Research Report

TODD C. HELMUS AND MARTA KEPE

A Compendium of Recommendations for Countering Russian and Other State-Sponsored Propaganda

Russia targeted the 2016 U.S. presidential election with a wide-scale social media–based propaganda campaign. Since that time, there is little indication that the Russian state has let up on this practice on social platforms; researchers have documented separate campaigns in 2018, 2019, and 2020 (Cheney and Gold, 2018; François, Nimmo, and Eib, 2019; National Intelligence Council, 2021). Other countries have also followed suit: Both Iran and China sponsored their own online disinformation campaigns targeting the United States (Gleicher, 2020a and Gleicher, 2020b). Countering such campaigns, which cost little to execute and can be precisely targeted, represents an extraordinarily important but complex task.

Since the Russian propaganda campaign that targeted the 2016 U.S. presidential election, policy researchers have penned a large trove of reports that offer recommendations for countering Russian influence efforts. These reports range from single-issue bulletins to comprehensive, book-length reports. With so many reports and so many discrete recommendations, it is virtually impossible for the average reader to gather and read the full slate of reporting and likewise difficult to keep track of the full breadth of policy considerations and discrete recommendations.

KEY FINDINGS

- Most reviewed studies recommend changes in government policies.
- A comparatively smaller number of studies urged policies that support broadcast and related content media.
- Falling in between are recommendations addressing social media platforms, coordination and synchronization mechanisms, and educational and awareness issues.
- The most common recommendations urge expansion of media literacy initiatives and suggest that platforms improve policies designed to detect and remove foreign propaganda content and improve advertising practices.

In this report, we seek to address this issue and perform at least some of this work. Specifically, we reviewed a large sampling of policy reports offering recommendations for countering Russian propaganda, then used Dedoose (a qualitative coding software program) to bin each of the offered recommendations into discrete categories. The narrative text for each category summarizes the key points and major themes of its included policy recommendations and attempts to highlight other relevant points.

For example, at least 30 reports recommend specific actions that the U.S. and allied governments can undertake to help limit the risk and impact of Russian propaganda. We identified nine separate subcategories of recommendations that address needed changes (for example, in the U.S. deterrence posture, intelligence collection and analysis, and information operations and public diplomacy). Note that Yadav (2020) takes a similar approach: The author also reviewed and tabulated policy recommendations for countering influence operations. Yadav offers the additional benefit of a downloadable coded database of reports; our report offers a more in-depth narrative description of report recommendations.

Our goal is for this report to serve as a reader's first stop for understanding the full slate of solutions available to policymakers. Therefore, we detail the recommendations that benefit from researcher consensus, and we provide lists of references for future reading.

Approach and Methodology

To gain insight into the recommendations offered to address Russian disinformation, we conducted a modified systematic review of policy papers related to disinformation. *Systematic reviews* are review papers that use systematic methods to collect individual published studies from available databases and analyze and synthesize the findings of those papers. Our focus for this review was disinformation-related public policy papers that offered policy recommendations.[1] Because of this, we conducted a search of the Policyfile database that yielded 156 think tank and policy reports published between January 2, 2016, and December 11, 2020.[2] To ensure that we had a substantive list of relevant reports, we added other material to this list of reports using a less systematic approach. We reviewed a list of policy recommendation reports posted on the EUvsDisinfo website (European External Action Service's East StratCom Task Force, undated). We also added several well-known policy reports that were not found on this list (including two substantive reports by the Alliance for Securing Democracy [Berzina et al., 2019; and Fly, Rosenberger, and Salvo, 2018]), and we reviewed a list of additional reports provided by one of this report's reviewers. After reviewing the contents of each report, we settled on 64 studies that met the criteria for entry: a clearly demarcated recommendations section and a focus on recommendations intended to address disinformation or propaganda. We provide a list of the qualifying studies at the end of this report.

Figures 1–3 offer a basic description of this data set. First, the majority of studies were published in either 2018 or 2019 (Figure 1). Most of the authoring institutions hail from the United States, although 17 percent come from Europe (Figure 2). Finally, a majority focus specifically on propaganda and social media; a minority are devoted to international relations, election security, or a smattering of other topics grouped into an "other" category (Figure 3).[3]

Each of the final 64 studies were coded using the qualitative coding platform Dedoose. The major categories identified and coded for this report are

- social media platform policies

FIGURE 1
Year of Publication for Qualifying Studies

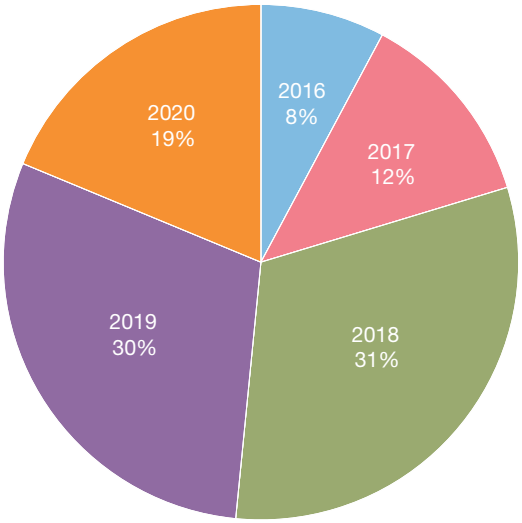


FIGURE 2

Institutional Origin for Qualifying Studies

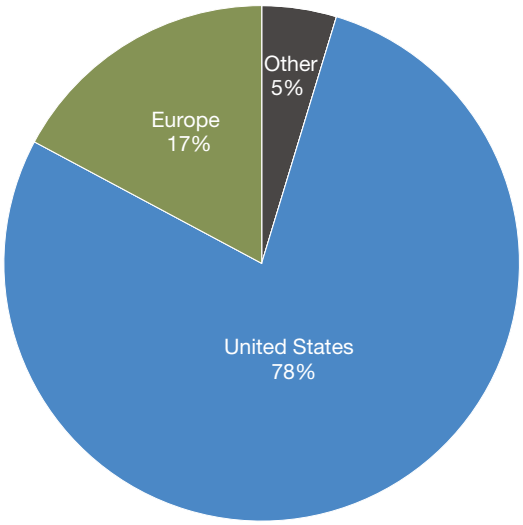
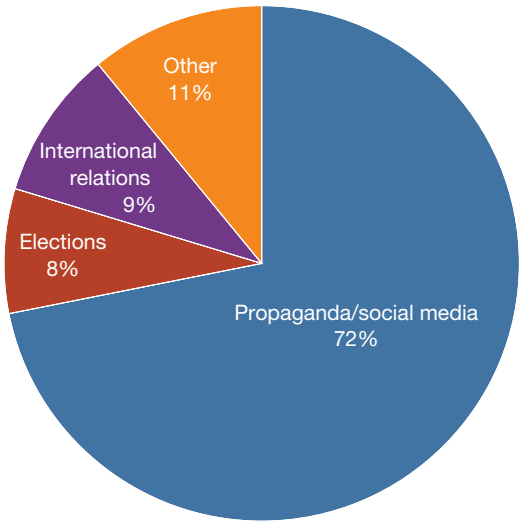


FIGURE 3

Major Focus Areas for Qualifying Studies



- U.S. and allied government policies
- coordination recommendations
- awareness and education recommendations
- recommendations for supporting various media and media content.

Within each major category, we coded for specific subcategories. We describe these subcategories in more detail throughout this report. (They are also summarized in Figures 4–9). The goal of this coding was to capture all disinformation-related recommendations. To avoid weeding through large sections of prose, we coded only those recommendations located in demarcated "Recommendations" sections or chapters.

Figure 4 identifies the number of reports that offered recommendations across five major categories, in no particular order: platform policies, government policies, coordination, awareness and education, and support for media.

Limitations

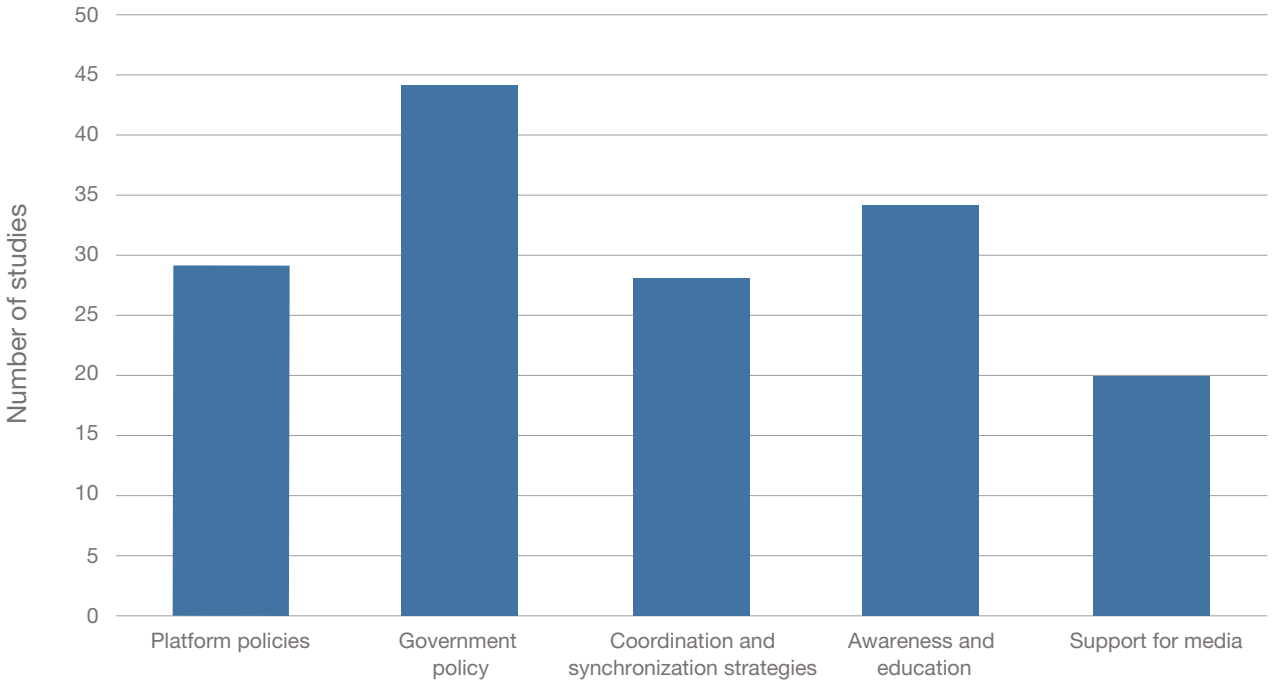
Several limitations apply to this study. First, our search query did not capture every policy report written on the Russian propaganda problem set. In addition, our requirement of a clearly specified recommendations section led to omission of several well-researched documents. Still, we hope that our final data set of 64 documents represents a reasonable sample of all relevant policy literature. Second, contrary to best practices for systematic reviews, we were unable to have two separate and trained reviewers code each report. This practice can increase accuracy of qualitative coding, but our study lacked such resources. Instead, one author made two separate passes at coding recommendations. In the first pass, codes were applied to the individual articles themselves. In the second pass, each code was reviewed for accuracy and fixes to those codes were applied as necessary. Finally, we note that the analysis for this report focused on categorizing and explaining recommendations. More analysis is necessary to fully understand the challenges and constraints involved in adopting these recommendations.

Organization of This Report

In the remainder of this report, we examine the major categories of codes applied to our data set. First, we review recommendations for changes to social media platform policies and recommendations for U.S. and other government policies. We then turn to recommended coordination changes, recommendations for improving awareness of disinformation, and recommendations for media-relevant policies. We conclude with a section in which we summarize key points and highlight some ongoing efforts to address these recommendations.

FIGURE 4

Number of Reports Coded for Each of the Major Categories of Recommendations



Recommendations for Platform Policies

Social media platforms (such as Facebook, Twitter and YouTube) and search engines (such as Google) play an obvious role in countering disinformation because much of the disinformation content resides on their feeds. Key recommendations for such platforms are listed in identifying and removing foreign propaganda content, revising their advertising policies, tuning algorithms, improving industry level coordination, revising membership policy, and other measures (Figure 5).

Content Identification and Removal

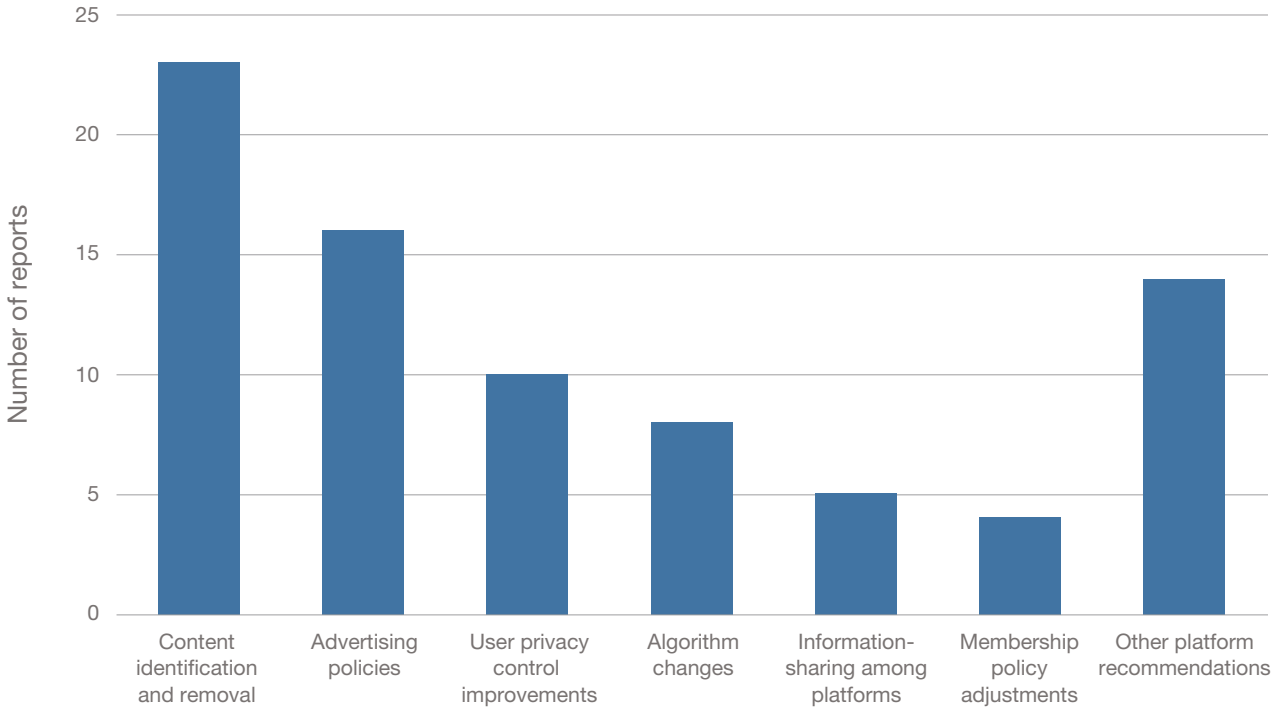
The recommendation made most often is that platforms should continue to do more to detect and, if necessary, remove malicious state-sponsored content. These studies urge platforms to "strengthen their investment" in detection technologies that have the ability to identify not only fake persona accounts used by Russian agents in the 2016 election but also fake pictures and videos, including deep-fakes (Stamos et al., 2019). These reports also argue for greater use of human moderators, the use of behavioral indicators, and the development of other advanced means that can inform technical detection.[4] It is noted that such efforts should focus on the use of automated bot accounts, another Russian tactic (Barrett, 2019). One study notes that preventing bots from "following," "liking," "sharing," and "retweeting" can serve as an added layer of protection (Stamos et al., 2019, p. 50).

Other studies offer suggestions for processes that should guide such detection efforts, such as greater transparency in how technology firms make decisions about content removal and adoption or creation of an executive-level position that would have companywide responsibility and authority over countering Russian propaganda.[5]

Many studies do not shy from urging greater regulations governing the removal of malicious content. There are suggestions that legislation create "strong incentives" for content removal (Cohen, 2018); create "industry standards" for content moderation (Berzina et al., 2019); delineate consequences for those who create, disseminate, or amplify misinformation (Brattberg and Maurer, 2018); and require the identification and labeling of bots driven by foreign actors and the provision of options for users to block them (Rosenbach and Mansted, 2018). It is also recom-

FIGURE 5

Number of Reports Coded for Platform Policy Recommendations



mended that platforms should draft annual reports for government agencies about identified and election-related disinformation (Kolga, Janda, and Vogel, 2019).

Advertising Policy Revisions

Russia spent more than $100,000 on approximately 3,000 Facebook advertisements targeted to reach specific U.S. audiences as part of the campaign to influence the 2016 election. It has been estimated that an ad buy of this magnitude could reach millions of viewers (Castillo, 2017). As a result, several studies urge that social media platforms and regulators adopt stricter rules governing advertising policy. Most frequently, these studies recommend adoption of policies featured in a 2017 Senate bill called the Honest Ads Act.[6] The act, introduced by Democratic U.S. Senator Mark Warner of Virginia, would subject internet advertisements to the same rules governing TV and radio ads by requiring the platform to identify who purchased an online political ad.[7] It has received support from Facebook and Twitter, although its ultimate passage remains uncertain. As Stanford University's Nathaniel Persily and Alex Stamos observe,

> The Honest Ads Act represents an important first step in bringing online advertising within the regulatory ambit of existing law. At a minimum, the U.S. Congress must pass and President Trump must then sign into law the Honest Ads Act to establish fair and reasonable guidelines for online advertising in political campaigns, including the regulation of foreign actors in this domain. (Persily and Stamos, 2019, p. 32)

Other authors recommend that the Honest Ads Act and related regulations go further. For example, two reports urge that foreign governments and individuals should be outright prohibited from purchasing online election related advertisements (Persily and Stamos, 2019; Vandewalker and Norden, 2018). To give the measure some teeth, Persily and Stamos argue for additional tweaks to the Honest Ads Act that would give the Federal Election Commission responsibility for determining specific election-related issues that require ad transparency and would require greater levels of disclosure for micro-targeted advertisements. Another report suggests that enforcement authority should be given to the Federal Trade Commission or Federal Communications

Commission rather than the Federal Election Commission because of their greater enforcement capacities (Barrett, 2019). Another report recommends that social media firms prepare so-called white lists of websites preapproved for advertising (Barrett, Wadhwa, and Baumann-Pauly, 2018).

User Privacy Control Improvements

Targeted advertising is advertising that directs advertisements to audiences with particular traits, interests, and preferences. Social media platforms collect enormous amounts of information on their users and have become a powerful venue for targeted advertising. Russia used this feature to reach and influence Americans who were most likely to react positively to its content (Helmus et al., 2020; Ribeiro et al., 2019). Several studies urge creation of policies that give users more control over their targetable personal data. For example, platforms should give users the option to modify the signals that algorithms use to customize a social media news feed (Ghosh and Scott, 2018) or at least ensure that users are aware of how data are collected (Berzina et al., 2019). Regulations should also ensure greater consumer privacy and protection (Polyakova and Fried, 2019; Lamond, 2018; Rosenbach and Mansted, 2018), such as notifying consumers when their data are being shared with data brokers (Polyakova and Boyer, 2018).

Algorithm Changes

Social media firms use complex and often secret algorithms to determine what content shows up on a user's computer screen. Modifications to these algorithms could offer users greater protection against malicious content. First, Russian and other state-sponsored content (such as that disseminated by the Russian broadcasting station RT or its online news engine, Sputnik) should be deprioritized in the results of Google searches or in the results of online news feeds (Polyakova and Fried, 2019; Kenney, Bergmann, and Lamond, 2019; Kolga, 2019; Kolga, Janda, and Vogel, 2019). Such a practice would apply to all media outlets registered under the Foreign Agent Registration Act (FARA). Furthermore, platforms should work to demote sensationalist and divisive content in their user feeds that generate the most user engagement.[8] Russian trolls and bots have leveraged such divisive content as a key component of their information campaigns (Barrett, 2019; Posard et al., 2020).

Membership Policy Adjustments

Anonymously created social media accounts have been the backbone of state-sponsored efforts to disseminate propaganda. To address this threat, several reports urge that platforms strengthen their membership policies. For example, Watts (2017) argues that platforms can adopt human verification systems, such as CAPTCHA, that would limit the use of automated accounts. Others suggest that platforms require users to confirm their identity at the time of account registration or give greater scrutiny to anonymous accounts (Kolga, Janda, and Vogel, 2019; Kenney, Bergmann, and Lamond, 2019). Polyakova and Fried go so far as to consider social media channels that provide "authentic spaces" that would be accessible only to verified human beings—not bots, cyborgs, or impersonators (Polyakova and Fried, 2019, p. 63). These authors do recognize, however, that the safety of some civil society or human-rights groups operating in authoritarian countries might depend on access to anonymous social media accounts (Polyakova and Fried, 2019, p. 63).

Information-Sharing Among Platforms

Given that state sponsors of propaganda use multiple social media platforms for their campaigns, it stands to reason that coordination among platforms will strengthen their ability to detect complex disinformation campaigns (Meleshevich and Schafer, 2018; Fly, Rosenberger, and Salvo, 2018). As Berzina and colleagues (2019) observe, "Social media companies should institutionalize information-sharing bodies across platforms to facilitate communication about potential threats and inauthentic activities, and to coordinate efforts to quickly respond to cross-platform information operations" (Berzina et al., 2019, p. 35). The Global Internet Forum to Counter Terrorism—a collaboration involving technology companies, civil society groups, and government organizations—is seen as one example that could be applied to disinfor-

mation (Lamond and Venook, 2020).[9] The success of such a collaboration mechanism might require a legal framework that would allow social media companies to share metadata of disinformation actors with one another in real time (Stamos et al., 2019).[10] Stamos, the former chief security officer at Facebook and a cybersecurity expert at Stanford, also recommends that such collaboration mechanisms facilitate the sharing of best practices. He notes that Google, Facebook, and Twitter all have a responsibility to share such lessons with each other, their smaller competitors, and even government agencies (Stamos et al., 2019).

Other Platform Recommendations

Policy researchers also offer several other recommendations. First, they argue, social media companies should provide disclaimers to content generated by FARA-registered foreign media organizations, such as RT and Sputnik (Kolga, 2019; Polyakova and Fried, 2019). Persily and Stamos, for example, recommend that this be a regulation, suggesting "a disclaimer at the bottom of RT broadcasts and internet videos that simply identifies the station either as an 'agent of the Russian government' or 'sponsored by the Russian government'" (Persily and Stamos, 2019, p. 40).

Other recommendations urge that tech-firms offer greater support for research and analysis conducted by academic and nonprofit institutions (Polyakova and Fried, 2019). In offering an argument for greater transparency of platform policies and practices, Bodine-Baron and colleagues note that one "key aspect of transparency" is enabling outside experts to verify and validate platform approaches to disinformation (Bodine-Baron et al., 2018, p. 57). Others argue that platforms should be more forthcoming in providing raw data to academics and to directly fund research on ways to enhance detection of illicit content (Barrett, Wadhwa, and Baumann-Pauly, 2018; Marcellino et al., 2020b).

Finally, other recommendations focus on creating a senior platform executive overseeing platform efforts to combat disinformation (Barrett, 2019; Barrett, Wadhwa, and Baumann-Pauly, 2018), making it easier for consumers to understand the creation of policies to govern the handling of stolen information, and introducing greater ethics education for computer scientists (Polyakova and Boyer, 2018).

> Anonymously created social media accounts have been the backbone of state-sponsored efforts to disseminate propaganda.

Recommendations for Government Policy

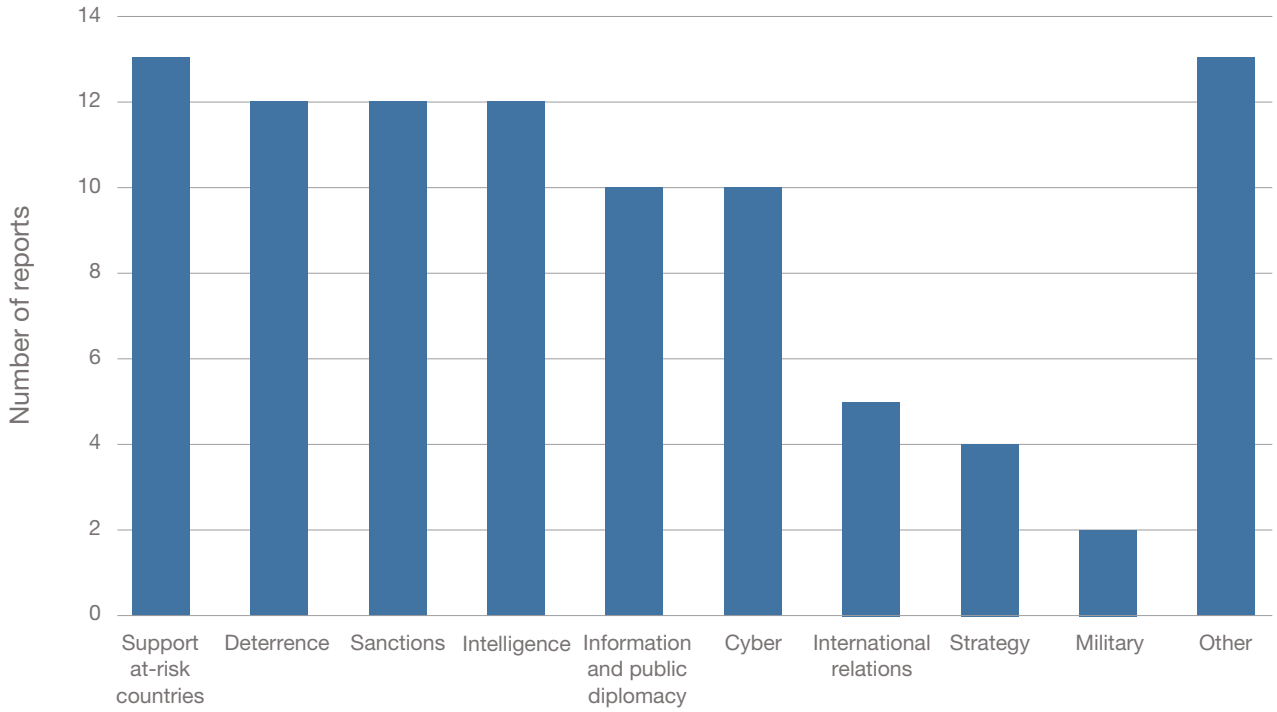
Figure 6 identifies the number of studies coded under different government policy actions. Ranking from most to least coded, policy reports urge that the U.S. and allied governments sanction past Russian state misbehavior regarding disinformation, deter future misbehaviors, increase and, if necessary, use defensive cyber capabilities, support at-risk countries, ramp up intelligence collection of Russian targets, and engage in public diplomacy and other messaging efforts.[11]

Support and Engagement with At-Risk Countries and Regions

One line of policy solutions is to offer support in consolidating states and regions that are at unique risk of Russian propaganda (Meister, 2016). Several studies, for example, highlighted the value of supporting democratic institutions and processes in at-risk countries (Fly, Rosenberger, and Salvo, 2018)—notably the Eastern European regions of the Balkans, the Baltics, Moldova, and Ukraine. Examples of support vary: supporting human rights, countering corruption, supporting rule of law, building democracy, supporting economic development, and strengthen-

FIGURE 6

Number of Reports Coded for Government Policy Recommendations



ing of minority rights (Bond, 2017; Helmus et al., 2018; Meister, 2016; Galeotti, 2017; Knake, 2020; U.S. Senate Foreign Relations Committee, 2018). The goal of such efforts would be to improve overall resilience of these countries and limit opportunities for Russia to sow division. In addition, both Eisentraut and de Leon (2018) and Helmus and colleagues (2018) highlight the value of direct aid in helping ensure that at-risk populations, such as Russian speaking minorities, in Eastern Europe support the West. A host of studies also urge support for foreign media and journalism (these are highlighted in the "Support Media" section of this report). Finally, other studies address the value of strategic messaging; for example, messaging that emphasizes the West's shared interests with at-risk regions could offer a compelling rationale for siding with the West (Helmus et al., 2018). It also could highlight the presence of other forms of Western aid (Eisentraut and de Leon, 2018). Such recommendations are in line with a suggestion articulated more broadly by Paul and Matthews (2016) to "increase the flow of persuasive information and start to compete, seeking to generate effects that support U.S. and NATO objectives."

Deterrence

Deterrence is the next highlighted category. Deterrence is the threat of force to dissuade an opponent from taking an unwelcome action (Rühle, 2015).[12] For deterrence posture to be successful, the United States and its allies would need to send a clear and consistent warning that Russian and other state-sponsored attempts to meddle in U.S. politics and covertly disinform the U.S. populace will be met with penalties.[13] Such a public and high-level warning issued by the German government and intelligence services might have played a role in Russia deciding not to leak information obtained during a 2016 hack of the German parliament (Polyakova and Boyer, 2018). The comparatively weak U.S. response is regarded as potential encouragement for Russia and other actors that might seek to use similar methods (Polyakova and Boyer, 2018). As a result of this weak response, Fried and O'Toole (2020) urge that deterrence responses be baked into congressional legislation.

Several reports highlight different strategies for deterrence responses. The response does not necessarily need to be in kind: Meddling in elections could

be met with sanctions or assistance to third-party countries that are countering the adversary in other domains (Jones, 2018). The United States also could enforce various mandatory response regimes that would impose sanctions if the Director of National Intelligence determines that a foreign power interfered in a U.S. federal election.[14] Finally, the deterrence strategy must be accompanied by clear messaging that defines the specific actions that will merit a formal response (Bergmann and Kenney, 2017).

Sanctions

Sanctions constitute another method for imposing costs on foreign regimes for interfering with U.S. elections. At least eight reports recommended that the United States impose sanctions against Russia for its efforts to interfere in the 2016 elections. As Lamond and Dessel observed, "Congress should immediately move forward with sanctions legislation against Russia for its interference in U.S. and European elections" (Lamond and Dessel, 2019, p. 25). Similarly, the Stanford Internet Observatory report on election interference urged "country-specific and timely responses that impose real, effective costs" (Lin, Painter, and Grotto, 2019, p. 66).

Sanctions directed against the Russian state for election interference have been limited. The Countering America's Adversaries Through Sanctions Act was signed into law in 2017, but its less-than-rigorous enforcement has been critiqued (Barrett, Wadhwa, and Baumann-Pauly, 2018; Fly, Rosenberger, and Salvo, 2018). In 2018, the Trump administration issued Executive Order 13848, which directs sanctions against persons found to have interfered in U.S. elections (Polyakova and Fried, 2019). Other developed sanction regimes await passage.[15]

Other reports offer suggestions for improving the effectiveness of sanctions. These reports recommend coordination of sanctions with allies (Berzina et al., 2019; Blanc and Weiss, 2019), the need to identify conditions that would have to be met to remove the sanctions (Blanc and Weiss, 2019; Lin, Painter, and Grotto, 2019; Meister, 2016), and the need to game out Russian responses to additional sanctions (Lin, Painter, and Grotto, 2019). One report urges that sanctions specifically target culpable individuals (Galeotti, 2017); others urge broader government targets. In addition, two reports urge that the United States reinstate and use the U.S. State Department's Office of Sanctions Coordination (Blanc and Weiss, 2019; Lamond, 2018).

Intelligence

Intelligence can help root out foreign disinformation campaigns in their earliest stages. Several reports urge efforts to strengthen the intelligence community's role in detecting and responding to disinformation threats. Not surprisingly, the most common recommendation was to increase intelligence and counterintelligence collection against Russia and China.[16] Janda (2016), for example, says, "National governments need to set clear priorities for their counterintelligence agencies—i.e., exposing Russian agents and cooperators." To achieve such ends, Jones (2018) suggests that it is necessary for the intelligence community to bolster its open-source intelligence collection capabilities, possibly making investments in artificial intelligence and pattern analysis so that they can detect online threats. A more basic need is the development of the requisite expertise to be able to identify and monitor adversary information operations.[17]

Beyond intelligence collection, it was also suggested that the intelligence community look for ways to support efforts related to public diplomacy related by declassifying intelligence that could be used to publicly counter Russian or other state-sponsored efforts (Bergmann and Kenney, 2017; U.S. Senate Foreign Relations Committee, 2018). A classic example of such an effort is the unclassified assessment produced by the intelligence community detailing the Russian influence campaign targeting the 2016 U.S. election (Office of the Director of National Intelligence, 2017). Other studies recommend that the intelligence community establish formal and informal relationships with social media platforms; doing so could enable more-effective sharing of threat information. (See the later section on public-private partnerships.)[18]

Information Dissemination and Public Diplomacy

Recommendations for public diplomacy initiatives to help counter disinformation varied widely. Policy

researchers, for example, urged that the United States engage in a more proactive and wider use of public diplomacy efforts (Bergmann and Kenney, 2017), publicize foreign propaganda and disinformation efforts more routinely (U.S. Senate Foreign Relations Committee, 2018), work to create a positive image of the United States and democratic values (Borshchevskaya, 2017), share experiences and lessons with other countries and international organizations (Bergmann and Kenney, 2017), and even increase cultural exchanges between U.S. citizens and people in Russia and neighboring countries that are vulnerable to Russian influence (U.S. Senate Foreign Relations Committee, 2018). In addition, Giles (2017) recommended that the United States denounce or name and shame adversaries who perform information operations.

The recommendation made most often, however, was to use all levels of political, intelligence, and law enforcement leaders to send a clear message that foreign interference is not tolerated (Barrett, Wadhwa, and Baumann-Pauly, 2018; Brattberg and Maurer, 2018; Lamond and Dessel, 2019; U.S. Senate Foreign Relations Committee, 2018). Such messaging can support deterrence policies. It has been observed that strong presidential leadership on countering and deterring foreign influence would help elevate these threats to the level of meriting a national U.S. strategy (U.S. Senate Foreign Relations Committee, 2018).

Cyber Policy and Capabilities

Several studies recommended improvements to U.S. defensive and offensive cyber capabilities. One report notes that "although cybersecurity has not featured prominently in the disinformation debate, it should be understood as an essential part of the solution" (Ghosh and Scott, 2018, p. 31). The report also notes, "Frequently, disinformation and cyberattacks are a paired phenomenon. Hackers breach email accounts or sensitive files and spill the contents into the media, often commingling truth and falsehood" (Ghosh and Scott, 2018, p. 31).

The reviewed sources emphasize the need for robust national policies to enhance the U.S. ability to detect cyberattacks (Kagan, Bugayova, and Cafarella, 2019), protect political party information and supporter data to increase the resilience of the electoral process and related cyberinfrastructure (Kolga, Janda, and Vogel, 2019; Bergmann and Kenney, 2017), and boost national defense and offense cyber capabilities (Berzina et al., 2019). Another suggestion is that the security protocols of the electoral process and infrastructure should be made more robust—for example, by introducing two-factor authentication for political party websites and databases (Kolga, Janda, and Vogel, 2019).

The studies also identify the need for offensive capabilities that offer an opportunity to respond to identified disinformation campaigns. These could include a wide variety of electronic warfare and cyberspace operations capabilities, such as ones that would help combat cyberhacking and intrusions, provide better cyberthreat assessment, and improve forecasting and cyberintrusion detection capabilities (Bergmann and Kenney, 2017; Kagan, Bugayova, and Cafarella, 2019).[19] Berzina and colleagues (2019) argued than European democracies should consider performing cyber operations against state actors in response to cyberattacks on critical infrastructure.

International Relations and Diplomacy

Only six studies offered recommendations for improvements in international relations and diplomacy. As with public diplomacy, these recommendations varied widely and offered no clear policy consensus: clear articulation of the U.S. position on foreign influence (Bodine-Baron et al., 2018), European Union and NATO support to local counter disinformation activities (Janda, 2016), and a demonstration of commitment to the Balkan region by U.S. and European countries (Stronski and Himes, 2019).

Strategy

Recommendations suggest that it is critical that policymakers develop a broad national strategy (Spaulding, Nair, and Nelson, 2019). As Janda (2016) observes, counterdisinformation initiatives should be tied together and implemented as part of a broader U.S. national strategy (Janda, 2016; Posard et al., 2020). Kagan, Bugayova, and Cafarella (2019) likewise report that a high-level strategic approach

should be driven, first and foremost, by the strategic vision of the country, not serve as a reactive policy to foreign influence. This strategic approach also should address global U.S. interests rather than consider them on a theater-by-theater basis.

Military

Two studies offered recommendations relevant to the military. NATO countries could ensure that the organization improves its capabilities and reduces its potential military vulnerabilities in case Russia does choose to "seize tactical opportunities" (Lamond, 2018). In addition, vigilance should be maintained about malign use of information against NATO members and their military forces (Janda, 2016).

Recommendations for Coordination and Synchronization Strategies

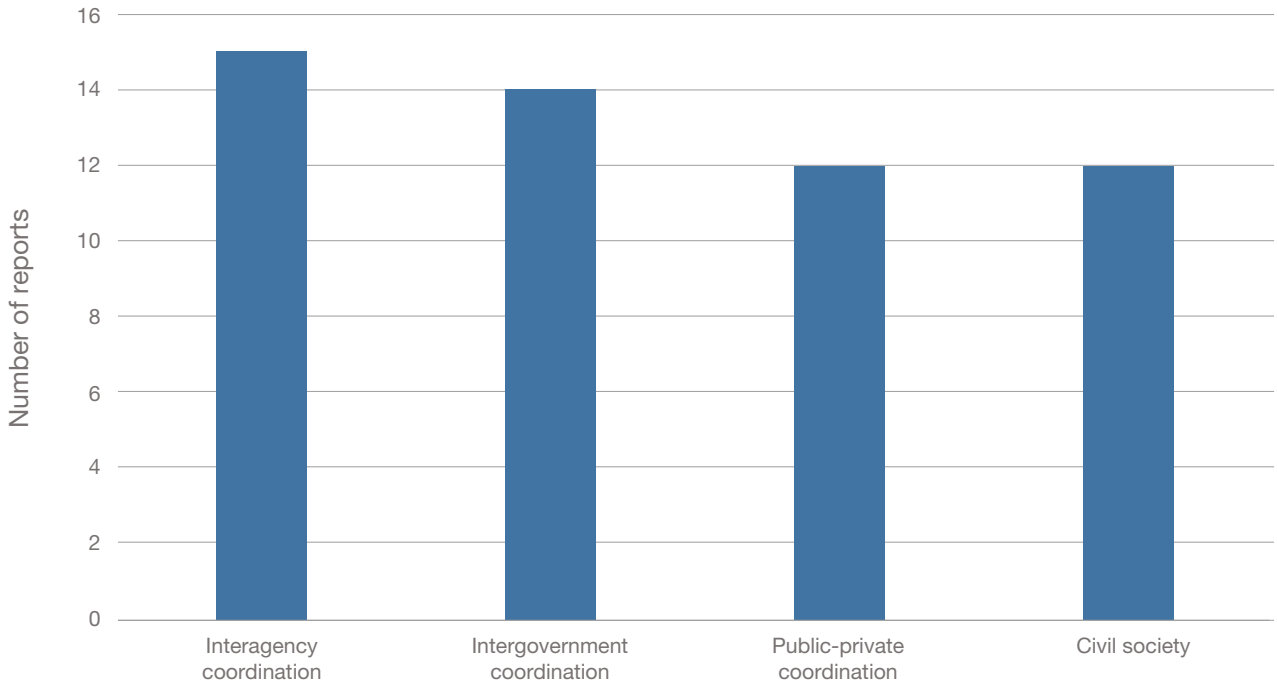
There are numerous actors engaged in countering disinformation, from individual governments and their respective departments and agencies to social media companies and civil society. Therefore, it is not surprising that coordination mechanisms play a prominent role in the variously reviewed policy papers. The tally of papers addressing coordination are featured in Figure 7.

Interagency Coordination

Agencies and departments of the U.S. and allied governments must ensure that their efforts are coordinated and synchronized. At least in the United States, effective and harmonious interagency coordination has been an unrealized goal that has afflicted execution of several key policy goals, such as strategic communications (Paul, 2009). A central feature of numerous policy prescriptions is a call for dedicated interagency leadership to guide the vast apparatus of government. Recommendations encompassed designation of lead agencies (Polyakova and Fried, 2019) or cabinet officials (Janda, 2016) or appointment of a senior-level coordinator (Berzina et al., 2019; Fly, Rosenberger, and Salvo, 2018). Other recommendations suggest that the United States create an "Interagency Fusion Cell" (U.S. Senate Foreign Relations Committee, 2018, p. 55) or a "Counter

FIGURE 7

Number of Reports Coded for Coordination Recommendations



Disinformation Center" that would function as a smaller version of the National Counter Terrorism Center (Polyakova and Fried, 2019, p. 6). Others recommend that the U.S. National Security Council and the Office of the Director of National Intelligence modify their existing structures to accommodate a specialized disinformation office (Barrett, Wadhwa, and Baumann-Pauly, 2018; Fly, Rosenberger, and Salvo, 2018).

Intergovernment Coordination

Russian and other adversary disinformation efforts have become a global problem. Russia, for instance, has targeted elections in the United States and France, the referendum in the United Kingdom to split from the European Union, and opinions of populations throughout the Russian near abroad. Consequently, many policy reports urge a coordinated international response to foreign propaganda. These recommendations coalesce around three critical lines of effort.

First, governments must coordinate to share information on best practices and ongoing threats.[20] For example, Polyakova and Fried (2019) recommend the creation of a transatlantic Counter-Disinformation Coalition that would bring together relevant governments and social media companies to share experiences and information on disinformation efforts and to develop nonbinding best practices.

Second, governments should work together to detect and disrupt foreign influence operations.[21] These studies offer several alternatives, such as strengthening Interpol for counterdisinformation investigations (Jones, 2018), using collective engagement and possibly treaties to promote deterrence (Kolga, Janda, and Vogel, 2019; McFaul, 2019; Polyakova and Fried, 2019), and coordinating information security and detection and counterdisinformation activities (Kenney, Bergmann, and Lamond, 2019; Kolga, 2019). The U.S. Senate Committee on Foreign Relations argued for a coalition to "build awareness of and resilience to" Kremlin disinformation efforts and recommended that the Organization for Security and Co-operation in Europe serve as a forum for exposing disinformation attacks (U.S. Senate Foreign Relations Committee, 2018, p. 159).

Finally, at least four studies recommended that international institutions—such as the NATO Strategic Communications Centre of Excellence in Riga or the European Centre of Excellence for Countering Hybrid Threats—serve as resource hubs for disinformation efforts.[22]

Public-Private Coordination

Governments must coordinate with the private sector, particularly social media firms engaged in detecting and countering disinformation. Bodine-Baron and colleagues (2018) recommend creation of a formal mechanism that would facilitate the sharing of threat information among platforms and intelligence agencies. Other reports offer similar prescriptions.[23]

Civil Society

Finally, civil society is a needed focal point for coordination. Several studies call for establishing formal government relationships with civil society.[24] Other reports highlight the value of enhancing links between civil society groups. For example, Jones (2018) argues that that it is important to foster international links between civil society groups to enable sharing of best practices, and Eisentraut and de Leon (2018) note that government can assist in such efforts by creating an online registry of local initiatives to provide a platform for sharing best practices.

Finally, the government should play a direct role in funding counterdisinformation civil society work.[25] One report arguing the critical need for such support states:

> Disinfo-countering NGO [nongovernmental organization] initiatives need to be financially supported. Trustworthy and operational NGO projects are urgently needed. . . . [T]hose organizations are heavily underfinanced and therefore it is more or less volunteer activities which cannot yield systematic professional results. . . . Those projects need to work in national environments with a deep understanding of the national discourse and a high degree of credibility among journalists and security-related institutions. Ukrainian StopFake.org is a good example of an engaged NGO. Each EU

member state needs to have at least one non-governmental institution which would conduct activities in this area on a daily basis with national relevance. (Janda, 2016, p. 18)

Recommendations for Improving Awareness of Russian Disinformation

Improving awareness of Russian disinformation efforts calls for fact-checking initiatives that help correct instances of misinformation or false news, media literacy programs that educate consumers to think more critically about media and information, and warning regimens that increase awareness of specific foreign propaganda campaigns. Figure 8 summarizes the number of reports coded for these categories.

Media Literacy

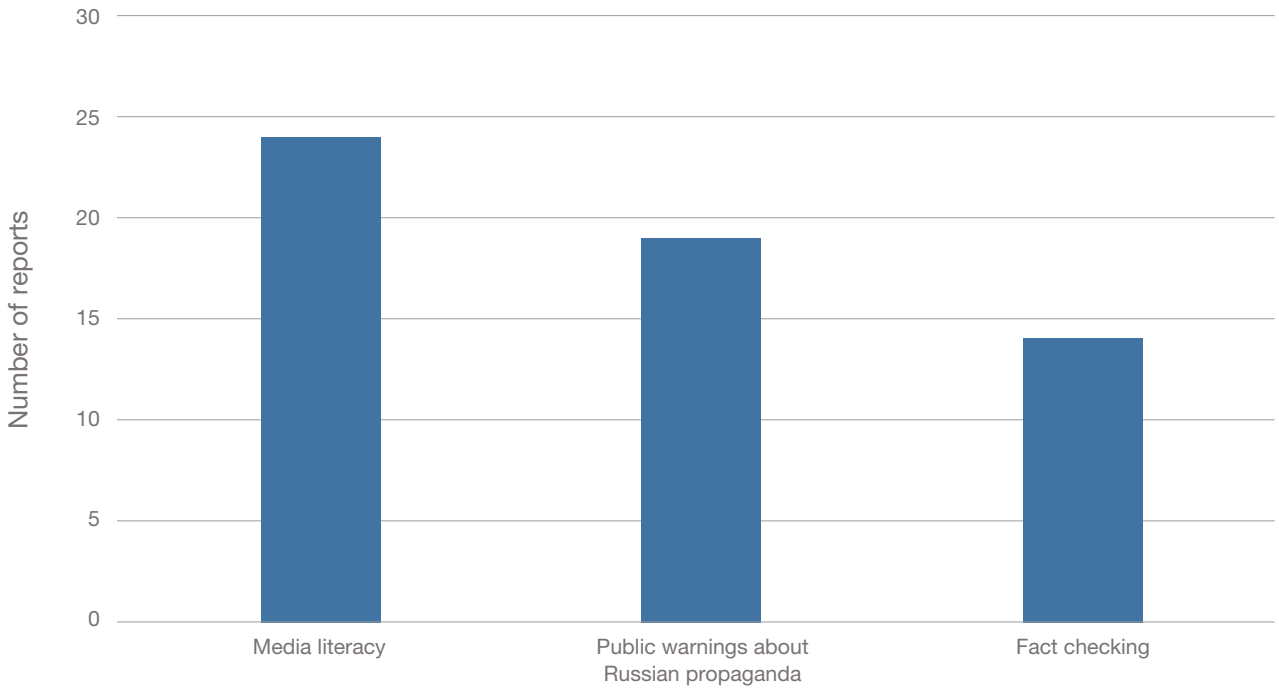
Even the best efforts of social media platforms to detect and remove malicious content will fail to keep up with the vast flow of online disinformation. The individual consumer who scrolls through his or her social media feed consequently serves as the last line of defense against foreign propaganda. Media literacy programs seek, in part, to help audiences be curious about sources of information, assess their credibility, and think critically about the material presented (Stamos et al., 2019).

At least 24 studies argue that access to media literacy training must be strengthened and expanded. These reports urged greater investment in developing new and effective media literacy curricula (Brattberg and Maurer, 2018; Cohen, 2018; Polyakova and Fried, 2019; Kamarck, 2018; U.S. Senate Foreign Relations Committee, 2018). They also urge that such a curriculum be integrated into and beyond primary and secondary educational settings.[26] One such report observes that "developing digital media literacy through broader education campaigns is thus essential in order to train British citizens to cope in the modern information environment . . ." (Dobrowolski, Gioe, and Wanless, 2020, p. 36)

Evidence suggests that media literacy interventions work. A diverse array of media literacy interventions have demonstrated a moderate and positive impact in improving participants' beliefs, attitudes, and behaviors related to media (Jeong, Cho, and

FIGURE 8

Number of Reports Coded for Awareness Improvement Recommendations



Hwang, 2012; Guess et al., 2020). Recent RAND Corporation research also suggests that online media literacy content can reduce audience engagement with Russia propaganda memes (Helmus et al., 2020).

Public Warnings About Russian Propaganda

Several policy papers conclude that the public should be warned about Russian propaganda campaigns and thus recommend that governments and social media firms issue formal notifications or warnings of specific foreign disinformation campaigns (Fly, Rosenberger, and Salvo, 2018; Lamond and Dessel, 2019). Polyakova and Fried (2019) and Jones (2018) recommend use of a formal rapid alert system; Helmus and colleagues (2018) point to the weekly alerts issued by the European StratCom Task Force. Relatedly, authors highlight the importance of public attribution of identified disinformation campaigns (Berzina et al., 2019; Brooking and Kianpour, 2020; Kagan, Bugayova, and Cafarella, 2019).

Several studies highlight the success that such alerts have had in the past. Increasing awareness in Europe has "enabled society, media, and governments to put appropriate defenses in place" (Giles, 2017). The French and German governments used intelligence about Russian information campaigns to warn their citizens (Rosenbach and Mansted, 2018), Nordic and Baltic countries routinely highlight the presence of Russian propaganda (Bergmann and Kenney, 2017) and the European StratCom Task Force has helped raise awareness of Russian propaganda in Europe's policy circles (Helmus et al., 2018). Most recently, research by RAND has shown that labeling Russian propaganda content as such can blunt audience engagement with the content. RAND research also showed that audiences react positively to government-issued public service announcement warnings of Russian propaganda (Posard, Reininger, and Helmus, 2021).

Fact-Checking

Russia routinely engages in the dissemination of false news headlines meant to advance its strategic interests. Fourteen studies highlighted the need to support and expand fact-checking efforts. Both Eisentraut and Leon (2018) and Bergmann and Kenney (2017) highlighted the value of a European initiative called the Strategic Communications Task Force, which routinely publicizes examples of Russian disinformation and offers corrective information. Other studies indicate that journalists and other members of civil society play a critical role in advancing fact-checking initiatives. These studies encourage the expansion of civil society–based fact-checking networks (Berzina et al., 2019; Polyakova and Fried, 2019; Lucas and Pomeranzev, 2016), support for journalists in such at-risk regions as the Balkans (Eisentraut and de Leon, 2018), and the emulation of such journalistic initiatives as FactCheck.org, PolitiFact.com, and the German Marshall Fund's Hamilton 68 dashboard (Brattberg and Maurer, 2018).

Social media companies have begun to incorporate fact-checking mechanisms into their social media feeds. These platforms label some questionable online news stories as disputed or false.[27] The obvious advantage of such fact-checks is that they can directly reach the audiences targeted by misinformation. Summative studies of the research literature have shown that online fact-checking efforts—such as real-time corrections, crowdsourced fact-checking, and algorithmic tagging—can successfully mitigate the effects of misinformation (Walter, Brooks, et al., 2020a).[28] Therefore, policy researchers urge that such efforts continue and be expanded.[29]

Recommendations for Supporting Media

Both old and new media alike play a critical role in shaping opinions. Journalists help audiences translate news and events for foreign and domestic audiences; online influencers shape opinions on social media, and access to high-quality broadcast media give Russian-speaking audiences alternatives to Russian state media. Figure 9 highlights some of the key topics addressed in this broad category of recommendations.

Support Domestic and Foreign Journalism

Journalists serve as gatekeepers of information for society at large; in line with this reality, policy pro-

posals highlight the need to support and protect this group. Several reports highlight the need to support journalism in the West. A common refrain from such proposals is that reinforcement of standards and training ensures that journalists do not become unwitting amplifiers of foreign propaganda and disinformation. Some studies highlight the need to reinforce "quality standards and practices" (Brattberg and Maurer, 2018, p. 31), enhance journalist training (Janda, 2016), support investigative journalism (Berzina et al., 2019), assess standards governing how journalists use stolen information (Stamos et al., 2019; Bergmann and Kenney, 2017; Berzina et al., 2019), and ensure that journalism trade associations police ethics violations among their membership (Janda, 2016).

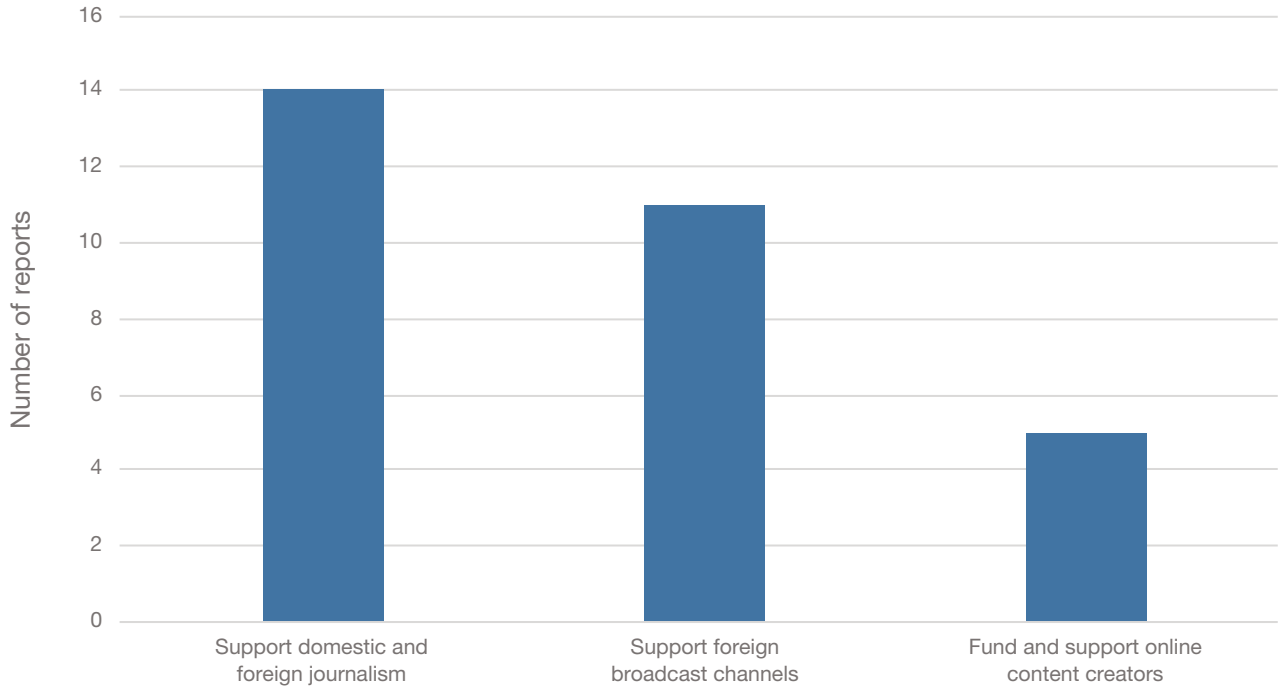
Other reports emphasize supporting journalists who serve at-risk populations. Here, the focus is on training and enhancing the capacity of journalists (Christie, 2019; Janda, 2017) or improving journalistic networks (Lucas and Pomeranzev, 2016) in such areas as Ukraine, the Western Balkans, and the Baltics (Eisentraut and de Leon, 2018; Helmus et al., 2018; Ukrainian Election Task Force, 2018). Other policy papers highlight the value of investigative journalism (Barbashin, 2018), which is seen as a critical tool to "counter propaganda with facts" (Meister, 2016, p. 14). In one example of such training, the United States sponsored a Tech Camp in Riga that brought together reporters and editors not only from European Union member states but also partner countries for training on digital literacy (U.S. Embassy in Latvia, 2015). The international community also supports regional NGOs, such as the Baltic Centre for Media Excellence.

Support Foreign Broadcast Channels

In some regions—such as the Baltic countries of Estonia, Latvia and Lithuania—Russia is able to effectively support its internet-based disinformation campaign with more-traditional television broadcasts of Russian news and other Russian-language programming. In such locations as this, studies recommend that governments do more to support pro-Western broadcast channels, notably by increasing financial support for direct Western government broadcasting efforts, such as the foreign-language versions of the United Kingdom's British Broadcasting Counsel,

FIGURE 9

Number of Reports Coded for Media Support Recommendations



the German government's Deutche Welle, or the U.S. government's Radio Free Europe or Current Time.[30]

Other studies also urge that the West offer greater financial support to locally run and aired programming.[31] One cited example is the Estonian Russian-language public broadcaster ETV+, which is in need of greater financial support (Lucas and Pomeranzev, 2016). As another author observes, "From Poland to Ukraine to Hungary to Moldova, local media are most attuned to local circumstances, social mores, and political cultures. They are uniquely suited to produce and present content that addresses the complexity of liberal democratic development in ways that resonate with their audience" (Barbashin, 2018).

Fund and Support Online Content Creators

Beyond support of formal media channels, recommendations also address supporting local and informal messengers. A previous RAND report on Russian influence in Eastern Europe recommended that Western government support Russian-language influencers and other social media producers in the region who are best positioned to influence the region's Russian-speaking audience (Helmus et al., 2018). Other studies refer to enhancing the capacities of and empowering "positive third-party messengers, whether they are governments, NGOs, or other entities," (Kolga, 2019) and extending beyond "traditional outlets and formats" to "blogs, vlogs, infotainment, [and] memes," which are "crucial means for reaching younger generations" (Barbashin, 2018, p. 5). One study, for example, notes that "Civil society should engage with social media influencers across various themes to counter information operations and raise awareness" (Berzina et al., 2019, p. 390).

Conclusions and Current Status

In this report, we have summarized the major recommendations offered by academics and policy researchers for countering Russian-authored propaganda campaigns targeting the United States and its allies. The recommendations span platform and government policies, coordination mechanisms, educational efforts, and media support initiatives. The expanse of such recommendations highlights the critical challenges that confront policymakers and private institutions as they seek to counter Russian and other state-sponsored propaganda campaigns.

To what extent have such recommendations been enacted? Answering this question is beyond the scope of this effort, although we can offer a brief snapshot at recent policy changes.

First, social media platforms have continued to update their policies and practices. Twitter, for example, recently banned all political advertisements, required the clear labeling of all bots, removed millions of bots from its network, uncovered and removed several state-sponsored disinformation campaigns, and introduced a process for fact-checking. Facebook now offers a "Paid for by" disclosure for political advertisements. It also developed a searchable archive of political ads and verifies the U.S. residency of political advertisers (Nunziato, 2020). Overall, the changes are laudable though they have been labeled as "ad hoc" (Nunziato, 2020, p. 36) and described as "falling short of what's needed" (Weinberger, 2020). A policy debate continues over the need for regulatory fixes that would create a common and enforceable standard across platforms.

The platforms have used human and automated methods to remove foreign propaganda content from their servers. In 2019, for instance, Facebook, removed more than 50 global propaganda networks (Gleicher, 2020a). Ultimately, such efforts must continue to improve if the platforms hope to rapidly uncover foreign disinformation and stay ahead of evolutions in foreign disinformation tactics.

For government policies, the most-common recommendations dealt with punishing Russia for its 2016 (and ongoing) propaganda campaign and deterring Russia from engaging in such actions in the future. A related recommendation called for issuing clear and unambiguous warnings to Russia for identified propaganda campaigns. To date, the U.S. government has not offered unified and consistent policies on these ends (Polyakova and Boyer, 2018). This should be a focus of the incoming Biden presidential administration.

Awareness-building programs are on the rise. One of the most common recommendations called for greater development and access to media literacy campaigns. Domestically, at least 14 states have instituted laws requiring the integration of media literacy across school curricula at all grade levels (Media Literacy Now, 2020), and the United States has funded and organized several overseas media literacy–training efforts.[32] Such efforts are an important step, although the challenge of improving media literacy skills at the population level cannot be understated (Bodine-Baron et al., 2018). Highly scalable media literacy content disseminated over online channels could help overcome this challenge.

In addition, several fact-checking efforts have been launched, especially on social media platforms. Twitter has implemented a fact-checking policy that labels misleading posts. The fact-checking process also applies to political posts, except for those directly authored by an elected official. Facebook has also tweaked its algorithms to deprioritize false posts in users' news feeds. Those attempting to share debunked posts are alerted to this fact with a warning notice (Nunziato, 2020). The platforms obviously face a significant challenge in ensuring that fact-checking efforts occur quickly and in uniform fashion. In addition, some fact-checking efforts have come under increasing attack from political partisans who feel targeted by such measures (Isaac and Browning, 2020).

Finally, the United States has sought to support foreign media environments. The United States launched the Russian-language television program, *Current Time*, which broadcasts television programming to audiences in the Baltics, Ukraine, the Caucasus, and Central Asia. Some have suggested increasing the U.S. budget for this program; proposals to dramatically cut funding to the show's parent organization, U.S. Agency for Global Media, risk undercutting U.S. efforts in the region ("Trump Administration's 2020 Budget . . . ," 2019). One challenge is the sheer cost of implementing broadcast programs, especially in such regions as Eastern Europe, where audiences are fragmented by language and culture.

> In this report, we have summarized the major recommendations offered by academics and policy researchers for countering Russian-authored propaganda campaigns targeting the United States and its allies.

The U.S. Global Engagement Center (GEC) has also launched media support efforts for accurate reporting in North Macedonia, independent media in vulnerable European countries, and civil society efforts to build resistance to disinformation. The GEC has funded an implementer to train civil society actors in 14 European nations on ways that their organizations can help their communities rapidly identify and respond to disinformation in locally relevant ways (Gabrielle, 2019).

Notes

[1] The search query read: Title, Keyword and Abstract content: (russia*) AND title-abs-key((disinformation OR propaganda OR "social media" OR "truth decay" OR "influence campaign*" OR troll* OR bot OR bots OR "information operation*" OR "coordinated inauthentic" or interference or manipulation). This yielded a total of 136 papers.

[2] Pro-Quest Library Guide defines PolicyFile in the following way:

> Policy File Index is a unique resource for U.S. public policy research. Users are able to access timely, updated information from over 350 public policy think tanks, nongovernmental organizations, research institutes, university centers, advocacy groups, and other entities. Over 75 public policy topics are covered, from foreign policy to domestic policy. (ProQuest, undated)

[3] It should be noted that election security reports constitute a relatively small share of our list. This is because we did not code for election security policies in our analysis (given that the main focus is propaganda). As a result, several well-researched studies on election security were not included in our data set.

[4] For example, see Barrett, Wadhwa, and Baumann-Pauly, 2018; Berzina et al., 2019; Brattberg and Maurer, 2018; Christie, 2019; Fly, Rosenberger, and Salvo, 2018; Kolga, 2019; Marcellino et al., 2020a; Persily and Stamos, 2019; and Watts, 2017.

[5] For example, see Stamos et al., 2019; Barrett, 2019; Barrett, Wadhwa, and Baumann-Pauly, 2018; Bodine-Baron et al., 2018; and Polyakova and Fried, 2019.

[6] Overall, several studies support either the entire Honest Ads Act or specific components of it. See Barrett, Wadhwa, and Baumann-Pauly, 2018; Christie, 2019; Cohen, 2018; Polyakova and Fried, 2019; Ghosh and Scott, 2018; Lamond, 2018; Persily and Stamos, 2019; Polyakova and Boyer, 2018; Rosenbach and Mansted, 2018; Rudolph and Morley, 2020; Vandewalker and Norden, 2018; and Watts, 2017.

[7] The bill would also require each moderately sized digital platform to maintain a public file of all election-related communications purchased by any entity paying that platform more than $500.00 for published ads. The bill also would also require platforms to "make all reasonable efforts" to ensure that foreign individuals and entities are not purchasing political advertisements to influence the U.S. electorate (Warner, 2019).

[8] For example, see Barrett, 2019; Christie, 2019; Dobrowolski, Gioe, and Wanless, 2020; Polyakova and Fried, 2019; and Rosenbach and Mansted, 2018. For an excellent piece on the challenges to implementing such algorithmic changes, see Hao, 2021.

[9] Collaboration is also commonly used to address child pornography and freedom of press and privacy.

[10] Another potential forcing function for improved coordination would be the regulatory requirement that social media platforms adopt standard terms of service. Creating such terms of service would demand that social media companies "agree on both common definitions of impersonator and inauthentic accounts and standards on removing bots, and, though this is more questionable, what qualifies as hate speech, credible versus weak content, and violent or harm-ful content (e.g., anti-vaccination propaganda)" (Polyakova and Fried, 2019, p. 19).

[11] Several recommendations from various other sources fell within an "other" category, such as suggestions for congressional hearings and a smattering of items addressing various issues, such as the need for a top-to-bottom assessment of U.S. capabilities, changes to money laundering laws, strengthening of anti-money laundering laws, and more funding at the State Department.

[12] The way that deterrence signaling is done should be carefully tailored to the adversary: Sometimes a private mode of signaling might be necessary because of the adversary's domestic political issues (McFaul, 2019). Some authors suggest that the deterrent messaging should contain explicit red lines—detailed specifications about the costs that would be imposed in case of their interference (Bergmann and Kenney, 2017; McFaul, 2019). Such red lines could also define what the United States considers to be a cyberattack, thus decreasing ambiguity. If such red lines are conveyed, it becomes of utmost importance to follow through and impose them or risk losing credibility.

[13] For example, see Galeotti, 2017; Jones, 2018; Lin, Painter, and Grotto, 2019; Marcellino et al., 2020b; Rosenbach and Mansted, 2018; Brattberg and Maurer, 2018; Fly, Rosenberger, and Salvo, 2018; and Polyakova and Fried, 2019.

[14] For example, see Lin, Painter, and Grotto, 2019; McFaul, 2019; U.S. Senate Foreign Relations Committee, 2018.

[15] One item on hold is the bipartisan DETER (Defending Elections From Threats by Establishing Redlines) Act, which would authorize a fresh round of sanctions on Russia if the Kremlin meddles again in U.S. elections (Barrett, Wadhwa, and Baumann-Pauly, 2018). Another is the Defending American Security from Kremlin Aggression Act of 2018 which would, in part, increase economic, political, and diplomatic pressure on Russia in response to its continued interference in U.S. elections (Lamond, 2018).

[16] For example, see Jones, 2018; Rosenbach and Mansted, 2018; Bergmann and Kenney, 2017; Berzina et al., 2019; Galeotti, 2017; Janda, 2016; Kamarck, 2018; and Lamond, 2018.

[17] For example, see Berzina et al., 2019; and Marcellino et al., 2020c.

[18] Other intelligence-related recommendations are to urge European Union member states to deny "agents of authoritarian interference access to the EU" (Berzina et al., 2019), and to promote more-consistent funding for intelligence and counter intelligence (Galeotti, 2017).

[19] Some authors also call for formal guidelines within the North Atlantic Treaty Organization (NATO) on the definition of government-sponsored cyberattacks in the context of NATO's Article 5 (U.S. Senate Foreign Relations Committee, 2018). However, changing cyber norms would most likely be a challenging process. Because of the unique characteristics of the cyber domain, caution should be taken to avoid trying to emulate nuclear norms.

[20] For example, see Berzina et al., 2019; Fly, Rosenberger, and Salvo, 2018; Polyakova and Fried, 2019; Jones, 2018; and Polyakova and Boyer, 2018.

[21] For example, see Kolga, Janda, and Vogel, 2019; McFaul, 2019; Polyakova and Fried, 2019; Jones, 2018; Kagan, Bugayova, and Cafarella, 2019; Kolga, 2019; Gonzalez and Dale, 2020; and Fly, Rosenberger, and Salvo, 2018.

[22] For example, see Berzina et al., 2019; Polyakova and Fried, 2019; Helmus et al., 2018; and Polyakova and Boyer, 2018.

[23] For example, see Barrett, Wadhwa, and Baumann-Pauly, 2018; McFaul, 2019; Polyakova and Boyer, 2018; and Kolga, 2019.

[24] For example, see Brattberg and Maurer, 2018; Janda, 2017; Kolga, 2019; and Marcellino et al., 2020b.

[25] For example, see Polyakova and Fried, 2019; Hosa and Wilson, 2019; Janda, 2016; Kolga, 2019; Kolga, Janda, and Vogel, 2019; Fly, Rosenberger, and Salvo, 2018; and Marcellino et al., 2020a.

[26] For example, see Barbashin, 2018; Eisentraut and de Leon, 2018; Helmus et al., 2018; Janda, 2016; Kolga, 2019; Kolga, Janda, and Vogel, 2019; and Lucas and Pomeranzev, 2016.

[27] "How Does the Twitter Fact-Check Policy Work . . . ," 2020; Facebook, undated; Ritter, 2020; Rodriguez, 2020.

[28] See also Walter and Murphy, 2018; and Walter, Cohen, et al., 2020b.

[29] For example, see Barrett, 2019; Barrett, Wadhwa, and Baumann-Pauly, 2018; Bergmann and Kenney, 2017; Giles, 2017; Helmus et al., 2018; and Watts, 2017.

[30] For example, see Barbashin, 2018; Helmus et al., 2018; Meister, 2016; and Bergmann and Kenney, 2017.

[31] For example, see Eisentraut and de Leon, 2018; Barbashin, 2018; Borshchevskaya, 2017; Helmus et al., 2018; Hosa and Wilson, 2019; and Kolga, 2019.

[32] The nonprofit organization IREX has launched its "Learn to Discern" media literacy training program in Ukraine and elsewhere (Irex, undated). Several other civil society and technology-driven initiatives are following suit: GEC launched media literacy in Bulgaria, Latvia, and Spain (Gabrielle, 2019).

References

Reviewed Policy Papers

Barbashin, Anton, *Improving the Western Strategy to Combat Kremlin Propaganda and Disinformation*, Washington, D.C.: Atlantic Council, 2018.

Barrett, Paul M., *Tackling Domestic Disinformation: What the Social Media Companies Need to Do*, New York: NYU Stern Center for Business and Human Rights, 2019.

Barrett, Paul M., Tara Wadhwa, and Dorothee Baumann-Pauly, *Combating Russian Disinformation: The Case for Stepping Up the Fight Online*, New York: NYU Stern Center for Business and Human Rights, 2018.

Bergmann, Max, and Carolyn Kenney, *War by Other Means: Russian Active Measures and the Weaponization of Information*. Washington, D.C.: Center for American Progress, 2017.

Berzina, Kristine, Nad'a Kovalčíková, David Salvo, and Etienne Soula, *European Policy Blueprint for Countering Authoritarian Interference in Democracies*, Washington, D.C.: German Marshall Fund of the United States, 2019.

Blanc, Jarrett, and Andrew S. Weiss, *U.S. Sanctions on Russia: Congress Should Go Back to Fundamentals*, Washington, D.C.: Carnegie Endowment for International Peace, 2019.

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence*, Santa Monica, Calif.: RAND Corporation, RR-2740-RC, 2018. As of March 8, 2021: https://www.rand.org/pubs/research_reports/RR2740.html

Bond, Ian, *Contested Space: Eastern Europe Between Russia and the EU*, London: Centre for European Reform, 2017.

Borshchevskaya, Anna, *Russia's Strategic Objectives in the Middle East and North Africa*, Washington, D.C.: Washington Institute for Near East Policy, 2017.

Brattberg, Erik, and Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Washington, D.C.: Carnegie Endowment for International Peace, 2018.

Brooking, Emerson T., and Suzanne Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*, Washington, D.C.: Atlantic Council, 2020.

Cederberg, Gabriel, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*, Cambridge, Mass.: Belfer Center for Science and International Affairs, 2018.

Christie, Edward Hunter, "Political Subversion in the Age of Social Media," *European View*, Vol. 18, No. 1, 2019, pp. 122–122.

Cohen, Howard, *Tech Tock . . . Time Is Running Out to Find Solutions to Mis- and Disinformation and Privacy Problems*, Cambridge, Mass.: Belfer Center for Science and International Affairs, 2018.

Danvers, William, *U.S. and Russia Relations Under Trump and Putin*, Washington, D.C.: Center for American Progress, 2016.

Dobrowolski, Daniel, David V. Gioe, and Alicia Wanless, "How Threat Actors are Manipulating the British Information Environment," *RUSI Journal,* Vol. 165, No. 3, 2020, pp. 22–38.

Eisentraut, Sophie, and Stephanie de Leon, *Propaganda and Disinformation in the Western Balkans: How the EU Can Counter Russia's Information War*, Berlin: Konrad Adenauer Foundation, 2018.

Fly, Jamie, Laura Rosenberger, and David Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, Washington, D.C.: German Marshall Fund of the United States, 2018.

Fried, Daniel, and Brian O'Toole, *Pushing Back Against Russian Aggression: Legislative Options*, Washington, D.C.: Atlantic Council, 2020.

Galeotti, Mark, *Controlling Chaos: How Russia Manages Its Political War in Europe*, London: European Council on Foreign Relations, 2017.

Ghosh, Dipayan, and Ben Scott, *#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet*, Cambridge, Mass.: Shorenstein Center on Media, Politics and Public Policy, 2018.

Giles, Keir, *Countering Russian Information Operations in the Age of Social Media*, London: Council on Foreign Relations, 2017.

Gonzalez, Mike, and Helle Dale, *The Axis of Disruption*, Washington, D.C.: Heritage Foundation, 2020.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, RR-2237-OSD, 2018. As of March 8, 2021: https://www.rand.org/pubs/research_reports/RR2237.html

Hosa, Joanna, and Andrew Wilson, *Zelensky Unchained: What Ukraine's New Political Order Means for Its Future*, London: European Council on Foreign Relations, 2019.

Janda, Jakub, *Full-Scale Democratic Response to Hostile Disinformation Operations*, Prague: European Values Center for Security Studies, Kremlin Watch Program, 2016.

———, *A Framework Guide to Tools for Countering Hostile Foreign Electoral Interference*, Prague: European Values Center for Security Studies, November 5, 2017.

Jones, Simon, *Combating Information Operations: Developing an Operating Concept*, Cambridge, Mass.: Belfer Center for Science and International Affairs, 2018.

Kagan, Frederick W., Nataliya Bugayova, and Jennifer Cafarella, *Confronting the Russian Challenge: A New Approach for the US*, Washington, D.C.: American Enterprise Institute, 2019.

Kamarck, Elaine, *Malevolent Soft Power, AI, and the Threat to Democracy*, Washington, D.C.: Brookings Institution, 2018.

Kenney, Carolyn, Max Bergmann, and James Lamond, *Understanding and Combating Russian and Chinese Influence Operations*, Washington, D.C.: Center for American Progress, 2019.

Knake, Robert K., *Banning Covert Foreign Election Interference*, New York: Council on Foreign Relations, 2020.

Kolga, Marcus, *Stemming the Virus: Understanding and Responding to the Threat of Russian Disinformation*, Ottawa: Macdonald-Laurier Institute, 2019.

Kolga, Marcus, Jakub Janda, and Nathalie Vogel, *Russia-Proofing Your Election: Global Lessons for Protecting Canadian Democracy Against Foreign Interference*, Ottawa: Macdonald-Laurier Institute, 2019.

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

Lamond, James, and Talia Dessel, *Democratic Resilience: A Comparative Review of Russian Interference in Democratic Elections and Lessons Learned for Securing Future Elections*, Washington, D.C.: Center for American Progress, 2019.

Lamond, James, and Jeremy Venook, *Blunting Foreign Interference Efforts by Learning the Lessons of the Past*, Washington, D.C.: Center for American Progress, 2020.

Liik, Kadri, *Winning the Normative War with Russia: An EU-Russia Power Audit*, London: European Council on Foreign Relations, 2018.

Lin, Herbert, Chris Painter, and Andrew Grotto, "Deterring Foreign Governments from Election Interference," in Michael McFaul, ed., *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, Stanford, Calif.: Stanford University, 2019, pp. 63-70.

Lucas, Edward, and Peter Pomeranzev, "Winning the Information War," *Washington*, Vol. 11, 2016, pp. 30–39.

Marcellino, William, Kate Cox, Katerina Galai, Linda Slapakova, Amber Jaycocks, and Ruth Harris, *Human–Machine Detection of Online-Based Malign Information*, Santa Monica, Calif.: RAND Corporation, RR-A519-1, 2020a. As of March 8, 2021: https://www.rand.org/pubs/research_reports/RRA519-1.html

Marcellino, William, Christian Johnson, Marek N. Posard, and Todd C. Helmus, *Foreign Interference in the 2020 Election: Tools for Detecting Online Election Interference*, Santa Monica, Calif.: RAND Corporation, RR-A704-2, 2020b. As of March 8, 2021: https://www.rand.org/pubs/research_reports/RRA704-2.html

Marcellino, William, Krystyna Marcinek, Stephanie Pezard, and Miriam Matthews, *Detecting Malign or Subversive Information Efforts over Social Media: Scalable Analytics for Early Warning*, Santa Monica, Calif.: RAND Corporation, RR-4192-EUCOM, 2020c. As of March 8, 2021: https://www.rand.org/pubs/research_reports/RR4192.html

Mazarr, Michael J., Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*, Santa Monica, Calif.: RAND Corporation, RR-2713-OSD, 2019. As of March 8, 2021: https://www.rand.org/pubs/research_reports/RR2713.html

Meister, Stefan, *Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign*, Washington, D.C.: German Marshall Fund of the United States, 2016.

Meleshevich, Kirill, and Bret Schafer, *Online Information Laundering: The Role of Social Media*, Washington, D.C.: German Marshall Fund of the United States, 2018.

Paul, Christopher, and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016. As of March 9, 2021: https://www.rand.org/pubs/perspectives/PE198.html

Persily, Nate, Megan Metzger, and Zachary Krowitz, "Confronting Efforts at Election Manipulation from Foreign Media Organizations," in Michael McFaul, ed., *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, Stanford, Calif.: Stanford University, 2019, pp. 35–42.

Persily, Nate, and Alex Stamos, "Regulating Online Political Advertising by Foreign Governments and Nationals," in Michael A. McFaul, ed., *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, Stanford, Calif.: Stanford University, 2019, pp. 27–34.

Pettyjohn, Stacie L., and Becca Wasser, *Competing in the Gray Zone: Russian Tactics and Western Responses*, Santa Monica, Calif.: RAND Corporation, RR-2791-A, 2019. As of March 9, 2021: https://www.rand.org/pubs/research_reports/RR2791.html

Polyakova, Alina, and Spencer Phipps Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Washington, D.C.: Brookings Institution, 2018.

Polyakova, Alina, and Daniel Fried, *Democratic Defense Against Disinformation 2.0*, Washington, D.C.: Atlantic Council, 2019.

Posard, Marek N., Marta Kepe, Hilary Reininger, James V. Marrone, Todd C. Helmus, and Jordan R. Reimer, *From Consensus to Conflict: Understanding Foreign Measures Targeting U.S. Elections*, Santa Monica, Calif.: RAND Corporation, RR-A704-1, 2020. As of March 9, 2021: https://www.rand.org/pubs/research_reports/RRA704-1.html

Postnikova, Elena, *Agent of Influence: Should Russia's RT Register as a Foreign Agent?* Washington, D.C.: Atlantic Council, 2017.

Rosenbach, Eric, and Katherine Mansted, *Can Democracy Survive in the Information Age?* Washington, D.C.: Belfer Center for Science and International Affairs, 2018.

Rudolph, Josh, and Thomas Morley, *Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies*, Washington, D.C.: German Marshall Fund of the United States, 2020.

Selga, Ēriks K, *The Legal Implications of Malicious Exploitation of Social Media*, Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2020.

Spaulding, Suzanne, Devi Nair, and Arthur Nelson, *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System*, Washington, D.C.: Center for Strategic and International Studies, 2019.

Stamos, Alex, Sergey Sanovich, Andrew Grotto, and Allison Berke, "Combatting State-Sponsored Disinformation Campaigns from State-Aligned Actors," in Michael A. McFaul, ed., *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, Stanford, Calif.: Stanford University, 2019, pp. 43–52.

Stronski, Paul, and Annie Himes, *Russia's Game in the Balkans*, Washington, D.C.: Carnegie Endowment for International Peace, 2019.

Ukrainian Election Task Force, *Exposing Foreign Interference in Ukraine's Election*, Washington, D.C.: Atlantic Council, November 15, 2018.

U.S. Senate Foreign Relations Committee, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, Minority Staff Report, January 10, 2018. As of March 8, 2021: https://www.foreign.senate.gov/imo/media/doc/SPrt_115-21.pdf

Vandewalker, Ian, and Lawrence Norden, *Getting Foreign Funds out of America's Elections*, New York: Brennan Center for Justice, 2018.

Watts, Clint, *Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions*, Washington, D.C.: German Marshall Fund of the United States, 2017.

Other Works Cited

Castillo, Michelle, "$100,000 in Russian-Bought Facebook Ads Could Have Reached Millions of Voters," CNBC, September 29, 2017. As of October 5, 2020: https://www.cnbc.com/2017/09/29/russian-facebook-ads-how-many-people-could-you-reach-with-100000.html

Cheney, Kyle, and Ashley Gold, "Facebook Suspends 'Inauthentic' Accounts, Sees Russia Link," *Politico*, July 31, 2018. As of April 4, 2021: https://www.politico.com/story/2018/07/31/facebook-suspends-inauthentic-propaganda-accounts-752615

European External Action Service's East StratCom Task Force, "Studies and Reports," *EUvsDisinfo*, webpage, undated. As of October 5, 2020: https://euvsdisinfo.eu/reading-list/

Facebook, "Business Help Center," webpage, undated. As of March 9, 2021: https://www.facebook.com/business/help/2593586717571940?id=673052479947730

François, Camille, Ben Nimmo, and C. Shawn Eib, *The IRACopyPasta Campaign*, New York: Graphika, October 21, 2019. As of August 30, 2020: https://public-assets.graphika.com/reports/graphika_report_copypasta.pdf

Gabrielle, Lea, Testimony Before the House Appropriations Subcommittee on State, Foreign Operations, and Related Programs, "United States Efforts to Counter Russian Disinformation and Malign Influence," July 10, 2019. As of October 5, 2020: https://docs.house.gov/meetings/AP/AP04/20190710/109748/HHRG-116-AP04-Wstate-GabrielleL-20190710.pdf

Gleicher, Nathaniel, "Removing Coordinated Inauthentic Behavior from Russia, Iran, Vietnam, and Myanmar," Facebook Blog, February 12, 2020a. As of April 6, 2021: https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/

Gleicher, Nathaniel, "Removing Coordinated Inauthentic Behavior," Facebook Blog, September 22, 2020b. As of October 5, 2020: https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-china-philippines/

Guess, Andrew M., Michael Lerner, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan, Jason Reifler, and Neelanjan Sircar, "A Digital Media Literacy Intervention Increases Discernment Between Mainstream and False News in the United States and India," *PNAS*, Vol. 117, No. 27, 2020, pp. 15536–15545.

Hao, Karen, "How Facebook Got Addicted to Spreading Misinformation," *MIT Technology Review*, March 11, 2021. As of March 25, 2021: https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/

Helmus, Todd C., James V. Marrone, Marek N. Posard, and Danielle Schlang, *Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions*, Santa Monica, Calif.: RAND Corporation, RR-A704-3, 2020. As of March 9, 2021: https://www.rand.org/pubs/research_reports/RRA704-3.html

"How Does the Twitter Fact-Check Policy Work and Why Was It Used Against Trump?" AS English News, May 28, 2020. As of March 9, 2021: https://en.as.com/en/2020/05/28/other_sports/1590669347_288101.html

Irex, "Strengthening Media Literacy in the Ukrainian Education System," webpage, undated. As of April 6, 2021: https://www.irex.org/project/strengthening-media-literacy-ukrainian-education-system

Isaac, Mike, and Kellen Browning, "Fact-Checked on Facebook and Twitter, Conservatives Switch Their Apps: 'If There Is No One to Argue with . . . How Long Will It Last?'" *Chicago Tribune*, November 11, 2020. As of December 20, 2020: https://www.chicagotribune.com/nation-world/ct-nw-nyt-conservative-social-media-20201111-tbpymgwvavc37cxw65g5p6iqeu-story.html

Jeong, Se-Hoon, Hyunyi Cho, and Yoori Hwang, "Media Literacy Interventions: A Meta-Analytic Review," *Journal of Communication*, Vol. 62, No. 3, 2012, pp. 454–472.

Media Literacy Now, *U.S. Media Literacy Policy Report 2020: A State-by-State Survey of the Status of Media Literacy Education Laws for K-12 Schools*, Watertown, Mass., 2020. As of October 5, 2020: https://medialiteracynow.org/wp-content/uploads/2020/01/U.S.-Media-Literacy-Policy-Report-2020.pdf

National Intelligence Council, *Foreign Threats to the 2020 U.S. Federal Elections*, Washington, D.C., March 10, 2021. As of April 5, 2021: https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

Nunziato, Dawn C., *Misinformation Mayhem: Social Media Platforms' Efforts to Combat Medical and Political Misinformation*, Washington, D.C.: George Washington University Law Faculty Publication, 2020.

Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, Washington, D.C., ICA 2017-01D, January 6, 2017.

Paul, Christopher, *Whither Strategic Communication? A Survey of Current Proposals and Recommendations*, Santa Monica, Calif.: RAND Corporation, OP-250-RC, 2009. As of March 9, 2021: https://www.rand.org/pubs/occasional_papers/OP250.html

Posard, Marek N., Hilary Reininger, and Todd C. Helmus, *Countering Foreign Interference in U.S. Elections*, Santa Monica, Calif.: RAND Corporation, RR-A704-4, 2021. As of April 5, 2021: https://www.rand.org/pubs/research_reports/RRA704-4.html

ProQuest, "Policy File Index: About," webpage, undated. As of April 6, 2021: https://proquest.libguides.com/policyfile/about

Ribeiro, Filipe N., Koustuv Saha, Mahmoudreza Babaei, Lucas Henrique, Johnnatan Messias, Fabricio Benevenuto, Oana Goga, Krishna P. Gummadi, and Elissa M. Redmiles, "On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook," *Proceedings on the ACM Conference on Fairness, Accountability, and Transparency*, Association for Computing Machinery, January 2019, pp. 140–149.

Ritter, Stephen, "What Does Twitter's Fact-Checking Tool Mean For Our Digital Identities?" Forbes, July 23, 2020. As of March 9, 2021: https://www.forbes.com/sites/forbestechcouncil/2020/07/23/what-does-twitters-fact-checking-tool-mean-for-our-digital-identities/?sh=579991053d51

Rodriguez, Salvador, "Mark Zuckerberg Says Social Networks Should Not Be Fact-Checking Political Speech," CNBC, May 28, 2020. As of March 9, 2021: https://www.cnbc.com/2020/05/28/zuckerberg-facebook-twitter-should-not-fact-check-political-speech.html

Rühle, Michael, "Deterrence: What It Can (and Cannot) Do," *NATO Review*, April 20, 2015. As of October 5, 2020: https://www.nato.int/docu/review/articles/2015/04/20/deterrence-what-it-can-and-cannot-do/index.html

"Trump Administration's 2020 Budget Request Calls for Closure of Three RFE/RL Language Services," Radio Free Europe, March 18, 2019. As of October 18, 2020: https://www.rferl.org/a/trump-administration-2020-budget-request-calls-for-closure-of-three-rfe-rl-language-services/29828716.html

U.S. Embassy in Latvia, "TechCamp Riga to Boost Investigative Journalism in Baltic States, Central and Eastern Europe," May 15, 2015. As of October 2, 2020: https://lv.usembassy.gov/pr_20150515/

Walter, Nathan, John J. Brooks, Camille J. Saucier, and Sapna Suresh, "Evaluating the Impact of Attempts to Correct Health Misinformation on Social Media: A Meta-Analysis," *Health Communication*, 2020a.

Walter, Nathan, Jonathan Cohen, R. Lance Holbert, and Yasmin Morag, "Fact-Checking: Meta-Analysis of What Works and for Whom," *Political Communication*, Vol. 37, No. 3, 2020b, pp. 350–375.

Walter, Nathan, and Sheila T. Murphy, "How to Unring the Bell: A Meta-Analytic Approach to Correction of Misinformation," *Communication Monographs*, Vol. 85, No. 3, 2018, pp. 423–441.

Warner, Mark R., U.S. senator from Virginia, "The Honest Ads Act," webpage, May 2019. As of April 6, 2021: https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act

Weinberger, Ariela, "Beyond Free Speech: Failures in Online Advertising Policy," New York: Roosevelt Institute, press release, September 29, 2020. As of October 10, 2020: https://rooseveltinstitute.org/2020/09/29/beyond-free-speech-failures-in-online-advertising-policy/

Yadav, Kamya, *Countering Influence Operations: A Review of Policy Proposals Since 2016*, Washington, D.C.: Carnegie Endowment for International Peace, November 30, 2020. As of April 5, 2021: https://carnegieendowment.org/2020/11/30/countering-influence-operations-review-of-policy-proposals-since-2016-pub-83333

About This Report

Since the Russian propaganda campaign that targeted the 2016 U.S. presidential election, numerous reports by academics and think tanks have recommended strategies and approaches for countering Russian propaganda. To better understand the full expanse and weight of such work, we conducted a careful review of policy recommendations from 2016 to 2020. We categorized the reports and highlighted key themes among policy recommendations. We conclude by identifying critical gaps.

We are grateful to the many researchers and analysts who have written previously on the topic of countering Russian disinformation; those writings provide the substantive basis of this report. We are also grateful to the RAND National Security Research Division and International Security Defense Policy Center leadership who helped make funding available for this research. Finally, we thank the reviewers of this study, Christopher Paul of the RAND Corporation and Colin Clarke of the Soufan Center. Any errors in this report are the sole responsibility of the authors.

The research reported here was completed in January 2021 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

This research was sponsored by the Office of the Secretary of Defense and conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD), which operates the RAND National Defense Research Institute (NDRI), a federally funded research and development center (FFRDC) sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

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

For more information on this publication, visit www.rand.org/t/RRA894-1.

www.rand.org

RR-A894-1