CHAPTER 4

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 legitimation 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 particularly, 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 & Blacksburn, 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 to 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 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 #RussianTroll (/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 position as victims by claiming that whose 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-semite. 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 surprise 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

[redacted]

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

[redacted]

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:

[redacted]
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:

[redacted]
Toronto Aug. 24
[redacted] **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 Russi an 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

[redacted] **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

[redacted] **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 borrish 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

[redacted] 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

[redacted] 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

[redacted] 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

[redacted] 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

[redacted] 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

[redacted] 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 grassroot 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

[redacted] **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 Douthat 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

[redacted]
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.