M. X. D., Cook, F. L., & Jacobs, L. R. (2004). Public deliberation, discursive participation, and citizen engagement: A review of the empirical literature. *Annual Review in Political Science*, 7, 315–344.

- Delfi.lt. (n.d.). Delfi.lt Apie [About]. <https://www.Delfi.lt/apie/>.
- Delfi.lt. (2015, March). Kremliaus “trolių” irštva: atskleidė, kas jie tokie. *Delfi.lt* <https://www.Delfi.lt/news/daily/world/kremliaus-troliu-irstva-atskleide-kas-jie-tokie.d?id=67437338>.
- Delfi.lt. (2018, November). Rinkimai—palanki terpė “troliams” skleisti sumaištį. Kibernetinis saugumas. *Delfi.lt*. <https://www.Delfi.lt/multimedija/kibernetinis-saugumas/rinkimai-palanki-terpe-troliams-skleisti-sumaisti.d?id=79509123>.
- Delfi.lt. (2020, May). Į kovą su dezinformacija gali stoti kiekvienas Lietuvos gyventojas: tereikia susipažinti su 6-iomis technikomis *Delfi.lt*. <https://www.Delfi.lt/partnerio-turiny/naujienos/i-kova-su-dezinformacija-gali-stoti-kiekvienas-lietuvos-gyventojas-tereikia-susipazinti-su-6-iomis-technikomis.d?id=84406873><https://getbadnews.Delfi.lt/>.
- Der Spiegel*. (2014, May). How Russia is winning the propaganda war. *Der Spiegel*. <https://www.spiegel.de/international/world/russia-uses-state-television-to-sway-opinion-at-home-and-abroad-a-971971.html>.
- Deuze, M. (2011). Media life. *Media, Culture & Society*, 33(1), 137–148.
- Devanny, J., Dwyer, A., Ertan, A., & Stevens, T. (2021). *The National Cyber Force that Britain Needs?* <https://dro.dur.ac.uk/32900/>.
- Diakopoulos, N. (2019). *Automating the news: How algorithms are rewriting the media*. Cambridge, MA: Harvard University Press.
- Dibbell, J. (2009, September). The assclown offensive: How to enrage the Church of Scientology. *Wired*. <https://www.wired.com/2009/09/mf-chanology/>.
- Diethelm, P., & McKee, M. (2009). Denialism: what is it and how should scientists respond? *European Journal of Public Health*, 19(1), 2–4.
- Disqus (n.d.). What is Disqus? *Disqus*. <https://help.disqus.com/en/articles/1717053-what-is-disqus>.
- Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication*, 13(1), 231–251.
- Dougherty, J. (2014). Everyone lies: The Ukraine conflict and Russia’s media transformation. *Harvard Kennedy School Shorenstein Center on Media, Politics and Public Policy, Discussion Paper Series*.
- Dugin, A. (2015). *Eurasian mission: An introduction to Neo-Eurasianism*. Budapest: Arktos Media.
- Duignan, B. (2020). *Postmodernism*. Britannica. <https://www.britannica.com/topic/postmodernism-philosophy>.
- Dukalskis, A. (2017). *The authoritarian Public Sphere: Legitimation and autocratic power in North Korea, Burma, and China*. London: Routledge.
- Dunlap, R. E., & McCright, A. M. (2011). Organized climate change denial. *The Oxford Handbook of Climate Change and Society*, 1, 144–160.
- Ekspertai.eu (2015, April). Naujaisi reagavimo į orlaivius ir laivus prie Baltijos valstybių sienų duomenys. *Ekspertai.eu*. <http://www.ekspertai.eu/naujaisi-reagavimo-i-orlaivius-ir-laivus-prie-baltijos-valstybiu-sienu-duomenys/?comm=1>.
- Ekström, M., & Westlund, O. (2019). The dislocation of news journalism: A conceptual framework for the study of epistemologies of digital journalism. *Media and Communication*, 7(1), 259–270.
- Elliott, C. (2014, May 4). The readers’ editor on . . . pro-Russia trolling below the

- line on Ukraine stories. *The Guardian*. <https://www.theguardian.com/commentis-free/2014/may/04/pro-russia-trolls-ukraine-guardian-online>.
- Ellis, E. G. (2019, April). Nobody Knows What “Troll” Means Anymore—Least of All Mueller. *Wired*. <https://www.wired.com/story/nobody-knows-what-troll-means-anymore-mueller/>.
- Elsawah, M., & Howard, P. N. (2020). “Anything that causes chaos”: The organizational behavior of Russia Today (RT). *Journal of Communication*, 70(5), 623–645.
- ELTA. (2017, January). NATO naikintuvai keturis kartus lydėjo Rusijos orlaivius. *Letuvos Diena*. <https://lietuvsodiena.lrytas.lt/aktualijos/2017/01/30/news/nato-naikintuvai-keturis-kartus-lydejo-rusijos-orlaivius-668832/>.
- Enli, G. (2015). *Mediated authenticity. How the media constructs reality*. New York: Peter Lang.
- Etim, B. (2017, June 13). The Times sharply increases articles open for comments, using Google’s technology. *New York Times*. <https://www.nytimes.com/2017/06/13/insider/have-a-comment-leave-a-comment.html>.
- European Commission. (2018). *A multi-dimensional approach to disinformation: Report of the independent high level group on fake news and online disinformation*. Luxembourg: Publications Office of the European Union. <https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1>.
- European Commission. (2019). Commission launches call to create the European Digital Media Observatory. <https://ec.europa.eu/digital-single-market/en/news/commission-launches-call-create-european-digital-media-observatory>.
- Ewen, S. (1996). *PR! A social history of spin*. New York: Basic Books.
- Factcheck (n.d.). *Factcheck: A project of the Annenberg Public Policy Center*. <https://www.factcheck.org/>.
- Faris, R., Roberts, H., Ertling, B., Bourassa, N., Zuckerman, E., & Benkler, Y. (2017). Partisanship, propaganda, and disinformation: Online media and the 2016 US presidential election. *Berkman Klein Center Research Publication*, 6. <https://cyber.harvard.edu/publications/2017/08/mediacloud>.
- Fattal, A. L. (2018). *Guerrilla marketing: Counterinsurgency and capitalism in Colombia*. Chicago: University of Chicago Press.
- Fazio, L. K., Brashier, N. M., Payne, B. K., & Marsh, E. J. (2015). Knowledge does not protect against illusory truth. *Journal of Experimental Psychology: General*, 144(5), 993–1002.
- Fenton, N. (2010). *New media, old news: Journalism and democracy in the digital age*. London: Sage.
- Fenton, N. (2018). Fake democracy: The limits of public sphere theory. *Javnost—The Public*, 25(1–2), 28–34.
- Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday*, 22(7–8). <https://firstmonday.org/ojs/index.php/fm/article/view/8005/6516>.
- Ferrara, E., Varol, O., Davis, C., F. Menczer, & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, 59(7), 96–104. <https://doi.org/10.1145/2818717>.
- Festinger, L. (1954). A theory of social comparison processes. *Human Relations*, 7(2), 117–140.

- Fichman, P., & Dainas, A. R. (2019). Graphicons and tactics in satirical trolling on Tumblr.com. *International Journal of Communication*, 13, 4261–4286. <https://ijoc.org/index.php/ijoc/article/view/10288/2781>.
- Fichman, P., & Sanfilippo, M. R. (2016). *Online trolling and its perpetrators: Under the Cyberbridge*. Lanham, MD: Rowman & Littlefield.
- Filer, T., & Fredheim, R. (2016). Sparking debate? Political deaths and Twitter discourses in Argentina and Russia. *Information, Communication & Society*, 19(11), 1539–1555. <https://doi.org/10.1080/1369118X.2016.1140805>.
- Fleishman, G. (2000, December 14). Cartoon captures spirit of the internet. *New York Times*. <https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html>.
- Fraser, D. (2009). “On the Internet, nobody knows you’re a Nazi”: Some comparative legal aspects of Holocaust denial on the WWW. In I. Hare & J. Weinstein (Eds.), *Extreme speech and democracy* (pp. 511–537). Oxford: Oxford Scholarship Online. <https://doi.org/10.1093/acprof:oso/9780199548781.001.0001>.
- Freedom House. (n.d.). Freedom in the world 2018: Russia. *Freedom in the world*. <https://freedomhouse.org/country/russia/freedom-world/2018>.
- Frischlich, L., Boberg, S., & Quandt, T. (2019). Comment sections as targets of dark participation? Journalists’ evaluation and moderation of deviant user comments. *Journalism Studies*, 20(14), 2014–2033.
- Fuchs, C. (2018). Propaganda 2.0: Herman and Chomsky’s propaganda model in the age of the Internet, Big Data and social media. In J. Pedro-Carañana, D. Broudy, & J. Klaehn (Eds.), *The propaganda model today: Filtering perception and awareness* (pp. 71–91). London: University of Westminster Press. <https://doi.org/10.16997/book27.f>.
- Furko, P. (2017). Manipulative uses of pragmatic markers in political discourse. *Palgrave Communications*, 3(1), 1–8.
- Gab. (n.d.). Gab AI INC. <https://gab.com/about/tos>.
- Gaden, G., & Dumitrica, D. (2015). The “real deal”: Strategic authenticity, politics and social media. *First Monday*, 20(1). <https://firstmonday.org/ojs/index.php/fm/article/view/4985/4197>.
- Garrett, R. K. (2009). Echo chambers online?: Politically motivated selective exposure among internet news users. *Journal of Computer-Mediated Communication*, 14(2), 265–285.
- Geiger, R. S. (2017). Beyond opening up the black box: Investigating the role of algorithmic systems in Wikipedian organizational culture. *Big Data & Society*, 4(2), <https://journals.sagepub.com/doi/full/10.1177/2053951717730735>
- Geissler, E., & Sprinkle, R. H. (2013). Disinformation squared: Was the HIV-from-Fort Detrick myth a Stasi success? *Politics and the Life Sciences*, 35(2), 2–99.
- Geissler, E., & Sprinkle, R. H. (2019). Were our critics right about the Stasi? AIDS disinformation and “disinformation squared” after five years. *Politics and the Life Sciences*, 38(1), 32–61.
- Gerschewski, J. (2013). The three pillars of stability: legitimization, repression, and co-optation in autocratic regimes. *Democratization*, 20(1), 13–38.
- Gervais, B. T. (2014). Following the news? Reception of uncivil partisan media and the use of incivility in political expression. *Political Communication*, 31(4), 564–583.

- Gessen, M. (2017). *The future is history: How totalitarianism reclaimed Russia*. New York: Granta Books.
- Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern Age*. Stanford, CA: Stanford University Press.
- Gil de Zúñiga, H., Veenstra, A., Vraga, E., & Shah, D. (2010). Digital democracy: Reimagining pathways to political participation. *Journal of Information Technology & Politics*, 7(1), 36–51.
- Gillespie, T. (2020). Content moderation, AI, and the question of scale. *Big Data & Society*, 7(2). <https://doi.org/10.1177/2053951720943234>.
- Global Stats. (n.d.). *Statcounter: Social Media Stats Lithuania Feb 2021-2022*. <https://gs.statcounter.com/social-media-stats/all/lithuania>.
- Global Stats. (n.d.). *Statcounter: Social Media Stats USA Feb 2021-2022*. <https://gs.statcounter.com/social-media-stats/all/united-states-of-america>.
- Godson, R., & Wirtz, J. J. (2000). Strategic denial and deception. *International Journal of Intelligence and Counterintelligence*, 13(4), 424–437.
- Goffman, E. (1959). *Presentation of everyday self*. New York: Doubleday Anchor Books.
- Goffman, E. (1967). *Interaction ritual: Essays in face-to-face behavior*. Chicago: Aldine.
- Goldschein, E. (2011, September, 30). 10 fake grassroots movements started by corporations to sway your opinion. *Business Insider*. <https://www.businessinsider.com/astroturfing-grassroots-movements-2011-9>.
- Golovchenko, Y., Hartmann, M., & Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation. *International Affairs*, 94(5), 975–994.
- Google News Initiative. (n.d.). *Google*. <https://blog.google/outreach-initiatives/google-news-initiative/>.
- Gorwa, R., & Guilbeault, D. (2020). Unpacking the social media bot: A typology to guide research and policy. *Policy & Internet*, 12(2), 225–248.
- Graham, D. A. (2019, August). Trump says there are some very bad people on both sides. *The Atlantic*. <https://www.theatlantic.com/ideas/archive/2019/08/very-bad-people-both-sides/595654/>.
- Graham, T., & Wright, S. (2014). Discursive equality and everyday talk online: The impact of “superparticipants.” *Journal of Computer-Mediated Communication*, 19, 625–642. <https://doi.org/10.1111/jcc4.12016>.
- Greenfield, R. (2011, December). RIP trolling as social critique. *The Atlantic*. <https://www.theatlantic.com/technology/archive/2011/12/rip-trollingsocial-critique/334207/>.
- Grossman, L. (2006, December). Time’s person of the year: You. *Time*. <http://content.time.com/time/magazine/article/0,9171,1570810,00.html>.
- Grybauskaitė, D. (2019, January). Lithuania’s cyber security experience in Davos. *President Dalia Grybauskaitė*. <https://grybauskaite.lrp.lt/en/press-centre/press-releases/lithuanias-cyber-security-experience-in-davos/31745>.
- The Guardian Editorial. (2015, March 2). The *Guardian* view on Russian propaganda: The truth is out there. *The Guardian*. <https://www.theguardian.com/commentisfree/2015/mar/02/guardian-view-russian-propaganda-truth-out-there#comments>.
- Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics*, 13(1), 42–54. <https://doi.org/10.1017/S1537592714003120>.

- Habermas, J. (2010). The public sphere: An encyclopedia article (1964). *The idea of the public sphere: A reader*, 114–120.
- Hale, V. (2017, July). Foreign influence? Soros & Co. drop \$500k on UK “fact check” org. *Breitbart*. <https://www.Breitbart.com/europe/2017/07/05/george-soros-funds-uk-fact-checker/>.
- Hall, S. (1985). Signification, representation, ideology: Althusser and the post-structuralist debates. *Critical Studies in Media Communication*, 2(2), 91–114.
- Hare, I., & Weinstein, J. (Eds.). (2010). *Extreme speech and democracy*. New York: Oxford University Press.
- Hart, R. P. (2018). *Civic hope: How ordinary Americans keep democracy alive*. Cambridge: Cambridge University Press.
- Hasher, L., Goldstein, D., & Toppino, T. (1977). Frequency and the conference of referential validity. *Journal of Verbal Learning & Verbal Behavior*, 16, 107–112. [https://doi.org/10.1016/S0022-5371\(77\)80012-1](https://doi.org/10.1016/S0022-5371(77)80012-1).
- Hatmaker, T. (2018, May). What we can learn from the 3,500 Russian Facebook ads meant to stir up US politics. *Techcrunch*. <https://techcrunch.com/2018/05/10/russian-facebook-adshouse-intelligence-full-list/>.
- Hazan, B. A. (2017). *Soviet propaganda*. New York: Routledge.
- Heikkilä, N. (2017). Online antagonism of the alt-right in the 2016 election. *European Journal of American Studies*, 12(12–2). <https://journals.openedition.org/ejas/12140>.
- Heinrich, A., & Pleines, H. (2018). The meaning of “limited pluralism” in media reporting under authoritarian rule. *Politics and Governance*, 6(2), 103–111.
- Heiser, J. D. (2014). *“The American empire should be destroyed”: Alexander Dugin and the perils of immanentized eschatology*. Malone, TX: Repristination Press.
- Helmus, T. C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A., & Winkelman, Z. (2018). *Russian social media influence: Understanding Russian propaganda in Eastern Europe*. Santa Monica, CA: Rand Corporation. https://www.rand.org/pubs/research_reports/RR2237.html.
- Herbst, S. (2010). *Rude democracy: Civility and incivility in American politics*. Philadelphia, PA: Temple University Press.
- Herf, J. (2009). *Nazi propaganda for the Arab world*. New Haven, CT: Yale University Press.
- Herring, S., Job-Sluder, K., Scheckler, R., & Barab, S. (2002). Searching for safety online: Managing “trolling” in a feminist forum. *Information Society*, 18(5), 371–384.
- Herring, S. C., & Nix, C. G. (1997, March). Is “serious chat” an oxymoron? Pedagogical vs. social uses of internet relay chat. *American Association of Applied Linguistics Annual Conference*, Orlando, FL. <http://ella.slis.indiana.edu/~herring/aaal.1997.pdf>.
- Hess, A. (2015, January). #IAm: The default mode of showing solidarity in the hashtag era. *Slate*. <https://slate.com/news-and-politics/2015/01/jesuischarlie-the-default-mode-of-showing-solidarity-in-the-hashtag-age.html>.
- Hilton, J. (1953). Calculated spontaneity. *Oxford Book of English Talk*. Oxford, UK: Clarendon Press.

- Hobbs, J. R. (1990). Topic drift. In B. Dorval (Ed.), *Conversational organization and its development* (Vol. 38, pp. 3–22). Norwood, NJ: Ablex Publishing.
- Hodge, E., & Hallgrimsdottir, H. (2019). Networks of hate: The alt-right, “troll culture,” and the cultural geography of social movement spaces online. *Journal of Borderlands Studies*, 35, 563–580.
- Hoffman, A. (2017, November). Here are the memes that Russian operatives shared to influence 2016. *Time*. <http://time.com/5006056/russia-election-2016-memes/>.
- Hofstadter, R. (2012). *The paranoid style in American politics*. New York: Vintage.
- Howard, P. N. (2020). *Lie machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives*. New Haven, CT: Yale University Press.
- Huhtinen, A. M., Streng, M., Särämä, S., & Kotilainen, N. (2018, June). Warfare in hybrid environment: Reflexive control as an analytical tool for understanding contemporary challenges. In *ECSM 2018 5th European Conference on Social Media* (pp. 69–75). Academic Conferences and Publishing.
- Iasiello, E. J. (2017). Russia’s improved information operations: From Georgia to Crimea. *Parameters*, 47(2), 51–63.
- Ihlebaek, K. A., & Holter, C. R. (2021). Hostile emotions: An exploratory study of far-right online commenters and their emotional connection to traditional and alternative news media. *Journalism*, 22(5), 1207–1222.
- Im, J., Chandrasekharan, E., Sargent, J., Lighthammer, P., Denby, T., Bhargava, A., Hemphill, L., Jurgens, D., & Gilbert, E. (2020, July). Still out there: Modeling and identifying Russian troll accounts on twitter. In *12th ACM Conference on Web Science* (pp. 1–10).
- Innovbusiness. (1993, December). О создании холдинговой компании “Российский государственный телерадиотехнический центр “эфир” и российской государственной радиовещательной компании “Голос России.” [How holding company “Russian national telerradiotechnical center “Ether” and Russian national radiomasscommunication company “Russian Voice” were founded.] http://www.innovbusiness.ru/pravo/DocumShow_DocumID_65277.html.
- Iosifidis, P., & Nicoli, N. (2020). *Digital democracy, social media and disinformation*. London: Routledge.
- Ireton, C., & Posetti, J. (Eds.) (2018). *Journalism, “fake news” and disinformation: A handbook for journalism education and training*. Paris: United Nations Educational, Scientific, and Cultural Organization. <https://en.unesco.org/fightfakenews>.
- Jaitner, M. L., & Kantola, H. (2016). Applying principles of reflexive control in information and cyber operations. *Journal of Information Warfare*, 15(4), 27–38.
- Jamieson, K. H. (2018). *Cyberwar: How Russian hackers and trolls helped elect a president what we don’t, can’t, and do know*. New York: Oxford University Press.
- Janckus, T. (2018, November). How to recognize and neutralize the propaganda spreading “trolls” and “bots” that are occupying the Internet. *Delfi.lt*. <https://www.Delfi.lt/en/politics/how-to-recognize-and-neutralize-the-propaganda-spreading-trolls-and-bots-that-are-occupying-the-internet.d?id=79526087>.
- Jang, S. M., & Kim, J. K. (2018). Third person effects of fake news: Fake news regulation and media literacy interventions. *Computers in Human Behavior*, 80, 295–302.

- Jankovicz, N. (2020). *How to lose the information war: Russia, fake news, And the future of conflict*. London: Bloomsbury.
- Jensen, E. (2016, August 17). NPR website to get rid of comments. *NPR Media*. <https://www.npr.org/sections/publiceditor/2016/08/17/489516952/npr-website-to-get-rid-of-comments>.
- Jolley, D., Douglas, K. M., & Sutton, R. M. (2018). Blaming a few bad apples to save a threatened barrel: The system-justifying function of conspiracy theories. *Political Psychology, 39*(2), 465–478.
- Jowett, G. S., & O'Donnell, V. (2018). *Propaganda & persuasion*. Los Angeles: Sage.
- Kalpokas, I. (2019). *A political theory of post-truth*. London: Palgrave Macmillan.
- Kargar, S., & Rauchfleisch, A. (2019). State-aligned trolling in Iran and the double-edged affordances of Instagram. *New Media & Society, 21*(7), 1506–1527.
- Karlova, N. A., & Fisher, K. E. (2013). A social diffusion model of misinformation and disinformation for understanding human information behaviour. *Information Research, 18*(1). <http://informationr.net/ir/18-1/paper573.html#.YAAviahKjIU>.
- Karpan, A. (Ed.). (2018). *Troll factories: Russia's web brigades*. New York: Greenhaven Publishing.
- Katz, E. (1957). The two-step flow of communication: An up-to-date report on a hypothesis. *Public Opinion Quarterly, 21*(1), 61–78.
- Keller, T., Graham, T., Angus, D., Bruns, A., Nijmeijer, R., Nielbo, K. L., Bechmann, A., Neudert, L.-M., Marchal, N., Bradshaw, S., Rossini, P., Stromer-Galley, J., Baptista, E. A., & de Oliveira, V. V. (2020). “Coordinated inauthentic behaviour” and other online influence operations in social media spaces. *AoIR Selected Papers of Internet Research*.
- Kennedy, M. (2017, January, 6). Putin ordered “influence campaign” aimed at US election, report says. *NPR*. <https://www.npr.org/sections/thetwo-way/2017/01/06/508568241/putin-ordered-influence-campaign-to-help-trump-u-s-intelligence-report-says>.
- Khaldarova, I., & Pantti, M. (2016). Fake news: Struggle over news coverage of the Ukrainian conflict. *Journalism Practice, 10*(7), 891–901.
- Khazan, O. (2013, October). Russia's online-comment propaganda army. *The Atlantic*. <https://www.theatlantic.com/international/archive/2013/10/russias-online-comment-propaganda-army/280432/>.
- King, G., Pan, J., & Roberts, M. E. (2017). How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review, 111*(3), 484–501.
- Koopmans, R., & Olzak, S. (2004). Discursive opportunities and the evolution of right-wing violence in Germany. *American Journal of Sociology, 110*(1), 198–230.
- Kottasová, I., & O'Brien, S. A. (2018, October, 29). Gab, the social network used by the Pittsburgh suspect, has been taken offline. *CNN*. <https://www.cnn.com/2018/10/29/tech/Gab-offline-pittsburgh/index.html>.
- Krafft, P. M., & Donovan, J. (2020). Disinformation by design: The use of evidence collages and platform filtering in a media manipulation campaign. *Political Communication, 37*(2), 194–214.
- Kuhn, T. S. (2012). *The structure of scientific revolutions*. Chicago: University of Chicago Press.

- Kurowska, X., & Reshetnikov, A. (2018). Neutrollization: Industrialized trolling as a pro-Kremlin strategy of desecuritization. *Security Dialogue*, 49(5), 345–363.
- Lane, R. E. (1962). *Political ideology: Why the American common man believes what he does*. Glencoe, IL: Free Press.
- Larrain, J. (1991). Stuart Hall and the Marxist concept of ideology. *Theory, Culture & Society*, 8(4), 1–28.
- Lasswell, H. (1950). Propaganda and mass insecurity. *Psychiatry*, 13, 283–299.
- Lee, K., Webb, S., & Ge, H. (2014). The dark side of micro-task marketplaces: Characterizing Fiverr and automatically detecting crowdurfing. In *AAAI International Conference on Weblogs and Social Media (ICWSM)* (pp. 275–284). Palo Alto, CA: Association for the Advancement of Artificial Intelligence.
- Lewandowsky, S., & Cook, J. (2020). *The conspiracy theory handbook*. <http://sks.to/conspiracy>.
- Liñán, M. V. (2010). History as a propaganda tool in Putin's Russia. *Communist and Post-Communist Studies*, 43(2), 167–178.
- Luca, M., & Zervas, G. (2016). Fake it till you make it: Reputation, competition, and Yelp review fraud. *Management Science*, 62(12), 3412–3427.
- Luceri, L., Deb, A., Badawy, A., & Ferrara, E. (2019, May). Red bots do it better: Comparative analysis of social bot partisan behavior. In *Companion Proceedings of the 2019 World Wide Web Conference* (pp. 1007–1012).
- Lyons, M. N. (2017). *Ctrl-alt-delete: The origins and ideology of the alternative right*. Somerville: Political Research Associates. <https://www.politicalresearch.org/2017/01/20/ctrl-alt-delete-report-on-the-alternative-right>.
- Lysenko, V., & Brooks, C. (2018). Russian information troops, disinformation, and democracy. *First Monday*, 22(5). <https://firstmonday.org/ojs/index.php/fm/article/view/8176/7201>.
- Macnamara, J. (2020). *Beyond post-communication: Challenging disinformation, deception, and manipulation*. New York: Peter Lang.
- Magun, A. (2016). Hysterical Machiavellianism: Russian foreign policy and the international non-relation. *Theory & Event*, 19(3). <https://muse.jhu.edu/article/623991>.
- Mansbridge, J. (1999). Everyday talk in the deliberative system. In S. Macedo (Ed), *Deliberative politics: Essays on democracy and disagreement* (pp. 211–239). New York: Oxford University Press.
- Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian internet policy. *Media and Communication*, 5(1), 29–41.
- Mareš, T. (2021). Mass media instrumentalization in foreign policy of states: Russian strategic toolset. In H. Mölder, V. Sazonov, A. Chochia, & T. Kerikmäe (Eds.). *The Russian federation in global knowledge warfare* (pp. 79–106). Cham, Switzerland: Springer.
- Martišius, M. (2014). Rusiško informacinio karo bruožai. *Informacijos Mokslai*, 69, 7–25.
- Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13(1), 114–133.
- Mason, G. (2012). “I am tomorrow”: Violence against Indian students in Australia.

- lia and political denial. *Australian & New Zealand Journal of Criminology*, 45(1), 4–25.
- Matsakis, L. (2018, October). Pittsburgh synagogue shooting suspect's Gab posts are part of a pattern. *Wired*. <https://www.wired.com/story/pittsburgh-synagogue-shooting-Gab-tree-of-life/>.
- Matthews, M. (1978). *Privilege in the Soviet Union: A study of elite life-styles under communism*, London: George Allen & Unwin.
- Mažeikis, G. (2010). *Propaganda and symbolic thinking*. Kaunas: Vytautas Magnus University Press.
- McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *Public Opinion Quarterly*, 36(2), 176–187.
- McVeigh, R., Cunningham, D., & Farrell, J. (2014). Political polarization as a social movement outcome: 1960s Klan activism and its enduring impact on political realignment in Southern counties, 1960 to 2000. *American Sociological Review*, 79(6), 1144–1171.
- Meidutė, A. (2018, October 28). Kremliaus ruporai širsta dėl bausmių “trolliams”: Pasipylė ir grasinimai karu *Delfi.lt*. <https://www.delfi.lt/news/daily/demaskuok/kremliaus-ruporai-sirsta-del-bausmiu-trolliams-pasipyle-ir-grasinimai-karu.d?id=79399331>.
- Michaelsen, M. (2017). Far away, so close: Transnational activism, digital surveillance and authoritarian control in Iran. *Surveillance & Society*, 15(3–4), <https://doi.org/10.24908/ss.v15i3/4.6635>.
- Milburn, M. A., & Conrad, S. D. (1998). *The politics of denial*. Cambridge, MA: MIT Press.
- Miller, D. T. (2021). Characterizing QAnon: Analysis of YouTube comments presents new conclusions about a popular conservative conspiracy. *First Monday*, 26(2), <https://firstmonday.org/ojs/index.php/fm/article/view/10168>.
- Mooney, C. (2012). *The republican brain: The science of why they deny science and reality*. Hoboken: John Wiley & Sons.
- Morozov, E. (2011). *The net delusion: How not to liberate the world*. London: Allen Lane.
- Morris, K. (2000). *British techniques of public relations and propaganda for mobilizing East and Central Africa during World War II* (Vol. 61). New York: Edwin Mellen Press.
- Moses, R. (1989). Denial in political process. In E. L. Edelstein, D. L. Nathanson, & A. M. Stone (Eds.), *Denial: A clarification of concepts and research* (pp. 287–297). New York: Plenum Press.
- Mueller, R. (2019, March). *Report on the investigation into Russian interference in the 2016 presidential election*. Washington, DC. <https://www.documentcloud.org/documents/5955372-Mueller-Report.html#document/p1>.
- Musiani, F. (2019, October). “Digital sovereignty”: Can Russia cut off its Internet from the rest of the world? *The Conversation*. <https://theconversation.com/digital-sovereignty-can-the-russian-internet-cut-itself-off-from-the-rest-of-the-world-125952>.
- Mustonen-Ollila, E., Lehto, M., & Huhtinen, A. (2018, March). Hybrid information environment: Grounded theory analysis. In *Proceedings of the International Conference on Cyber Warfare & Security* (pp. 412–419), University of Chester, UK. <https://doi.org/10.34190/EWS.20.006>.

- Naab, T. K., Heinbach, D., Ziegele, M., & Grasberger, M. T. (2020). Comments and credibility: How critical user comments decrease perceived news article credibility. *Journalism Studies*, 21(6), 783–801.
- Nadler, A. (2020). Pioneering countercultural conservatism: Limbaugh, Drudge, and Breitbart. In M. Bolter & E. Davis (Eds.), *Affective politics of digital media: Propaganda by other means* (pp. 153–169). London: Routledge.
- Nahon, K., & Hemsley, J. (2013). *Going viral*. Cambridge, UK: Polity.
- Nahon, K., Hemsley, J., Walker, S., & Hussain, M. (2011). Fifteen minutes of fame: The power of blogs in the lifecycle of viral political information. *Policy & Internet*, 3(1), 1–28.
- NBC News. (2018, August). Inside a Russian troll factory. *NBC News*. <https://www.nbcnews.com/think/video/inside-a-russian-troll-factory-1265275459562>.
- Newton, C. (2019, February). The trauma floor. The secret floor of Facebook moderators in America. *The Verge*. <https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona>.
- New York Times Home (n.d.). Comments. *New York Times*. <https://help.nytimes.com/hc/en-us/articles/115014792387-Comments>.
- Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2(2), 175–220.
- NPR Editorial (2008, September). NPR launches online community. *NPR*. https://www.npr.org/sections/inside/2008/09/npr_launches_online_community.html.
- Nussbaum, M. (2018, July). A look back at Trump's statements on whether Russia meddled in the election. *Politico*. <https://www.politico.com/story/2018/07/13/trump-statements-russia-meddling-719281>.
- Oates, S. (2013). *Revolution stalled: The political limits of the internet in the post Soviet sphere*. New York: Oxford University Press. <https://doi.org/10.1080/15228886.2015.1012783>.
- Oates, S. (2016). Russian media in the digital age: Propaganda rewired. *Russian Politics*, 1, 398–417.
- Oboler, A., Allington, W., & Scolyer-Gray, P. (2019). *Hate and violent extremism from an online sub-culture: The Yom Kippur terrorist attack in Halle, Germany*, https://www.gedenkstaettenforum.de/fileadmin/forum/2019-4_Report_on_Halle.pdf.
- Ohlin, J. D. (2016). Did Russian cyber interference in the 2016 election violate international law. *Texas Law Review*, 95(7), 1579–1598, <https://texaslawreview.org/wp-content/uploads/2017/11/Ohlin.pdf>.
- Ojala, M., Pantti, M., & Kangas, J. (2018). Professional role enactment amid information warfare: War correspondents tweeting on the Ukraine conflict. *Journalism*, 19(3), 297–313.
- O'Leary, S. (2002). Rumors of grace and terror. *Online Journalism Review*, 5. http://www.ojr.org/ojr/ethics/1017782038.php?__cf_chl_managed_tk__=pmd_W7r2dsNdRumbRsWQLGp9pGv_vYmC0hrO8iyFSU7zYz0-1634512102-0-gqNtZG-zNAuWjcnBszQs9.
- Olin, J. [Josh Olin]. (2022, March 8). The danger of “whatabout-ism” arguments, by John Oliver. [Video]. YouTube. <https://www.youtube.com/watch?v=RS82JNd0YzQ>

- Oliver, J. E., & Wood, T. J. (2014). Conspiracy theories and the paranoid style (s) of mass opinion. *American Journal of Political Science*, 58(4), 952–966. <https://doi.org/10.1111/ajps.12084>.
- Olwert, P. (2014, April). Hired Russians are cyber-bombing the Polish Internet? *Newsweek*. <https://www.newsweek.pl/swiat/wynajeci-rosjanie-cyber-bombarduj-polski-internet-newsweek-cyberatak/yweq02h>.
- Operation InfeKtion (2018, November). Russian disinformation from Cold War to Kanye. Opinion Video Series. *New York Times*. <https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html>.
- Orenstein, M. A. (2019). *The lands in between: Russia vs. the West and the new politics of hybrid war*. New York: Oxford University Press.
- Orwell, G. (2009). *1984*. New York: Everyman's Library.
- O'Shaughnessy, N. (2019). From disinformation to fake news: Forwards into the past. In P. Baines, N. O'Shaughnessy, & N. Snow (Eds.), *The SAGE handbook of propaganda* (pp. 55–70). London: Sage.
- O'Sullivan, P. B., & Carr, C. T. (2018). Masspersonal communication: A model bridging the mass-interpersonal divide. *New Media & Society*, 20(3), 1161–1180.
- Pagán, V. (2012). *Conspiracy theory in Latin literature*. Austin: University of Texas Press.
- Panciera, K., Halfaker, A., & Terveen, L. (May, 2009). Wikipedians are born, not made: a study of power editors on Wikipedia. In *Proceedings of the ACM 2009 International Conference on Supporting Group Work* (pp. 51–60).
- Paolillo, J. C. (2018). The flat earth phenomenon on YouTube. *First Monday*, 23(12). <https://www.firstmonday.org/ojs/index.php/fm/article/view/8251/7693>.
- Papacharissi, Z. (2004). Democracy online: Civility, politeness, and the democratic potential of online political discussion groups. *New Media & Society*, 6(2), 259–283.
- Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age*. Malden, MA: Polity Press.
- Papacharissi, Z. (2015). *Affective publics: Sentiment, technology, and politics*. Oxford: Oxford University Press.
- Papacharissi, Z. (2021). *After democracy: Imagining our political future*. New Haven, CT: Yale University Press.
- Pasitselska, O. (2017). Ukrainian crisis through the lens of Russian media: Construction of ideological discourse. *Discourse & Communication*, 11(6), 591–609.
- Pearce, K. E. (2015). Democratizing kompromat: The affordances of social media for state-sponsored harassment. *Information, Communication & Society*, 18(10), 1158–1174.
- Pearce, K. E., Vitak, J., & Barta, K. (2018). Privacy at the margins: Socially mediated visibility: Friendship and dissent in authoritarian Azerbaijan. *International Journal of Communication*, 12(22), 1310–1331.
- Peck, R. (2019). *Fox populism: Branding conservatism as working class*. Cambridge: Cambridge University Press.
- Phillips, A. (2010). Transparency and the new ethics of journalism. *Journalism Practice*, 4(3), 373–382.

- Phillips, W. (2015). *This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture*. Cambridge: MIT Press.
- Pipes, D. (1999). *Conspiracy: How the paranoid style flourishes and where it comes from*. New York: Simon and Schuster.
- Pitney Jr., J. J., (2001). *The art of political warfare*. Oklahoma: University of Oklahoma Press.
- Polletta, F., & Callahan, J. (2019). Deep stories, nostalgia narratives, and fake news: Storytelling in the Trump era. In J. Mast & J. Alexander (Eds.), *Politics of meaning/meaning of politics* (pp. 55–73). London: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-95945-0_4.
- Pomerantsev, P. (2014). *Nothing is true and everything is possible: The surreal heart of the new Russia*. London: Public Affairs.
- Poushter, A. (2018, October). 6 charts on how Russians and Americans see each other. *Pew Research*. <https://www.pewresearch.org/fact-tank/2018/10/04/6-charts-on-how-russians-and-americans-see-each-other/>.
- Pratkanis, A. R., & Aronson, E. (1992). *Age of propaganda: The everyday use and abuse of persuasion*. New York: Henry Holt.
- Priestly, T. (1996). Denial of ethnic identity: The political manipulation of beliefs about language in Slovene minority areas of Austria and Hungary. *Slavic Review*, 55(2), 364–398.
- Protruth Pledge. (n.d.). *Protruth Pledge*. <https://www.protruthpledge.org/>.
- Public Intelligence. (2000, September). *Information security doctrine of the Russian Federation*. Russian Federation, Ministry of Foreign Affairs <https://publicintelligence.net/ru-information-security-2000/>.
- Purvis, T., & Hunt, A. (1993). Discourse, ideology, discourse, ideology, ideology . . . *British Journal of Sociology*, 44(3), 473–499.
- Quandt, T. (2018). Dark participation. *Media and Communication*, 6(4), 36–48.
- Rae, M. (2021). Hyperpartisan news: Rethinking the media for populist politics. *New Media & Society*, 23(5), 1117–1132.
- Rahimi, B. (2003). Cyber dissent: the internet in revolutionary Iran. *Middle East Review of International Affairs*, 7(3), 101–115.
- Rahimi, B. (2008). The politics of the Internet in Iran. In M. Semati (Ed.), *Media, culture and society in Iran: Living with globalization and the Islamic State* (pp. 37–56). London: Routledge.
- Ramet, S. P. (2007). The denial syndrome and its consequences: Serbian political culture since 2000. *Communist and Post-Communist Studies*, 40(1), 41–58.
- Rand. (n.d.). Tools that fight disinformation online. *Rand*. <https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html>.
- Rapley, M. (1998). “Just an ordinary Australian”: Self-categorization and the discursive construction of facticity in “new racist” political rhetoric. *British Journal of Social Psychology*, 37(3), 325–344.
- Rawnsley, G. D. (2015). To know us is to love us: Public diplomacy and international broadcasting in contemporary Russia and China. *Politics*, 35(3–4), 273–286.
- Reagle, J. M. (2015). *Reading the comments: Likers, haters, and manipulators at the bottom of the web*. Cambridge, MA: MIT Press.

- Reestorff, C. M., & Stage, C. (2016). Media ecologies of crowds and participatory trolling: Muhammad movie trailer (2012) and Happy British Muslims (2014). In C. Fig, J. Loftager, J. Lohmann Stephensen, H. Nielsen, T. Olesen, & M. Sorensen (Eds.), *Democratic public sphere* (pp. 227–260). Aarhus: Aarhus Universitetsforlag.
- Reuters. (2018, October 20). Saudi Arabia deployed Twitter army against critics. *Reuters*. <https://www.reuters.com/article/us-saudi-khashoggi-twitter/saudi-arabia-deployed-twitter-army-against-critics-ny-times-idUSKCN1MU0VB>.
- Roberts, M. E. (2018). *Censored: Distraction and diversion inside China's great firewall*. Princeton, NJ: Princeton University Press.
- Rojas, H. (2010). “Corrective actions” in the public sphere: How perceptions of media and media effects shape political behaviors. *International Journal of Public Opinion*, 22(3), 343–363.
- Romano, A. (2018, October 18). Twitter released 9 million tweets from one Russian troll farm. Here’s what we learned. *Vox*. <https://www.vox.com/2018/10/19/17990946/twitter-russian-trolls-bots-election-tampering>.
- Rosamond, E. (2019). From reputation capital to reputation warfare: Online ratings, trolling, and the logic of volatility. *Theory, Culture & Society*, 37(2), 105–129. <https://doi.org/10.1177/026327641987253>.
- Rosenberg, M., Perlroth, N., & Sanger, D. E. (2020, January). “Chaos is the point”: Russian hackers and trolls grow stealthier in 2020. *New York Times*. <https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html>.
- Rossini, P., Stromer-Galley, J., Baptista, E. A., & Veiga de Oliveira, V. (2020). Dysfunctional information sharing on WhatsApp and Facebook: The role of political talk, cross-cutting exposure and social corrections. *New Media & Society*, 1461444820928059.
- Rossokhovatsky, D., & Khvostunova, O. (2019, July). Why Russia needs a “sovereign Rунet.” *Institute of Modern Russia*. imrussia.org/analysis/3029-
- Roudakova, N. (2017). *Losing pravda: Ethics and the press in post-truth Russia*. Cambridge: Cambridge University Press.
- Roth, Y. (2020, May 18). Bot or not? The facts about platform manipulation on Twitter. *Twitter blog*. https://blog.twitter.com/en_us/topics/company/2020/bot-or-not.
- Rowe, I. (2014). Civility 2.0: A comparative analysis of incivility in online political discussion. *Information, Communication & Society*, 18(2), 121–138.
- RTR Planeta. (n.d.). *RTR*. <http://rtr-planeta.com/>.
- Ruggieri, S., & Boca, S. (2013). At the roots of product placement: The mere exposure effect. *Europe's Journal of Psychology*, 9(2), 246–258.
- Salganik, M., & Lee, R., C. (2020, April). To apply machine learning responsibly, we use it in moderation. *New York Times*. <https://open.nytimes.com/to-apply-machine-learning-responsibly-we-use-it-in-moderation-d001f49e0644?gi=d65b95ddb9fc>.
- Sanfilippo, M., Yang, S., & Fichman, P. (2017). Trolling here, there, and everywhere: How context impacts trolling behaviors. *Journal of the American Society for Information Science and Technology*, 68(10), 2313–2327.
- Sanger, D., & Erlanger, S. (2014). Suspicion falls on Russia as “snake” cyberattacks target Ukraine’s government. *New York Times*. <https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html>.

- Schmuck, D., & Hameleers, M. (2020). Closer to the people: A comparative content analysis of populist communication on social networking sites in pre-and post-election periods. *Information, Communication & Society*, 23(10), 1531–1548.
- Semaan, B. C., Robertson, S. P., Douglas, S., & Maruyama, M. (2014, February). Social media supporting political deliberation across multiple public spheres: Towards depolarization. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (pp. 1409–1421).
- Shane, S. (2017, November 1). These are the ads Russia bought on Facebook in 2016. *New York Times*. <https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html>.
- Siapera, E., Hunt, G., & Lynn, T. (2015). # GazaUnderAttack: Twitter, Palestine and diffused war. *Information, Communication & Society*, 18(11), 1297–1319.
- Siegel, A. (2015). *Sectarian Twitter wars: Sunni-Shia conflict and cooperation in the digital age* (Vol. 20). Carnegie Endowment for International Peace.
- Siegelbaum, L. H. (2011). *Cars for comrades: The life of the Soviet automobile*. Ithaca, NY: Cornell University Press.
- Significant Cyber Incidents. (n.d.). Significant cyber incidents since 2006. *Center for Strategic and International Studies*. https://cis-website-prod.s3.amazonaws.com/s3fs-public/210604_Significant_Cyber_Events.pdf?Ig0rKRzJ9Bc2WS95MJVt1pKZll5eJLE7.
- Simons, G. (2015). Perception of Russia's soft power and influence in the Baltic states. *Public Relations Review*, 41(1), 1–13. <https://doi.org/10.1016/j.pubrev.2014.10.019>.
- Sivets, L. (2021). Controlling free expression “by infrastructure” in the Russian Internet: The consequences of RuNet sovereignization. *First Monday*, 26(5). <https://doi.org/10.5210/fm.v26i5.11698>.
- Snegovaya, M. (2015). Putin's information warfare in Ukraine. *Soviet Origins of Russia's Hybrid Warfare*. Washington, DC: Russia Report. <http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf>.
- Spayd, L. (2016, July). Want to attract more readers? Try listening to them. *New York Times*. https://www.nytimes.com/2016/07/10/public-editor/liz-spayd-new-york-times-public-editor.html?_r=0.
- Spiegel. (2014, May 30). How Russia is winning the propaganda war. *Der Spiegel*. <https://www.spiegel.de/international/world/russia-uses-state-television-to-sway-opinion-at-home-and-abroad-a-971971.html>.
- Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–26.
- Stewart, L. G., Arif, A., & Starbird, K. (2018, February). Examining trolls and polarization with a retweet network. In *Proc. ACM WSDM, Workshop on Misinformation and Misbehavior Mining on the Web*.
- Stroud, N. J., Van Duyn, E., & Peacock, C. (2016). News commenters and news comment readers. *Engaging News Project*, 1-21. <http://mediaengagement.org/wp-content/uploads/2016/03/ENP-News-Commenters-and-Comment-Readers1.pdf>.

- Stromer-Galley J. (2007). Measuring deliberation's content: A coding scheme. *Journal of Public Deliberation*, 3(1). <https://doi.org/10.16997/jdd.50>.
- Stromer-Galley, J. (2019). *Presidential campaigning in the internet age*. New York: Oxford University Press.
- Stukal, D., Sanovich, S., Tucker, J. A., & Bonneau, R. (2019). For whom the bot tolls: A neural networks approach to measuring political orientation of Twitter bots in Russia. *Sage Open*, 9(2), 2158244019827715.
- Su, L. Y. F., Xenos, M. A., Rose, K. M., Wirz, C., Scheufele, D. A., & Brossard, D. (2018). Uncivil and personal? Comparing patterns of incivility in comments on the Facebook pages of news outlets. *New Media & Society*, 20(10), 3678–3699.
- Šuminas, A. (2009). Politinė komunikacija socialinių tinklų svetainėse. *Informacijos Mokslo*, 51, 24–36.
- Sun, L. H., & Fichman, P. (2019). The collective trolling lifecycle. *Journal of the Association for Information Science and Technology*, 71(7), 770–783. <https://doi.org/10.1002/asi.24296>.
- Sunstein, C. R. (2007). *Republic.com 2.0*. Princeton, NJ: Princeton University Press.
- Szulecki, K. (2018). Truth in the time of Infowars: Moral politics and conscience. *East European Politics and Societies*, 32(2), 320–327.
- Tewksbury, D., & Scheufele, D. A. (2009). News framing theory and research. In J. Bryant & M. B. Oliver (Eds.), *Media Effects* (pp. 33–49). Routledge.
- Theus, K. T. (1994). Subliminal advertising and the psychology of processing unconscious stimuli: A review of research. *Psychology & Marketing*, 11(3), 271–290.
- Thomas, K., McCoy, D., Grier, C., Kolcz, A., & Paxson, V. (2013). Trafficking fraudulent accounts: The role of the underground market in Twitter spam and abuse. In 22nd {USENIX} Security Symposium ({USENIX} Security 13) (pp. 195–210).
- Thomas, T. L. (2015). *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*. Foreign Military Studies Office.
- Thornton, R. (2015). The changing nature of modern warfare: Responding to Russian information warfare. *RUSI Journal*, 160(4), 40–48. <https://doi.org/10.1080/03071847.2015.1079047>.
- Timberg, C. (2017, October). Russian operatives used Twitter and Facebook to target veterans and military personnel, study says. *Washington Post*. https://www.washingtonpost.com/news/theswitch/wp/2017/10/09/russian-operatives-used-twitter-and-facebook-to-targetveterans-and-military-personnel-study-says/?utm_term=.81fe659644c5.
- Toepfl, F. (2018). Innovating consultative authoritarianism: Internet votes as a novel digital tool to stabilize non-democratic rule in Russia. *New Media & Society*, 20(3), 956–972.
- Truth Factory. (2022, March 8). McCain and Clinton Bootgate 2017 and Eminem/Russian Collusion. YouTube. <https://www.youtube.com/watch?v=5dl7mJTjOZo>.
- Tsipursky, G. (2017). Towards a post-lies future: Fighting “alternative facts” and “post-truth” politics. *The Humanist*, 77(2), 12–15.
- Twitter Help Center (n.d.). *About verified accounts*. Twitter. <https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts>.
- Usher, N. (2014). *Making news at the New York Times*. Ann Arbor: University of Michigan Press.

- Vaidhyanathan, S. (2018). *Antisocial media: How Facebook disconnects us and undermines democracy*. New York: Oxford University Press.
- Vaišnys A., Kasčiūnas L., Jastramskis M., Keršanskas V., Kojala L., Klimanskis S., Garbačiauskaitė-Budrienė M., & Legatas Š. (2017). *Rusijos Propaganda: Analizė, Įvertinimas, Rekomendacijos*. Vilnius: Rytų Europos studijų centras. https://www.eesc.lt/uploads/news/id987/RESC%20monografija_propaganda.pdf.
- Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. New York: Oxford University Press.
- Van Deursen, A., & Van Dijk, J. (2011). Internet skills and the digital divide. *New Media & Society*, 13(6), 893–911.
- Van Dijck, J., & Poell, T. (2013). Understanding social media logic. *Media and Communication*, 1(1), 2–14.
- Van Dijk, J. A. G. M. (2013). A theory of the digital divide. In M. Ragnedda & G. W. Muschert (Eds.), *The digital divide: The Internet and social inequality in international Perspective* (pp. 49–72). New York: Routledge.
- Van Dijk, J. A. G. M., & Hacker, K. L. (2018). *Internet and democracy in the network society*. Oxford: Routledge.
- Van Dijk, T. A. (1992). Discourse and the denial of racism. *Discourse & Society*, 3(1), 87–118.
- Van Dijk, T. A. (2011). Discourse and ideology. In T. A. Van Dijk (Ed.), *Discourse studies: A multidisciplinary introduction* (2nd ed., pp. 379–407). Los Angeles: Sage.
- Van Gorkum, S. (2019). Hatari does not really want hatred to prevail. *ESC Daily*. <https://www.escdaily.com/hatari-does-not-really-want-hatred-to-prevail/>.
- Volchek D., & Sindelar, D. (2015, March 31). One professional Russian troll tells all. *RFERL*. <https://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html>.
- Wakefield, J. (2019, December). Russia “successful tests” its unplugged internet. *BBC News*. <https://www.bbc.com/news/technology-50902496>.
- Wanless, A., & Berk, M. (2019). The audience is the amplifier: Participatory propaganda. In P. Baines & N. O’Shaughnessy (Eds.), *The Sage Handbook of Propaganda* (pp. 85–104). London: Sage.
- Ward, C. (2020, April 12). Russian election meddling is back—via Ghana and Nigeria and in your feeds. *CNN*. <https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html>.
- Warner, M. (2002). Publics and counterpublics. *Public Culture*, 14(1), 49–90.
- Welch, D. (2013). “Today Germany, tomorrow the world”: Nazi propaganda and total war, 1943–45. In D. Welch (Ed.), *Propaganda, power and persuasion: From World War I to Wikileaks* (Vol. 90, pp. 96–101). New York: IB Tauris.
- Welch, D. (Ed.) (2013). *Propaganda, power and persuasion: From World War I to Wikileaks* (Vol. 90). New York: IB Tauris.
- Wenzel, A. (2020). *Community-centered journalism: Engaging people, exploring solutions, and building trust*. Champaign: University of Illinois Press.
- Wikipedia (n.d.). *Vatnik*. [https://en.wikipedia.org/wiki/Vatnik_\(slang\)](https://en.wikipedia.org/wiki/Vatnik_(slang)).
- Winkler, A. M. (1978). *The politics of propaganda: The office of war information, 1942–1945*. New Haven, CT: Yale University Press.
- Winter, A. (2019). Online hate: From the far-right to the “alt-right” and from the

- margins to the mainstream. In K. Lumsden & E. Harmer (Eds.). *Online othering: Exploring digital violence and discrimination on the Web* (pp. 39–63). Cham: Palgrave Macmillan.
- Woolley, S. (2020). *The reality game: How the next wave of technology will break the truth*. New York: Public Affairs.
- Woolley, S. C., & Guilbeault, D. (2017). *Computational propaganda in the United States of America: Manufacturing consensus online*. <https://ora.ox.ac.uk/objects/uuid:620ce18f-69ed-4294-aa85-184af2b5052e>.
- Woolley, S. C., & Howard, P. N. (Eds.). (2018). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. New York: Oxford University Press.
- Woolley, S., Pakzad, R., & Monaco, N. (2019). German Marshall Fund of the United States. <http://www.jstor.org/stable/resrep21229>.
- Xia, Y., Lukito, J., Zhang, Y., Wells, C., Kim, S. J., & Tong, C. (2019). Disinformation, performed: Self-presentation of a Russian IRA account on Twitter. *Information, Communication & Society*, 22(11), 1646–1664.
- Yablokov, I. (2015). Conspiracy theories as a Russian public diplomacy tool: The case of Russia Today (RT). *Politics*, 35(3–4), 301–315.
- Zabarskaitė, J. (2019). Rusijos Federacijos prezidento V. Putino naratyvų ideologiniai mechanizmai Lietuvos internetinėje žiniasklaidoje. *Parliamentary Studies*, 27, 76–118.
- Zakem, V., McBride, M. K., & Hammerberg, K. (2018). Exploring the utility of memes for US government influence campaigns. *CNA Analysis & Solutions*. https://www.cna.org/cna_files/pdf/DRM-2018-U-017433-Final.pdf.
- Zannettou, S., & Blackburn, J. (2018, September). Propaganda-spewing Russian trolls act differently online from regular people. *The Conversation*. <http://theconversation.com/propaganda-spewing-russian-trolls-act-differently-online-from-regular-people-100855>.
- Zannettou, S., Caulfield, T., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Blackburn, J. (2019). Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the Web. In *Companion Proceedings of the 2019 World Wide Web Conference* (pp. 218–226). ACM.
- Zelenkauskaite, A. (2017). Remediation, convergence, and big data: Conceptual limits of cross-platform social media. *Convergence*, 23(5), 512–527.
- Zelenkauskaite, A., & Balduccini, M. (2017). “Information warfare” and online news commenting: Analyzing forces of social influence through location-based commenting user typology. *Social Media+ Society*, 3(3), <https://doi.org/10.1177/2056305117718468>.
- Zelenkauskaite, A., & Bucy, E. P. (2016). A scholarly divide: Social media, big data, and unattainable scholarship. *First Monday*, 21(5). <https://journals.uic.edu/ojs/index.php/fm/article/view/6358/5511>.
- Zelenkauskaite, A., & Niezgodna, B. (2017). “Stop Kremlin trolls”: Ideological trolling as calling out, rebuttal, and reactions on online news portal commenting. *First Monday*, 22(5). <https://journals.uic.edu/ojs/index.php/fm/article/view/7795/6225>.
- Zelenkauskaite, A., Toivanen, P., Huhtamäki, J., & Valaskivi, K. (2020). Shades of

- hatred online: 4chan duplicate circulation surge during hybrid media events. *First Monday*, 26(1). <https://doi.org/10.5210/fm.v26i1.11075>.
- Zelizer, B. (2004). *Taking journalism seriously: News and the academy*. Thousand Oaks, CA: Sage Publications.
- Žižek, S. (Ed.). (2012). *Mapping ideology*. London: Verso Books.
- Вести Калмыкия (2014, November). Владимир Путин: поддержка русофобии на Украине приведет к катастрофе [Vladimir Putin: Support of Russophobia in Ukraine will lead to a catastrophe]. <https://vesti-kalmykia.ru/news/vladimir-putin-podderzhka-rusofobii-na-ukraine-privedet-k-katastrofe>.
- Гремин, А. (2006, November). 40 Лет По Конвейеру. *Понедельник*. <http://ponedelnik.info/society/40let-pokonveyeru>. [40 years through a conveyor.]
- Камышев, Д., & Болецкая, К. (2014). Владимир Путин наградил более 300 работников СМИ за «объективное освещение событий в Крыму». *Vedomosti.ru* [Vladimir Putin awarded more than 300 workers from the field of the mass information for the “objective coverage of the events in Crimea.”] <http://www.vedomosti.ru/politics/news/26101421/za-vzyatie-kryma#ixzz39hEZAan5>.
- Манойло, А. (2003). *Государственная Информационная Политика в Особых Условиях*. <http://www.psyfactor.org/lib/monografia.zip>. [Government informational politics during special circumstances.]
- Панарин, И., & Панарина, Л. (2003). *Информация Война и Мир*. [Information war and the world] Москва: Олма пресс. ISBN 5-224-04397-2.

Index

- accountability, lack of, 206, 229
- action, channeling of, 161
 - corrective actions, 169–70
 - counteraction, 47, 169–70
- active measures, 88
- advertising, 8, 131, 138, 151, 182, 207, 223, 236, 243
- affect, role of, 4–7, 124, 136, 144–45, 170, 218–19, 226, 233
 - affective propaganda, 255–58, 265–66
 - inauthentic affective narratives, 142
- affiliation tactics, 97, 120–21, 243
 - recommender affiliation, 222, 223–24
- agenda setting, 86, 87
- algorithms, 9, 18, 41, 61, 123–24, 132, 146, 246
- allusive subliminality, 223
- alternative facts, 134, 142, 186, 231–32
- alt-right groups, 135, 214–17, 240–43, 262
- amplification, of messages, 62, 123–24, 132, 174, 230–31, 242–43, 265
- Andrejevic, Mark, 136
- Annenberg Public Policy Center, 167
- anonymity, 6, 30–34, 66–70, 76–79, 94, 123, 175, 246, 267
 - See also* authenticity; invisibility; masking (online identity)
- antidemocratic processes, 131–32
- antipublics, 35, 37, 120–21, 221, 247–48, 257–58, 259
- anti-Semitism, 109–10, 114, 227, 232, 240–42, 248–50
- antivaccination, 232
- anxiety, 236
 - collective, 228, 245
- application programming interfaces (APIs), 41, 62
- appropriation
 - of history, 189–90
 - of ideological frames, 58–59, 136, 159–60, 202, 231, 240–41, 265
 - of online tools, for persuasion, 23, 77, 90, 126, 174, 210
- Aronson, Elliot, 96–97
- artificial intelligence (AI), 62, 129, 140, 165–68, 253
- assimilation, 43–44, 59, 247
- astroturfing, 1, 26–27, 29, 123, 171, 184–86, 246
- The Atlantic* (magazine), 186
- Atlanticism, 189
- attack and defense techniques, 99–100
- attention, redirection of
 - distraction, 100, 114, 182, 185, 195, 223, 227
 - See also* deflection
- attention economy, 78, 240
- authentication, 139, 163, 173
 - See also* bots

- authenticity, 5, 45, 60–64, 76, 80, 128–29, 159–60, 184, 250–58
 authentic opposition, Russian trolls as, 197–202, 209, 214
 coordinated inauthentic behaviors, 2
 genuine participation, 238–39
 mediated, 64
 non-genuine participation, 142–43
 projected, 226, 228
 strategic, 64
 See also anonymity
- authoritarian regimes, 9–11, 89, 124–25, 135–36, 172–73, 259
 new media and information warfare in, 173–77
 totalitarianism, 10–11, 188
 See also delegitimization rhetoric; information warfare, by Russia
- automation, 30, 34, 39, 70, 85, 126–28, 175, 226–27, 246
 artificial intelligence (AI), 62, 129, 140, 165–68, 253
 of comment moderation, 165–66
 computational, 3–9, 19, 28, 66, 82–84, 93–95, 122–25, 184, 239
 machine-learning techniques, 8, 18, 62, 129, 165
 spam, 42, 62, 174, 263–64
 See also bots
- avoidance tactics, 230, 245
- Azerbaijan, online spaces in, 175, 177
- backstage performance, 76
- Baden, Christian, 143, 145, 231
- baiting, 225
- Bakardjieva, Maria, 5, 42–43
- Balčytienė, Auksė, 18
- Bannon, Steve, 240–41
- Belarus, online spaces in, 175
- Benkler, Yochai, 5, 7, 8, 28, 100, 120, 248
- big data, 42
- Bill of Rights (US), 253
- bin Salman, Mohammed, 177
- Black Lives Matter movement, 59, 88
- blaming rhetoric, 34–35, 108–9, 226
- antipublic discourse, 120–21
- blame shifting, 82, 112–13, 222, 224–25, 229
- othering, 35–36, 224–25, 226, 247
- self-blame, 107–9, 222
- unfair treatment, of Russian trolls, 172, 196–97
- zero-sum game, 209–12, 226
See also conspiracy theories; scapegoating
- blue wave, 113, 114
- Bolsonaro, Jair, 246
- bots, 93–94, 183, 243, 253, 256
 botnet, 176
 Botometer, 41–42, 167
 masking (online identity), role in, 46, 50, 56, 61–63, 79, 93–94, 182–83
 mistrust in institutions, role in, 131, 134, 138, 142, 144, 160
 newsbots, 163
 social bots, 62–63
 sockpuppet bots, 62
 See also automation
- bottom-up propaganda flow, 256–57
- boyd, danah, 64
- Brazil, online spaces in, 124
- Breitbart (extreme news site), 65, 82, 119–20, 164, 217–18, 221, 240–45, 262
- data from, 267–68
- denialism on, 226–27, 240–41, 243–44, 245, 254
- disinformation on, 20, 30–35
- Disqus platform, comments via, 66–70, 71, 72, 73, 131, 139, 144
- examples of user comments, 38, 48–52, 57, 69–75, 102–4, 106–7, 109–15, 118, 147–48, 154–56, 196–97, 202–7, 210–11, 214–15, 217
- rules for posting, 138
- Brexit frame, 215–16
- Britain
 British Broadcasting Company (BBC), 178

- propaganda in, 98
 - spies, 107
- broad ideologies, 262
- Bruns, Axel, 146
- Bulgarian news portals, 254
- Business Insider* (news source), 184
- calculated spontaneity, 63
- calling out, of Russian trolls, 34, 39, 47–56, 75, 79, 169–70, 198–99, 211, 250–51, 255
- camouflage and alter ego, mask as, 59–60
- categorization, 98–100
- censorship, 175, 177, 197, 209, 217, 227, 259
 - communication, limiting of, 174
 - infrastructure-based, 178
 - 2000 doctrine, 179–82, 183
 - See also* freedom of speech; silencing
- Center for Strategic and International Studies (US), 175–76
- Central Intelligence Agency (CIA) (US), 2
- Chakars, Janis, 10
- chaos
 - definition of, 80, 260
 - imperviousness to, 255–60
- Charlie Hebdo* (satirical newspaper), 58
- Chen, Adrian, 2
- China, online spaces in, 11, 175, 184–85
- Choukas, Michael, 18–19, 46, 59–60, 79, 90–93, 161, 235, 245–46, 260–61, 265
- Christian-Democrats, 153
- circumspect performers, 55
- clarity, 132–33, 140–41, 159, 161
 - See also* obscurity
- classical propaganda, 34, 80, 84, 88, 95–98, 121–23, 135, 261
- climate change, 230, 232
- Clinton, Hillary, 102–3, 104, 112–13, 119–20, 129, 224–25, 244
- closed society, 96
- coercive diplomacy, 175–76
- Cold War, 171, 245
 - See also* Russia; Soviet propaganda
- collective anxiety, 228, 245
- collective denial, 230
- commenting user typology (CUT)
 - framework, 64–75
 - facets of commenting, 70–71
 - multi-story commenting, 72–73
 - opposition commenting, 73–75
 - private *versus* public commenting, 66–70
 - temporality, of commenting, 71–72
- commercialization of media, 148, 150–52, 153–54
- communication
 - interactional coherence, apositively limiting of, 174
 - post-communication, 17, 257
 - See also* censorship; freedom of speech; silencing
- Communist Party, 12, 14–15, 185
- community-based flagging, 140, 168–70
 - elves (community moderators), 36, 168–70, 210
 - See also* flagging; grassroots movements
- complicity, 54, 148, 261–62
- computational propaganda, 3–9, 19, 28, 66, 82–84, 93–95, 122–25, 184, 239
- conceal distortion, 235
- confirmation bias, 223
- consent, 174–75
- conspiracy theories, 181, 193, 221, 237, 264
- climate change denial, 230, 232
- disinformation, role in, 4–6, 34–35
 - as diversion tactic, 231–34
- flat-earth followers, 232
- Holocaust denial, 232, 249–50
- insider-job, 82, 115, 116–17
- mistrust in institutions, role in, 132, 152–53
- political polarization, role in, 103, 113–17, 120, 122
 - See also* blaming rhetoric

- contagion, of content, 93, 123–24
See also virality
- context collapse, 64
- contextualization, 84, 179, 188
- conversational digression, 225–26
- co-optation, 175
- coordinated inauthentic behaviors, 2
- coordinated messaging, resistance to, 98
- corrective actions, 169–70
- counteraction, 47, 169–70
- counterarguments, 152, 213, 260
- countercultural conservatism, 228–29
- counterfactual elements, 6–7
- counternarrative, 233
- counterpublics, 37, 66, 71, 257–58, 259
- covert propaganda, 57, 59–60, 79, 90
See also overt propaganda
- cracks in society, 3, 74–75, 200–201, 214, 250
 mistrust in institutions, role in, 150, 153–54
 political polarization, role in, 88–89, 99–101, 120
 what about, 105–13
See also political polarization, exploitation of; whataboutism
- credibility, 143, 167, 233, 264
See also institutions, instilling mistrust in
- Crimea, conflict with Russia, 20, 172–73, 191–95
See also Ukraine
- crisis actors, 40
- critical thinking, 248–49, 261–62
- cross-platform analyses, 19–20
- crowdturfers, 186
- culturescape, 240
- Cushion, Stephen, 153
- cybercoercion, 175–76
- cyberwar, 7, 27–28, 45, 85, 190
See also information warfare
- cynicism, 135, 226, 246, 261
- Daily Stormer (white supremacist website), 241
- Danet, Brenda, 33–34, 39, 40
- Darczewska, Jolanta, 20, 193–94
- dark participation, 35–36, 129–32, 136, 146, 162–63, 166, 169–70, 256–57
- data
 big data, 42
 ownership of, 130–31
- Davis, Mark, 7, 35, 120–21, 221, 247–48
- Dean, Jodi, 265
- debate, 4–7, 11, 19, 22
See also democratic deliberation
- debunking, 75–76
 Debunk.eu (fact-checking service), 167
See also prebunking
- decentralization, 19, 23, 89–90, 93, 95, 153, 248, 254
- deception, 4, 60–63, 96, 160, 220, 230, 257, 265
 fake comments, 185–86
 fake news, 3–4, 129, 133–36, 142, 147, 163, 167, 196, 226
 false claims, of Russophobia, 194
 false-flag narratives, 40, 225
 false perception of user empowerment, 130
 fraudulent accounts, 45
 lying, 59–60, 88–89, 229, 230
See also false equivalences
- decision-making processes, 161
- defense and attack techniques, 99–100
- deflection, 1, 34–35, 155, 230, 235, 259
 political polarization, role in, 82, 100
 victim-playing, role in, 182, 196, 204, 208–9, 214–18
See also whataboutism
- delegitimization rhetoric, 154–57, 164, 198, 202–19
- disbelief, 202–4
- dismissal, 204–9, 210, 222, 226, 229, 246
- mockery, 155, 196–98, 205–6, 212–13, 215, 222, 225–26, 234–35, 238
- provocation, 196, 213, 221–22

- zero-sum game, 209–12, 226
See also deflection; legitimization;
 Russophobia frames
- Delfi.lt (Lithuanian news site), 20–21,
 31–33, 45–46, 66, 120, 267
 comment management, 163
 examples of user comments, 58, 117,
 132–33, 150–53, 200–201, 210
 Get Bad News (online game), 164
 rules for posting, 137–38, 139
- democratic deliberation, 37, 79, 94,
 214–15, 231, 234, 245–49
 antidemocratic processes, 131–32
 contexts of, 143–46
 debate, 4–7, 11, 19, 22
 future of, 265–66
 mistrust in institutions, role in, 128–
 29, 133–34, 140–43, 158, 164–
 65
 “neo-democratic” networks, 265
 preconditions of, 136–39
See also freedom of speech; incivility,
 online; participation; public sphere
- Democrats, 111, 113–14, 119–20
- denial frames, 32–33, 76–77, 102, 159,
 267–69
 collective denial, 230
 face-value denial, 207, 219, 222
See also delegitimization rhetoric;
 frames; Russian trolling
- denialism, 1–3, 5, 18, 27, 37, 220–54
 collective denial, 230
 conspiracy theories and, 231–34
 construction, of denial, 222
 definition of, 220
 denial machine, 232
 denial materials, 249–50
 implications of, regarding Russian
 trolling, 221–27
 as procrastination strategy, 229–30
 psychology of, 227–31
 solutions, discussion of, 245–49
 as survival mechanism, 228–29
See also normalization traps to avoid
- Department of Justice (DOJ) (US), 31
- Deuze, Mark, 129
- digital divide, 42, 160
 digitalization, 128
 digital resilience, 260
 digital sovereignty, 178
 digital warfare, 100
 direct manipulation, 90, 91
 disbelief, 202–4
 discursive assimilation, 43–44
 discursive boundary work, 250
 discursive negativity, 238
 discursive opportunities of influence,
 224
 disdainful manipulation, 253
 disinformation, 48, 230–31, 258
 campaigns, 2, 20, 93–94, 142, 192,
 251, 262
 definition of, 1–9, 122, 135, 251
 strategies of, 7, 32
See also misinformation
- dismissal, 204–9, 210, 222, 226, 229,
 246
- disorientation, 5
- Disqus platform, 66–70, 71, 72, 73,
 131, 139, 144
- disruptive actors, 47
 disruptive communication, forms of, 4
 distancing, 49, 229
 distraction, 100, 114, 182, 185, 195,
 223, 227
- diversion, 23, 222–23, 229, 259
- Donath, Judith, 263–64
- doubt, 6, 206, 221, 229, 230–31, 233,
 236, 252, 263
 doubting frame, 159
 uncertainty, 34, 136, 247, 251, 259
- dramatic self-realization, 63–64
 dramaturgic loyalty, discipline, and
 circumspection, 48, 54–55
- Dugin, Alexander, 189
- Dukalskis, Alex, 174–75
- duplicate comments, 67–70, 267
- echo chambers, 146, 259
- elves (community moderators), 36, 168–
 70, 210
- Eminem, 116

- emotional regimes, 144
See also affect, role of
- enablers, of Russian trolling, 54–55, 56
- “The Engineering of Consent” (Bernays), 253–54
- Enli, Gunn, 64
- escapism, 253
- Eurasianism, 189
- European Commission, 166–67
- European Union (EU), 36, 175–76
- evidence, lack of, 203–4, 206, 207–8, 236
- Ewen, Stuart, 253
- expressive coherence, 63–64
- Facebook, 8, 25, 45, 125, 137–38, 158, 163, 168, 185, 243
- face saving strategies, 40, 47–48, 100, 229
- face-value denial, 207, 219, 222
- fact-checking, 133, 164, 166–67
- fake news, 3–4, 129, 133–36, 142, 147, 163, 167, 196, 226
See also deception
- false equivalencies, 106, 112, 120, 136, 147, 154–55, 196, 213
 zero-sum game, 209–12, 226
- false-flag narratives, 40, 225
- Federal Bureau of Investigation (FBI) (US), 2, 116–17, 127–28, 154–57, 212–13, 264
- Ferrara, Emilio, 62–63, 183
- Fichman, Pnina, 23, 225
- filter bubbles, 146
- Finland, online spaces in, 200–201, 260
- First Amendment (US Constitution).
See freedom of speech
- flagging, 163
 community-based, 140, 168–70
See also moderation, of news comments
- flat-earth followers, 232
- 4chan, 8, 70, 199, 242, 248
- Fox News, 113, 120, 150
- frames, 40, 84, 87, 141–42
 doubt-instilling, 159
 false-flag narratives, 40, 225
 hoaxes, 40, 87, 96, 203
 influence, 122
 justification, 24–25, 26, 31, 33, 83
 media framing theory, 31, 60–61, 140, 163, 262
 offense *versus* defense, 99–100
 Russophobia, 20, 32, 36–37, 172–74, 192–94, 195–202, 209, 214, 218–19
 US influence, what about, 105–9
 victim-playing, 20, 58–59, 251, 252
See also denial frames; Russian trolling
- Freedom House, 180
- freedom of speech, 9–10, 15, 36–37, 196, 201–3, 217–19, 242, 250, 253–54
- freedom of expression, 24, 214–15
See also censorship; hate speech; silencing
- Freedom Radio, 180
- frequency, of posting, 68–70, 71–73
 hyperactive posting, 64, 65, 72–73
 superposting, 64
See also commenting user typology (CUT) framework
- fronts, 61–62
 self-staging, 76
See also self-presentation management
- Fuchs, Christian, 123–24
- Gab.com (alt-right social networking site), 2, 20, 24, 30–33, 66–67, 196, 262, 267
 denialism on, 221, 224–25, 232–33, 242, 243–44, 248, 254
 examples of user comments, 57, 104, 106, 109–10, 113–16, 127, 146–47, 156–57, 197–99, 203–4, 207, 215–17, 227–28
 political polarization on, 82, 119–20
 rules for posting, 138–39
- geopolitics, 2, 172, 178–79, 181, 188–90
- Georgia, invasion of, 188, 191
- geotagging, 44

- Gessen, Masha, 10–11, 14, 188
- Get Bad News (online game), 164
- Giddens, Anthony, 261
- Goebbels, Joseph, 96–97
- Goffman, Erving, 33, 39–40, 47–48, 54, 56, 60–65, 68, 76–77, 255
- Google, 137–38, 165–66
- government institutions
- attack on, 154–57, 166–68
 - sponsorship of disinformation by, 21, 23, 27, 28
 - See also* institutions, instilling mistrust in
- grassroots movements, 36, 164, 167, 168–70, 184, 246
- See also* astroturfing; community-based flagging
- The Guardian* (newspaper), 2, 135, 195
- guilt, 107–9, 210–11, 222, 229
- self-guilt, 105–9, 113
- gullibility, 35, 113, 118–19, 122, 160, 203
- gun control, 225
- Habermas, Jürgen, 140, 142, 256, 259
- habituation, 234–36
- hacking, 176
- hard influence, 177, 190–91
- Hatari (Icelandic band), 248
- hate speech, 35, 99, 107, 158, 165, 237, 240–42, 247–48, 250
- See also* freedom of speech
- Herring, Susan, 24, 101, 224
- hierarchy, 15
- historical propaganda. *See* classical propaganda
- Hitler, Adolf, 96–98
- hoax framing, 40, 87, 96, 203
- Hoaxy (fact-checking service), 167
- Holocaust denial, 232, 249–50
- Howard, Philip, 28, 30, 94, 123, 124, 182
- hyperactive posting, 64, 65, 72–73
- See also* frequency, of posting
- hyperpartisan media, 135
- hysterical questioning, 234
- #IAm movement, 58–59
- identity, Russian, 172, 188–91
- ideologies, 251–52, 256, 259
- broad ideologies, 262
 - ideological analyses, 99–100
 - ideological struggle, 252
 - normative, 12
 - of/on the internet, 123–24
 - role in propaganda, 261
- illusory truth effect, 227, 228–29
- Ilyin, Ivan, 189
- immigration, 34–35, 109–11, 120, 200–201, 226, 241
- impersonation, 34, 45, 59, 62, 77
- impression management, 47, 56
- incivility, online, 29–30, 43–44, 138, 158–59, 162, 166, 210, 219, 225
- ambiguity of, 234, 236–39
 - definition of, 238
 - simulated civility, 177
- incomplete knowledge, 252
- indictment, of Russian trolls, 72, 73, 75, 107, 116, 127, 147–48, 173
- infiltration, 79, 192, 238
- influence, 83–90, 121–22, 133, 161–62, 242
- frames of, 122
 - hard, 177, 190–91
 - mutual, 144
 - what about US influence, 105–9
 - See also* persuasion; soft influence
- information
- circulation of, 139–40
 - diffusion practices, 26
 - flooding of, 27, 173, 227, 258–59
 - infoglut, 27, 258–59, 261
 - information bubbles, 123
 - information paralysis, 5
 - “maintenance” of, 188–89
 - misinformation, 3–4, 7, 9, 163
 - regulation of, 178
 - seeding of, 93
 - unverifiability of, 94, 96, 114, 233, 259
 - See also* disinformation; information warfare

- Information Security Doctrine of the Russian Federation, 179–82, 183
- information warfare, 18–23, 26–30, 84–85, 93, 114, 130, 135, 238, 247–48
- cyberwar, 7, 27–28, 45, 85, 190
- digital warfare, 100
- historical conditions, 191–92, 219
- hybrid tactics, 191, 192, 195, 219, 248
- imperviousness to chaos, 255–60
- new media in authoritarian regimes, 173–77
- news comments as zones of, 139–43
- user-generated content, 20–23, 32–33, 87–89, 121–23, 125–26, 158–61, 169–70
- See also* cyberwar; delegitimization rhetoric; victim-playing
- information warfare, by Russia, 177–95
- 2000 Doctrine, 179–82, 183
- by Internet Research Agency (IRA), 182–86
- reflexive control as soft influence, 186–87
- reinstating national pride, 188–91
- Ukraine, Russian trolling and, 191–95
- InfoStream.co (fact-checking service), 167
- infrastructure-based censorship, 178
- inoculation theory, 76
- “Inside a Russian Troll Factory” (video story, NBC News), 164
- insider-job conspiracy theories, 82, 115, 116–17
- “Inside Russia’s Social Media War on America” (Calabresi), 131–32
- Instagram, 24, 25, 125, 176–77
- institutions, instilling mistrust in, 35–36, 127–70, 222, 226, 247
- contexts that situate online public deliberation, 143–46
- government institutions, attack on, 154–57
- grassroots initiatives, 168–70
- media as an institution, discrediting, 146–54
- news deliberations, comments as forms of, 136–39
- news portal comments as information warfare zones, 139–43
- solutions, 162–68
- solutions, discussion of, 157–62
- See also* media, living in
- interactional coherence, 101–2
- Internet Protocol (IP) address concealment, 34, 44, 45–46, 66, 79, 138, 139
- Internet Research Agency (IRA) (Russia), 24–25, 38–39, 43, 45–46, 48, 172, 182–86, 264
- intimidation, 175, 177
- introspection, 216
- invisibility, 34, 77–79, 83, 85, 90, 93, 186–87, 233–37, 264
- of masks, 41–42, 56
- See also* anonymity; visibility
- Iran, online spaces in, 177
- ironic parody, 229
- Islamic State, 97, 198–99
- Islamophobia, 109, 111, 248
- Jamieson, Kathleen, 26, 27–28, 45, 55, 85, 87
- Japanese propaganda, 98
- #JeSuis movement, 58–59
- Juraitė, Kristina, 18
- justification frames, 24–25, 26, 31, 33, 83
- See also* denial frames; frames; Russian trolling
- Kalpokas, Ignas, 136
- Kaspersky antivirus software, 176
- Kazakhstan, online spaces in, 175
- Kennedy, John F., 212
- Khashoggi, Jamal, 177
- knowing, act of, 161
- kolkhoz (Soviet collective farm), 15
- Kremlin trolls, 132–33, 151–52

- Kuhn, Thomas, 11, 263
- Ku Klux Klan, 75
- language, 11–12
 offensive, 156
 of speculation, 6
The Last Jedi (film), 242
- lateral sense-making efforts, 84
- legality, of trolling, 138–39, 196, 202, 205, 206–7, 208–9
- Lega Nord (Italian far-right political party), 226
- legitimization, 172–75, 180–81, 208–11, 224, 245, 250, 253
 of consensus, 173, 174
 self-legitimization, 214
See also delegitimization rhetoric
- Lenin, Vladimir, 12, 13
- Le Pen, Marine, 89, 104
- limited pluralism, 173, 177
- literacy, 74
 media literacy, 16–19, 52–53, 118–19, 163–67, 231, 245–46, 260–64
- Lithuania, 11–12, 35, 125, 166
 cyberattacks in, 176
 Debunk.eu, 167
 elves (community moderators), 36, 168–70, 210
 independence of, 15–16, 190
 Russian trolling in, 2–3, 20–21, 25, 32, 34, 173, 195
See also Delfi.lt (Lithuanian news site)
- little Octobrists, 12, 13
- location, as mask, 44–46
- logic, lack of, 159, 213, 218–19, 220, 222, 225, 233, 250
See also false equivalencies
- lying, 59–60, 88–89, 229, 230
See also deception
- machine-learning techniques, 8, 18, 62, 129, 165
- Malaysian Airlines Flight 17, 63
- manipulation
 direct, 90, 91
 disdainful, 253
 propagandistic, 46
 self-manipulation, 122
- marginalia, news comment treatment as, 6, 8, 22, 30, 35, 143
- Martišius, Mantas, 190, 191, 194
- masking (online identity), 24, 29, 31, 33–34, 38–80, 235–36, 264
 propaganda as, 59–60
 solutions, discussion of, 75–79
 text as mask, 33–34, 39–40, 78
See also anonymity; authenticity; commenting user typology; invisibility; performativity
- masking (online identity), paradoxes of, 40–46
 invisibility, 41–42
 location as mask, 44–46
 play, masks at, 42–44
- masking (online identity), subversiveness of, 46–56
 defensive attributes, 47–56
 protective measures, 56
- mass media, 85–87, 89–90, 122–23, 140–41, 144–46, 158, 253
 commercialization of, 148, 150–52, 153–54
- masspersonal communication, 18
- Mažeikis, Gintautas, 10, 12
- media
 as an institution, discrediting, 113, 146–54
 hyperpartisan, 135
 living in, 129–36
 media ecosystems, 83–84, 125, 135, 143–44, 160, 177–82, 240, 250, 253–54, 262
 media framing theory, 31, 60–61, 140, 163, 262
 media literacy, 16–19, 52–53, 118–19, 163–67, 231, 245–46, 260–64
 mediatization, 136
 new media and information warfare in authoritarian regimes, 173–77
 post-truth, exploiting, 132–36
See also frames; news comments
- mediated authenticity, 64

- messaging frames, 160–61
 methodology, 30–37, 267–69
 #MeToo movement, 88
 Microsoft, 176
 mimicking, 226
 “mirroring sides” guilt, 210–11
 See also zero-sum game
 miscommunication, 47
 misconception, 252
 misinformation, 3–4, 7, 9, 163
 See also disinformation
 misrepresentation theory, 252
 mistrust, 34, 77–78, 80, 263–64
 See also institutions, instilling mistrust
 in
 mitigation, 229
 mobilization discourse, 100
 mockery, 155, 196–98, 205–6, 212–13,
 215, 222, 225–26, 234–35, 238
 moderation, of news comments, 162–68
 Moderator (machine-learning sys-
 tem), 165
 See also flagging
 modernism, 142–43, 161
 See also postmodernism; post-
 positivism
 Mueller, Robert, 24–27, 31, 115–16,
 154–56, 183, 219, 230–31, 239–
 40
 indictment of Russian trolls, 72, 73,
 75, 107, 116, 127, 147–48, 173

 Nadler, Anthony, 228–29
 narco-trafficking, 156–57
 narratives, oppositional, 161
 national interest, 91–92
 national pride, reinstating, 188–91
 National Public Radio (NPR) (US), 165
 National Security Agency (NSA) (US),
 2, 176
 National Socialism, 97
 Nazi Germany, 93, 95, 96–98, 248, 256
 NBC News, 164
 neo-Eurasianism, 189
 neoliberal critiques, 150–51, 153–54
 network propaganda, 28, 30

 neutrollization, 5
 new media, in authoritarian regimes,
 173–77
 newsbots, 163
 news comments, 8–9, 19–22, 28–29,
 32–33, 128–29, 195
 archival of, 139
 as forms of deliberation, 136–39
 as information warfare zones, 139–43
 management of, 162–68
 marginalia, treatment as, 6, 8, 22, 30,
 35, 143
 recommender affiliation, 222, 223–24
 See also Breitbart; commenting user
 typology; delegitimization rhetoric;
 Delfi.lt; Gab.com; institutions,
 instilling mistrust in; *New York*
 Times
 news comments, tactics used in, 102–19
 conspiracy theories, 113–17
 cracks in society, what about, 109–13
 gullibility, 118–19
 self-guilt, 105–9
 news comments, victim-playing Russian
 trolls in, 195–202
 authentic opposition, Russian trolls
 as, 197–202
 unfair treatment, of Russian trolls,
 172, 196–97
New York Times (magazine), 2, 31–33,
 35, 159, 177, 196, 243–45
 comment management, 162, 165–66
 data from, 267, 269
 denialism in, 221, 243–44, 245, 254
 examples of user comments, 51–54,
 81, 104–5, 108–9, 116–19, 148–
 50, 157, 199–200, 203–4, 207–9,
 211, 216, 249, 260
 masking (online identity) in, 66, 77
 Operation InfeKtion (video series), 88,
 157, 164, 229–30
 political polarization in, 82, 119–20
 rules for posting, 137, 139, 140
 noncooperative audience, 76–77
 nonparticipation, 261–62
 normalization traps to avoid, 234–45

- definitional trap, 234, 239–43
 habituation, 234–36
 incivility online, ambiguity of, 234, 236–39
 partisan division, exploited, 234, 243–45
 normative ideology, 12
 North Atlantic Treaty Organization (NATO), 176, 190, 194
- Obama, Barack, 103, 104–5, 119–20, 224–25
 obscurity, 7, 26, 133, 211, 236, 263
 masking (online identity), role in, 40–41, 44, 57, 70
 political polarization, role in, 82, 85
See also clarity
- occurrence of incidents, 47
 Oliver, John, 101
 online voting systems, 174
 Open Data Institute, 130
Operation InfeKtion (*New York Times* video series), 88, 157, 164, 229–30
 Orenstein, Mitchell, 20, 189, 247–48
 Orwell, George, 10–11
 othering, 35–36, 224–25, 226, 247
 overt propaganda, 59, 79
See also covert propaganda
- Panarin, Igor, 187
 Papacharissi, Zizi, 4, 17, 237
 paradigms, 262–63
 Kuhn, Thomas, 11, 263
 paranoid arguments, 225, 234
 participation
 nonparticipation, 261–62
 participatory propaganda, 125
 user participation online, 137–38, 141–42, 158–59, 163, 250
 partisan politics. *See* political polarization, exploitation of
Patriot (Indian newspaper), 96
 Pearce, Katie, 174
 Pentagon (US), 132
 performativity, 39, 54, 55–64, 78, 264
 camouflage and alter ego, mask as, 59–60
 circumspect performers, 55
 dramatic self-realization, 63–64
 performance theory, 33, 65, 76, 77
 performative packaging, 78–79
 persistent performance, 60–63
 self-presentation management, 40, 60–61, 64, 66, 80, 144, 229, 255
See also face saving strategies; masking (online identity)
- persuasion, 3–4, 18–19, 40, 46, 83, 91, 245, 253–54
 communication persuasion models, 85–87
 frameworks of, 84–85
 frameworks of information persuasion, 84–85
 habituation as, 236
 mass persuasion, 245–46
See also influence; propaganda
- Phillip Morris, 184
 Phillips, Whitney, 225, 240
 Pittsburgh synagogue shooting (2018), 242
- pledge of truth, 134–35
 Poland, online spaces in, 124, 195
 political polarization, exploitation of, 8, 34–35, 81–126, 146, 216–17, 262
 communication persuasion models, 85–87
 communicative tactics, 98–102
 denialism, role in, 224–25, 234, 243–45, 248
 frameworks of information persuasion, 84–85
 hyperpartisan media, 135
 provocation, 196, 213, 221–22
 solutions, discussion of, 119–21
See also news comments, tactics used
- in; propaganda, mechanics of
- politics
 dubious practices, 123
 echo chambers, 146, 259
 mudslinging, 82
 political trolling, 225

politics (*continued*)

- politico-historical narratives, 193–94
- post-truth, 136
- populism, 226, 228–29, 248
 - technopopulism, 246
- post-communication, 17, 257
- postmodernism, 10, 16–17, 134–36, 142–43, 159, 161, 233, 259
 - See also* modernism
- post-positivism, 218–19, 244
- post-publics, 1, 37, 257–60, 265
- post-truth, 173, 257, 262–63
 - denialism, role in, 221, 233, 239–40, 244
 - exploitation of, 132–36
 - mistrust in institutions, role in, 147, 158, 161, 163
 - See also* conspiracy theories
- Pratkanis, Anthony, 96–97, 248–49, 261–62, 265
- prebunking, 75–76
 - See also* debunking
- preconceived notions, exploitation of, 228–29
- preestablished fronts, 61, 62
- priming, 86, 87
- propaganda, 46, 235
 - affective, 255–58, 265–66
 - bottom-up flow, 256–57
 - British, 98
 - classical, 34, 80, 84, 88, 95–98, 121–23, 135, 261
 - computational, 3–9, 19, 28, 66, 82–84, 93–95, 122–25, 184, 239
 - counterfactual elements, 6–7
 - covert, 57, 59–60, 79, 90
 - critical thinking to counter, 248–49
 - definition of, 3–7, 90
 - versus* education, 260–61
 - “hater” propagandists, 242
 - imperviousness to, 255–57
 - instruments of, 187
 - in Japan, 98
 - in Latin literature, 120
 - as mask, 59–60
 - media literacy, 16–19, 52–53, 118–19, 163–67, 231, 245–46, 260–64

- models of, 256
 - in Nazi Germany, 93, 95, 96–98, 248, 256
- network, 28, 30
- overt, 59, 79
- participatory, 125
- Propaganda 2.0, 19
- propaganda addiction, 245
- propaganda playbook, 229–30
- prototypical elements of, 6–7
- rewired, 81
 - in school curricula, 12–14, 16–17
 - See also* influence; Soviet propaganda
- propaganda, mechanics of, 87–98
 - computational, 93–95
 - historical, 95–98
 - operational, 92
 - pre-operational, 92
 - tactical, 92
- provocation, 196, 213, 221–22
- public sphere, 1–3, 5, 35–36, 145, 169–70, 179–80, 186–87, 230, 256–60
 - affective publics, 4, 265–66
 - antipublics, 35, 37, 120–21, 221, 247–48, 257–58, 259
 - counterpublics, 37, 66, 71, 257–58, 259
 - Habermas, Jürgen, 140, 142, 256, 259
 - post-publics, 1, 37, 257–60, 265
 - public ambivalence, 76–77
- public sphere, in online spaces, 37, 124, 259–60, 264
 - denialism in, 237, 250, 254
 - disinformation in, 1–3, 5, 10
 - masking (online identity) in, 60, 79
 - mistrust in institutions, 162, 169–70
 - victim-playing in, 179–80, 186, 197, 209
- Putin, Vladimir, 72, 120, 136, 178, 188–89, 192, 194, 212, 245
- QAnon, 115
- Quandt, Thorsten, 132
- quinquennial plan, 12–13

- racism, 74–75, 110–11, 227, 240–41, 247, 248
- Radio Free Europe, 108–9
- rage, effects of, 247–48
- reactive strategies, 75
- Reagan, Ronald, 254
- rebuttal responses, 75
- recommender affiliation, 222, 223–24
- Reddit, 28, 248
- reflexivity
 - reflexive control, 186–87
 - reflexive modernization, 261
 - self-reflexivity, 261
- repetition, 97–98, 163, 193–94, 226–27, 256
 - contagion, of content, 93, 123–24
 - duplicate comments, 67–70, 267
 - virality, 6, 89, 93, 123, 142, 231
- repression, 175
- Republicans, 74, 82, 113, 120, 214, 217
- resonance, 224
- rewired propaganda, 81
- Roberts, Margaret, 173, 227, 259
- Rome, ancient, propaganda in, 120
- RTL Planeta (state-owned broadcaster in Russia), 181
- ruble troll, 151
- rules, for user comments, 61–62, 70, 137–39
 - community-based flagging, 140, 168–70
- rumors, 6, 8, 89, 93–94, 96, 132, 231, 232
- Runet (Russian computer network), 178–79
- Russia
 - Cold War, 171, 245
 - Crimean conflict, 20, 172–73, 191–95
 - Georgia, invasion of, 188, 191
 - Internet Research Agency (IRA), 24–25, 38–39, 43, 45–46, 48, 172, 182–86, 264
 - national identity, 172, 188–91
 - Russian Voice, 181
 - “Russia’s Online-Comment Propaganda Army” (Khazan), 186
 - Russia Today* (RT) (news source), 147, 181–82, 221
 - 2000 Doctrine, 179–82
 - Ukraine, conflict with, 36, 63, 134, 169, 173, 188, 191–95
 - See also* information warfare, by Russia; Russophobia frames; Soviet propaganda
- Russian trolling
 - calling out of, 34, 39, 47–56, 75, 79, 169–70, 198–99, 211, 250–51, 255 (*See also* trolling)
 - definitional trap, 234, 239–43
 - definition of, 27
 - enablers of, 54–55, 56
 - “feeding” of, 150–51
 - indictment of, 72, 73, 75, 107, 116, 127, 147–48, 173
 - Kremlin trolls, 132–33, 151–52
 - narrative of, 32
 - politicization of, 243–45
 - prototypes of, 65
 - ruble trolls, 151
 - self-sabotage, 39, 56–64
 - as “sock puppets,” 186
 - treatment of, as subcultural phenomenon, 239–42
 - troll farms, 2, 19, 162, 164, 177, 183
 - vatniks, 151–52
- Russophobia frames, 20, 32, 36–37, 172–74, 192–94, 195–202, 209, 214, 218–19
 - See also* delegitimization rhetoric; victim-playing
- sabotage
 - of Russian trolls, 47–56
 - self-sabotage, 39, 56–64
 - See also* calling out, of Russian trolls
- Sanders, Bernie, 103–4
- Sanfilippo, Madelyn, 23, 225
- sarcasm, 49, 52, 57–58, 111, 153, 212
- Saudi Arabia, online spaces in, 177
- scapegoating, 150, 204, 244
 - political polarization, role in, 82, 102–4, 106–7, 110–11, 119–20

- scapegoating (*continued*)
 victim-playing, role in, 211, 214–17
See also blaming rhetoric
- school curricula, propaganda in, 12–14, 16–17
- seeding, of information, 93
- self-blame, 107–9, 222
See also conspiracy theories
- self-guilt, 105–9, 113
- self-legitimization, 214
- self-manipulation, 122
- self-presentation management, 40, 60–61, 64, 66, 80, 144, 229, 255
See also fronts
- self-reflexivity, 261
- self-sabotage, 34, 56–64
- self-staging, 76
See also fronts
- self-victimization frame. *See* victim-playing
- Semaan, Bryan, 266
- SemanticForce.net (fact-checking service), 167
- semantic media literacy, 261
- sense-making process, 133, 137, 141, 144, 158, 231
 lateral, 84
- “shared responsibility” argument, 211–12
- signaling, online, 263–64
- silence
 as a form of a democratic participation repertoire, 17–18
 silent countermovement, 15–16
- silencing, 175, 177, 186, 251
 prohibited debate topics, 11
 silenced generation, 10–15
See also censorship; freedom of speech
- skepticism, 17, 25–27, 134, 170, 208, 236, 245, 257–58, 259
- social conflict, 247
- social media, 8, 64, 86, 95, 122–23, 144, 165, 174
 Disqus platform, 66–70, 71, 72, 73, 131, 139, 144
 Facebook, 8, 25, 45, 125, 137–38, 158, 163, 168, 185, 243
 4chan, 8, 70, 199, 242, 248
 Google, 137–38, 165–66
 Instagram, 24, 25, 125, 176–77
 Reddit, 28, 248
 vulnerabilities of, 17–23
 Web 2.0, 10, 19, 143, 144, 259–60
 WhatsApp, 28, 130, 246
 Wikipedia, 61, 169
 Yahoo, 137–38, 176
 Yelp, 184
 YouTube, 101, 116, 125, 181, 232
See also Gab.com; news comments; Twitter
- social order, maintenance of, 174
- societal perception, change in, 249–50
- sociotechnicality, 7–9, 19, 30, 250
 masking (online identity), role in, 40, 44, 58, 66, 78
 mistrust in institutions, role in, 137, 173–74
 political polarization, role in, 86, 94–95, 115
- soft influence, 21, 132, 171, 177, 179, 191, 257, 258, 260
 reflexive control as, 186–87
- solidarity, 14, 54, 57–59, 198, 209
- solutions, to Russian trolling, 37, 75–79, 119–21, 157–68, 245–49, 260–64
- Soros, George, 50, 113, 114–15, 117, 164, 210–11
- source verification, 134, 163, 262–63
- Soviet propaganda, 26, 88, 96, 98, 100, 122, 135–36, 187
 Cold War, 171, 245
 historical lens, 9–17
 tactics, 76–77
See also Russia
- spam, 42, 62, 174, 263–64
- speculation, language of, 6
- Spiegel* (German newspaper), 191, 195
- sports stories, compared to Russian trolling stories, 67–68
- Springer, Nina, 143, 145
- Starbird, Kate, 3, 40

- Star Wars* (film series), 242
- strategic authenticity, 64
- strategic information operations, 3, 179
- subliminality, 223, 236, 244
- Šuminas, Andrius, 125
- superposting, 64
- See also* commenting user typology (CUT) framework; frequency, of posting
- surveillance, 174, 175, 176–77, 178, 207
- Syria, online spaces in, 198–99, 201
- tactful inattention, 56
- Taiwan, online spaces in, 124, 167
- targeted trolling, 242
- technopopulism, 246
- text, 99
- as mask, 33–34, 38, 39–40, 78
- third parties, 139, 144, 174, 176
- Disqus platform, 66–70, 71, 72, 73, 131, 139, 144
- outsourcing of comment management to, 163, 165, 166
- third-person effect, 122
- Time* (magazine), 130, 131–32, 159
- tone, of messages, 226, 238
- Torba, Andrew, 242
- totalitarianism, 10–11, 188
- transparency, of journalistic practice, 133–34
- trolling, 23–30
- characteristics of, 24, 164, 212–13
- definitional trap, 234, 239–43
- definition of, 10, 23–24
- false-flag, 225
- government sponsorship of, 21, 23, 27, 28
- neutrollization, 5
- political trolling, 225
- Soros trolls, 50, 210–11
- as subculture, 239–42
- targeted, 242
- troll farms, 2, 19, 162, 164, 177, 183
- use of word in news comments, 20–21, 32–33, 267
- See also* masking (online identity); Russian trolling
- Trump, Donald, 70, 74, 119–20, 129, 134, 142, 212, 225–26, 246
- truth, 95–96, 140–43, 161, 231, 242, 246
- alternative facts, 134, 142, 186, 231–32
- confirmed truthfulness, 133
- mash-up of, 181–82
- pledge of, 134–35
- verification of, 5–6, 134, 262–63
- See also* deception; post-truth
- Twitter
- denialism on, 243, 246
- IRA-controlled accounts, 24–25, 183
- masking (online identity) on, 41–42, 45–46, 61–62
- mistrust in institutions, role in, 131, 137–38, 160, 163, 167
- political polarization on, 84–85, 93–94, 125
- victim-playing, role in, 174, 184
- 2000 Doctrine, 179–82, 183
- Ukraine, 125, 167
- conflict with Russia, 36, 63, 134, 169, 173, 188, 191–95
- uncertainty, 34, 136, 247, 251, 259
- See also* doubt
- United Kingdom (UK), 98, 107, 135, 167
- United Nations Educational, Scientific and Cultural Organization (UNESCO), 167
- United States, 125
- Bill of Rights, 253
- Center for Strategic and International Studies, 175–76
- Central Intelligence Agency (CIA), 2
- cyberattacks in, 176
- Cyber Command, 176
- Department of Justice (DOJ), 31
- Federal Bureau of Investigation (FBI), 2, 116–17, 127–28, 154–57, 212–13, 264

- interference in other countries, 105–9, 125
- National Public Radio (NPR), 165
- National Security Agency (NSA), 2, 176
- Pentagon, 132
- State Department server, hacking of, 176
- United States, First Amendment (US Constitution). *See* freedom of speech
- United States, Russian trolling in 2016 presidential election
 - denialism in, 243–44, 246–47
 - disinformation in, 2–3, 19–21, 24–26
 - mistrust in institutions, role in, 129, 131, 154–55, 159, 162, 164
 - political polarization in, 86, 88, 122–23
 - victim-playing in, 173, 183
- unspoken knowledge, 6
- unverifiability, of information, 94, 96, 114, 233, 259
- “user-as-consumer” business model, 160
- Vaidhyanathan, Siva, 8, 26
- values, 90, 91, 97, 128, 169, 219, 261
- vatniks, 151–52
- Vedomosti* (Russian newspaper), 191, 194
- victim-playing, by Russia, 36–37, 171–219, 222
 - new media and information warfare in authoritarian regimes, 173–77
 - See also* delegitimization rhetoric; information warfare, by Russia; news comments, victim-playing Russian trolls in
- victim-playing frames, 20, 58–59, 251, 252
- violence, 138, 212, 242
- virality, 6, 89, 93, 123, 142, 231
 - See also* contagion, of content
- visibility, 27, 44, 55, 66–70, 78, 89, 224, 230–31, 263
 - See also* invisibility
- vulnerabilities, 3, 35–36, 228, 244–45, 254, 264
 - mistrust in institutions, role in, 129–30, 133, 141, 146, 153–54, 160–61
 - of social media, 17–23
- web, as a zero institution, 265–66
- Web 2.0, 10, 19, 143, 144, 259–60
 - See also* social media
- web brigades, 162, 192
- Wenzel, Andrea, 144
- whataboutism, 182, 256, 259
 - cracks in society, 105–13
 - denialism, role in, 221–23, 225–27, 229
 - mistrust in institutions, role in, 136, 155–57
 - political polarization, role in, 82–83, 100–102, 104–5, 119–20
 - See also* deflection
- WhatsApp, 28, 130, 246
- Wikipedia, 61, 169
- Wired* (magazine), 239–40
- Woolley, Samuel, 28, 30, 94, 123–24, 246
- World War II, 9, 46, 59, 88, 96–98, 122, 256
- Yahoo, 137–38, 176
- Yanukovych, Viktor Fedorovych, 192
- Yelp, 184
- Yeltsin, Boris, 181
- “you” phenomenon, 130, 131, 136–37, 159–60, 161
- youscan.io (fact-checking service), 167
- YouTube, 101, 116, 125, 181, 232
- Zabarskaitė, Jolanta, 261
- Zelenkauskaite, Asta, 32, 45–46
- Zelizer, Barbie, 133
- zero institution, web as a, 265–66
- zero-sum game, 209–12, 226
- Žižek, Slavoj, 252