CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

APRIL 2023

IMPROVING DOMESTIC RESILIENCY TO DISINFORMATION TARGETING THE U.S. JUSTICE SYSTEM

PREPARED BY

MATT TRICE

Table of Contents

Acknowledgments

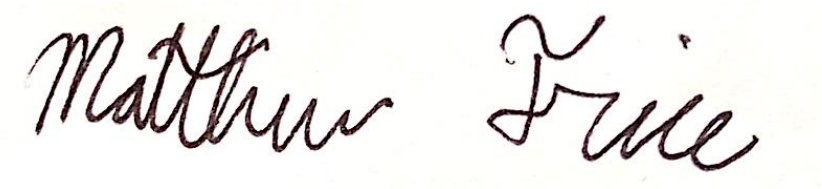
I would like to begin by thanking Suzanne Spaulding, Senior Adviser for Homeland Security in the International Security Program at the Center for Strategic & International Studies (CSIS), for giving me the opportunity to work with some of the premier minds and scholars in the national security arena throughout the writing of this capstone. I am grateful to be given the opportunity to apply the knowledge I have gained through my formal education at the Batten School.

This report would not have been possible without Devi Nair, Associate Director and Associate Fellow in the International Security Program at CSIS. Thank you for your unending support, sage advice, and all the time spent reviewing my work and meeting with me to share ideas. Your knowledge, guidance, and positivity kept me going throughout this process. I could not have had a better partner and thank you for your mentorship.

I would also like to thank Noah Myung, Associate Professor of Public Policy and Economics at the University of Virginia's Frank Batten School of Leadership and Public Policy, and Jim Wyckoff, Professor of Education and Public Policy at the University of Virginia's Frank Batten School of Leadership and Public Policy, for their thoughtful feedback, encouragement to push harder, and patience in helping me to navigate this entire process. I appreciated each of you making class engaging and am better for having both of you as advisors.

Honor Statement

On my honor as a student I have neither given nor received unauthorized aid on this assignment.



Disclaimer

The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy, University of Virginia. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgments and conclusions are solely those of the author, and are not necessarily endorsed by the Batten School, by the University of Virginia, or by any other agency.

Executive Summary

In 2022, 46% of American's stated that they had either very little or no confidence in the United States criminal justice system (Jones, 2022). That figure is 12 percentage points greater than the average share of no confidence expressed over the last 30 years between 1993-2022.

A major contributing factor to American's declining faith in the U.S. justice system is Russia. **As part of its more extensive disinformation operations aimed at undermining trust in Western democracies, Russia has grown adept at spreading narratives that actively undermine public trust and confidence in both the American judicial system and the rule of law.**

The public's perceived confidence in the U.S. justice system requires attention from policymakers because faith in the justice system, and democratic institutions as a whole, is essential for a well-functioning democratic society. Characterizing institutional confidence as political trust, Turper & Aarts (2017) note that political trust is "an essential component of the civic culture that is necessary for stability of democratic systems" (p. 417).

Based on a review of the relevant scholarly literature and assessment of interventions interested in building resiliency to disinformation, this report identifies three policy options that could be implemented in response to Russian disinformation that specifically targets the U.S. justice system:

1. Public threat awareness campaign paired with media and information literacy education
2. Network of state-level disinformation rapid response teams tasked with monitoring, publicizing, and responding to disinformation attacking the justice system
3. Expanding public-private partnerships between the federal government and social media and technology companies

To assess the merits of each of these potential policy options, this report examines the (a) direct cost, (b) effectiveness, (c) political feasibility, and (d) practical feasibility associated with each alternative. The subsequent analysis finds that **establishing a network of state-level disinformation rapid response teams offers the best value** in countering Russian disinformation centered on the U.S. justice system. The direct cost of this policy option is estimated to be roughly $12 million and has the potential to increase American citizens' correct identification of fake news by 0.80 standard deviations and reduce their beliefs in false news by 0.38 standard deviations.

Introduction

From its interference in the 2016 American Presidential election to the 2022 invasion and ongoing war in Ukraine, Russia has grown adept at employing a highly coordinated, high volume disinformation campaign as part of its long-term information warfare operations to undermine, destabilize, and cause harm to the citizens and governments of open Western democracies (*Disinformation and Russia's War of Aggression against Ukraine*, 2022; Theohary, 2018). One primary target that faces the persistent threat of Russia's disinformation campaign is the United States' justice system. While disinformation operations used by Russia during the war in Ukraine and in the 2016 American Presidential election has been elevated in American public discourse, a persisting lack of the explicit recognition in how Russia systematically advances disinformation targeting justice system instructions remains. By specifically targeting the justice system, Russian disinformation strives to erode the perceived legitimacy and integrity of judicial institutions, personnel, and legal processes which are integral to the overall strength of American democracy.

This report examines the nature of Russian disinformation operations that specifically target the United States' justice system and considers policy options as a means to respond and fight back against the threat. It provides an overview of the problem, explains its significance, situates the stake the Center for Strategic and International Studies (CSIS) has in addressing the issue, and considers the magnitude of the consequences and downstream effects of the problem. Next, this report reviews the body of evidence on potential solutions and evaluates the direct costs, overall effectiveness, and feasibility associated with each solution. It concludes with a policy recommendation and discusses the necessary next steps for implementation.

This report's final recommendation calls for establishing a network of state-level disinformation rapid response teams. Disinformation rapid response teams have already been suggested by some American policymakers as a way to address disinformation along with vulnerabilities within the justice system it seeks to exploit (*Disinformation Task Force Concluding Report*, 2022). This recommendation offers the greatest value in countering Russian disinformation that specifically targets the U.S. justice system, relative to other potential policies that this report details below, and is an avenue through which greater attention and saliency of the threat disinformation poses to the justice system can be elevated in the public domain.

Problem Statement

The vulnerability of the American criminal justice system's perceived legitimacy and integrity to disinformation is too high relative to average levels from the last 30 years. In 2022, Gallup's annual public opinion poll surveying the confidence citizens have in major American institutions saw 14% of respondents state they had either a "great deal" or "quite a lot" of confidence in the United States (U.S.) criminal justice system (see Figure 1). In contrast, the figure was 25% for the U.S. Supreme Court (Jones, 2022). The share of confidence reported for each institution set a new record, reaching the lowest point over the last three decades (Jones, 2022).

As public confidence in the criminal justice system and Supreme Court has declined, the threat environment has grown. In 2021, over 4,500 threats were issued against U.S. federal judges according to statistics from the U.S. Marshals Service reflecting an exponential growth in the rate of threats over the past several years according to the Director of U.S. Marshals Service Ronald Davis (Lynch & Lynch, 2022). As part of its more extensive disinformation operations aimed at undermining trust in western democracies, Russia has exacerbated this decline in confidence and grown adept at spreading narratives that actively undermine public trust and confidence in both the American judicial system and the rule of law.

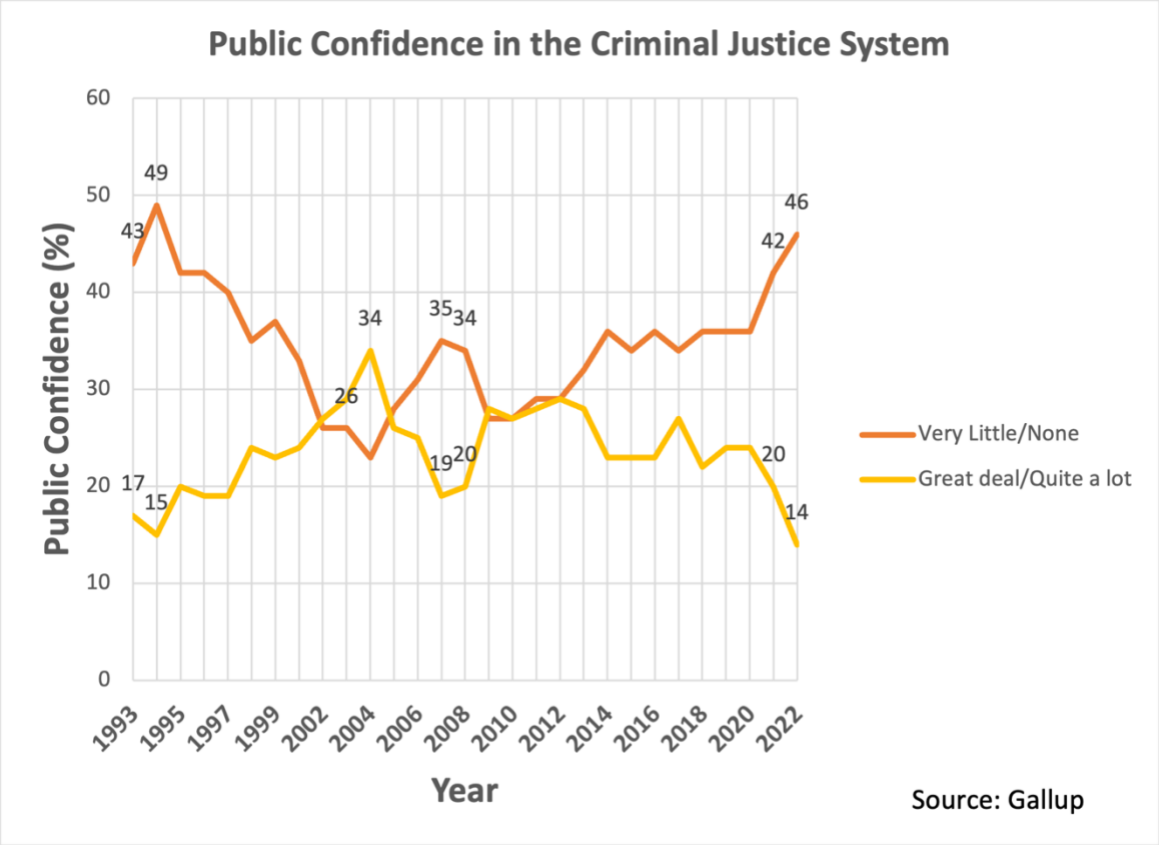


Figure 1: Public Confidence in the Criminal Justice System

Client Overview

Serving as a bipartisan, nonprofit policy research organization the Center for Strategic and International Studies (CSIS) works to define the future of national security (*About CSIS | Center for Strategic and International Studies*, n.d.). The work at CSIS is uniquely characterized by non-partisanship, inter-disciplinary scholarship, innovation, professionalism, and integrity. The scholars, subject matter experts, and resources at CSIS' disposal uniquely position it to host dialogues, deliver informed analysis, and make impactful recommendations to key policymakers across the national security policy sphere.

In the course of its work to define the future of national security, the vulnerability of the U.S. justice system to Russian disinformation is a problem particularly relevant to CSIS. The Defending Democratic Institutions project at CSIS "seeks to counter foreign and domestic adversaries in their efforts to disrupt democracy and cultivate a public distrust of democratic institutions via cyber and disinformation operations" (*Defending Democratic Institutions | International Security Program | CSIS*, n.d.). With the U.S, justice system being a focal element of the project, CSIS experts associated with the project have written analytical reports about Russian disinformation and hosted events with critical stakeholders since at least 2018.

Today, tensions between the US and Russia continue to increase and show no signs of slowing down. In working to advance its foreign policy objectives, Russia has displayed a disregard for fundamental international standards through the ongoing war in Ukraine where it has deployed disinformation operations in concert with the initial invasion (Bowen & Welt, 2021; *Disinformation and Russia's War of Aggression against Ukraine*, 2022). Russia's information operations, influence campaigns, and disinformation tactics threaten not only the US and American democratic values, but liberal democracies around the globe today as much as they ever have in the past. As such, CSIS recognizes the significance of the problem of Russian disinformation undermining the US justice system and has actively taken on a role of elevating the issue in policy discussions about national security.

.

Problem Background

Legal and Regulatory Environment

The Global Engagement Center (GEC) at the Department of State (DOS) is responsible for leading the U.S. Government's (USG) effort in countering disinformation and propaganda from foreign actors (GEC Special Report, 2020). In addition to coordinating the USG response to Russian disinformation, GEC partners with research, civil society, and academic institutions in the fulfillment of its mandate to combat disinformation aiming to influence the security, policies, or stability of the U.S. (Global Engagement Center, n.d.; Lucas et al., 2022).

Causes of the Problem

Disinformation that specifically targets and adversely impacts the legitimacy and integrity of the American justice system is driven by multiple root causes. These causes are categorized into primary root causes and secondary root causes. Primary root causes directly contribute to the problem. Secondary root causes further primary root causes, though they hold no direct relationship with the problem (Wagner, 2014). This section begins by laying out the disinformation narratives Russia employs in spreading its propaganda, then outlines the primary root causes followed by secondary root causes.

Russian Disinformation Narratives

The false narratives Russia leverages in its efforts to spread disinformation about the American judicial system are strategic in nature. Russian disinformation "latches on to legitimate criticisms of the justice system" (Spaulding & Rishikof, 2018, para. 16) to advance notions that partisanship, corruption, and fundamental unfairness are pervasive throughout the entire system. Spaulding et al. (2019) identify four key Russian narratives that reinforce the assertion that the judicial system is neither impartial nor independent. These frames assert that the justice system "tolerates, protects, and covers up crimes committed by immigrants[;] operationalizes the institutionally racist and corrupt police state[;] directly supports and enables corporate corruption[; and] is a tool of the political elite" (Spaulding et al., 2019, p. 2).

Primary Root Causes

Primary root causes of the disinformation problem stem from both the tactical dissemination methods Russia employs to advance false narratives as well as the character of the false narratives themselves. One primary root cause behind the false narratives that target the U.S. justice system is the plausible deniability that they afford to Russia (*GEC Special Report*, 2020). The state-supported actors who advance these false narratives masquerade as authentic, independent organizations and individuals. Examples of these actors include Russian state-linked media outlets, social media groups, and proxy websites. While these actors advance Russian foreign policy objectives that directly damage and threaten the legitimacy of the American justice

system through the spread of disinformation, Russia's government looks to deny any association with said actors.

At the tactical level, Russia uses a mix of multichannel and high-volume messaging to spread disinformation. Paul & Matthews (2016) highlight this feature, labeling "the contemporary Russian model for propaganda as 'the firehose of falsehoods'" (p. 1). The multiple channels of the Russian disinformation network include state-funded media outlets, namely Sputnik News and RT, which spread propaganda and disinformation in support of the Kremlin's foreign policy goals, appearing as legitimate international news outlets (Report, 2022). The spread of disinformation by Sputnik News and RT leverages several mediums, such as "social media, satellite television, and traditional radio and television broadcasting" (Paul & Matthews, 2016, p. 2).

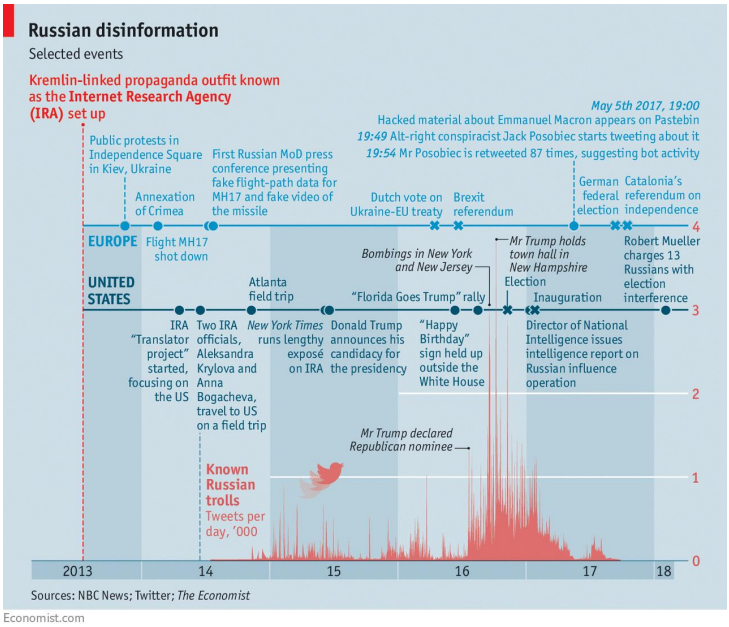


Figure 2: IRA-linked Disinformation

Russia also sponsors an army of internet "trolls" who work to harness the political and racial identities of authentic social media accounts to instigate anger and drive divisiveness (Freelon & Lokot, 2020). Many of these trolls and social media operatives are employed by the Internet Research Agency (IRA), a private company financially supported by the Kremlin (Freelon & Lokot, 2020). Chen (2015) describes how the IRA has "become known for employing hundreds of Russians to post pro-Kremlin propaganda online under fake identities, including on Twitter, in order to create the illusion of a massive army of supporters" (para. 9). The digital disinformation campaign that Russian trolls facilitate is not only amplified by the sheer number of operatives, but also by the rate at which the operatives are actively creating disinformation (see Figure 2). Paul & Matthews (2016) assert that "the trolls are on duty 24 hours a day, in 12-hour shifts, and each has a daily quota of 135 posted comments of at least 200 characters" (p. 2).

Proxy websites are another primary root cause of Russian disinformation narratives. These sites are aligned with the Kremlin's overall disinformation strategy but external to Russia itself. Proxy sites play a strategic role in furthering the proliferation of disinformation that serves to undermine trust in western democracies and their institutions. This role is evidenced in proxy's ability to publish articles that Russian news sites and other state-sponsored media outlets can reference, providing the appearance of objectivity and impartiality (Harding, 2015).

Secondary Root Causes

The first secondary root cause contributing to many primary causes of the disinformation problem is Russia's New Generation Warfare doctrine. This military strategy employs information itself as a weapon on a battlefield that has shifted from the physical plane to the psychological (Derleth, 2020). Issued in 2014, Russia's New Generation Warfare doctrine has governed the strategic approach that Putin and the Kremlin has used in Russia's disinformation campaign (Oliker, 2015).

Another secondary root cause connected to primary causes of the Russian disinformation problem is the widespread use of social media by the American public. Seven out of ten Americans now engage with one another on social media (Social Media Fact Sheet, 2021). While the number of Americans actively engaged on social media increases, so does the amount of time users find themselves on the various social media platforms. On average, Americans spend over 1,300 hours annually on social media sites, with Facebook leading the way at 325 hours over a year (Suciu, 2021).

As Americans' usage of social media has grown over the last decade (See Figures 3 & 4), trust in traditional media outlets and sources of news has declined (Brenan, 2021; Social Media Fact Sheet, 2021). This development has made it easier for state-funded media outlets posing as independent, objective news organizations and Russian social media troll farms to captivate Western audiences with the propaganda they produce. In 2021, only 46% of Americans reported having trust in traditional media, the first time that less than half of American's expressed faith in traditional media (Salmon, 2021).

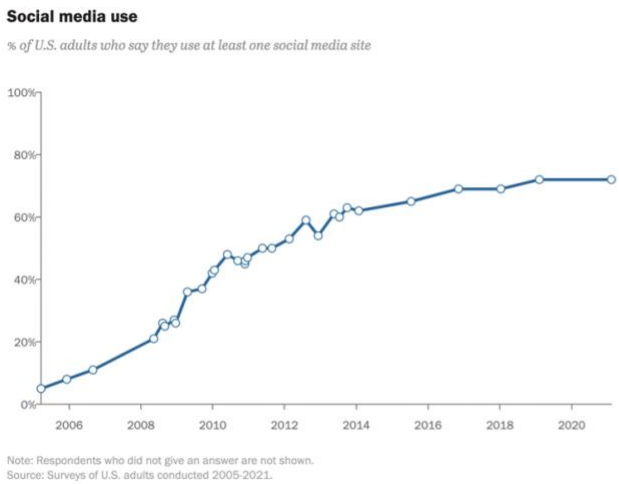


Figure 3: Americans' Social Media Usage

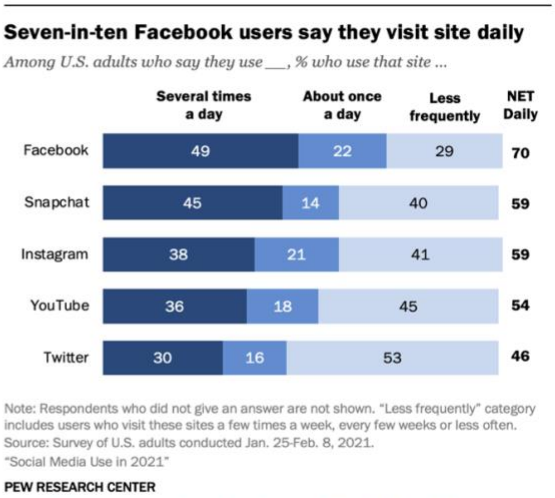
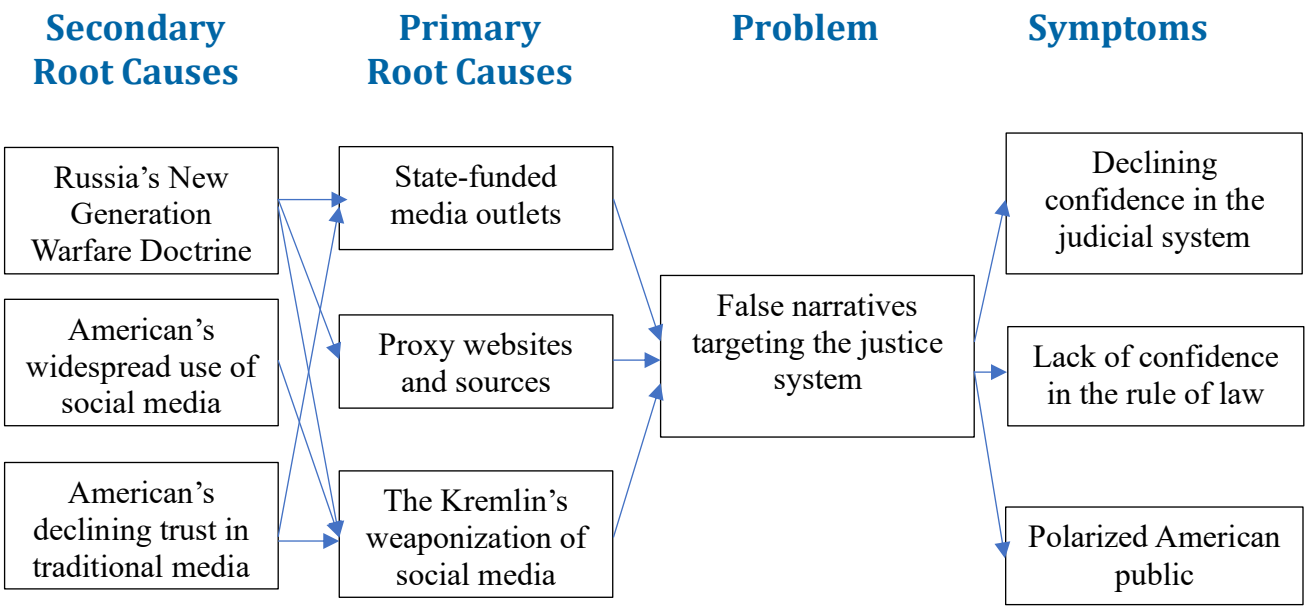


Figure 4: Daily Social Media Usage


Secondary Root Causes
Primary Root Causes
Problem
Symptoms
Russia's New Generation Warfare Doctrine
American's widespread use of social media
American's declining trust in traditional media
State-funded media outlets
Proxy websites and sources
The Kremlin's weaponization of social media
False narratives targeting the justice system
Declining confidence in the judicial system
Lack of confidence in the rule of law
Polarized American public

Consequences of the Problem

Symptoms of the Russian disinformation problem include the lack of confidence from the American public in the justice system and rule of law, as well as an overall more polarized citizenry. These symptoms bear costs on society in both direct and indirect ways. The direct costs to society associated with Russian disinformation efforts, however, are hard to quantify. In an attempt to identify the monetary cost to society associated with fake news in the context of the COVID-19 pandemic, researchers at the Johns Hopkins Bloomberg School of Public Health estimated that misinformation and disinformation about COVID-19 vaccines was responsible for $50 to $300 million worth of costs on a daily basis (*COVID-19 Vaccine Misinformation and Disinformation Costs*, n.d.). Though the COVID-19 target, context, and scope of the disinformation informing this cost estimate is characterized differently than Russian disinformation targeting the U.S. justice system, the estimate still provides a sense as to the order of magnitude of the societal costs that disinformation can generate.

In a 2019 study commissioned by CHEQ, a private computer and network security company, Professor Roberto Cavazos at the University of Baltimore analyzed the monetary costs associated with disinformation and fake news, though the disinformation cases used in the analysis were not specifically tied to Russia. The study examined incidents where disinformation and false news stories changed the stock market valuations of private companies, notably identifying how one fake news story "caused stock market losses of $300 billion in a single incident" (The Economic Cost of Bad Actors on the Internet, 2019, p. 6). The commissioned study concluded that "based on an analysis of past cases involving fake news inflicting damage on global markets, we find a potential loss up of up to 0.05% of stock market value is at risk due to fake news. This amounts to $39 billion annual loss as a direct result of fake news" (The Economic Cost of Bad Actors on the Internet, 2019, p. 6). While it is difficult to translate the direct monetary costs found in this study to the direct costs of Russian disinformation and propaganda focused on subverting the American judicial system, understanding the magnitude of the direct economic impact of disinformation in the context of private company valuations and global stock markets provides a foundational perspective of the magnitude of the problem.

The costs and outcomes of disinformation associated with American elections offer another example for understanding the potential harmful implications concerning the reduction of trust in the judicial system and rule of law. When the legitimacy of the 2020 election was called into question from numerous politicians, namely President Donald Trump, violence and threats targeting public officials, election workers, and the media abounded, culminating in the January 6th insurrection attack on the U.S. Capitol. Disinformation had a hand in provoking these attacks and continued being a significant concern heading into the 2022 Congressional elections (Panditharatne et al., 2022). It stands to reason that similar violent outcomes could take place as a result of disinformation targeting the justice system, such as physical attacks against U.S. court system infrastructure or personnel such as, judges, lawyers, and jury members.

The opportunity costs associated with Russian disinformation also burden society. An example of one opportunity cost is the funding received by the GEC. The GEC is responsible for leading the USG's effort in countering disinformation and propaganda from foreign actors (GEC Special Report, 2020). The GEC received roughly $62 million in 2020, money which could have been used to pursue other means rather than appropriated to combat disinformation (THE GLOBAL ENGAGEMENT CENTER: LEADING THE UNITED STATES GOVERNMENT'S FIGHT AGAINST GLOBAL DISINFORMATION THREAT, 2020)

Evidence on Potential Solutions

This literature review identifies, analyzes, and synthesizes the scholarship on potential methodologies to combat Russian disinformation aiming to undermine confidence in the American judicial system and the rule of law. It identifies policy solutions that subject matter experts have recommended in the past. It analyzes the related research in the social science community, giving particular focus to the efficacy of the recommended policy intervention. To defend democratic values and bolster confidence in the U.S. justice system, proposed policy solutions target Russia's three-part pathological model used in its disinformation campaign, specifically the production, distribution and redistribution, and consumption of subversive content (Matthews et al., 2021).

Limiting Exposure by Addressing Production

Policy interventions that limit the exposure Americans experience to Russian disinformation seeks to remedy the public's declining faith in the U.S. justice system by curtailing new fraudulent and distortive information Russia produces. The literature discusses several defensive practices governments could employ to target the production side of disinformation campaigns, thereby limiting the exposure of propaganda citizens encounter (Matthews et al., 2021). These defensive interventions include digital identity verification policies; data protection laws; government content regulation policies; and, cyber operations (Matthews et al., 2021).

The overall strength of evidence in the literature surrounding the efficacy of these four practices targeting the production of disinformation is weak, as the magnitude of existing empirical research is limited. Moreover, scholars have claimed that solely employing a strategy singularly targeting the production aspect of Russia's disinformation pathological model may not affect the problem (Scheufele & Krause, 2019). This possible absence of an effect is due to individuals' trust in the disinformation narratives persisting as a result of the false narrative being perpetuated by other influential actors, such as news pundits, politicians, and members within their social circles (Matthews et al., 2021; Scheufele & Krause, 2019). Still, policies harnessing multimodal approaches to combat disinformation and its effects may benefit from incorporating methodologies focused on the production of disinformation into their overall strategy.

Focusing on digital identity verification policies, some scholarly research has studied the effects of using blockchain technologies and deep learning techniques to accurately identify rumors on social media. Rani et al. (2022) studied how blockchain technology and deep learning techniques can work to detect, as well as prevent, the transmission of rumors online. The experimental results from their proposed model outperformed other methods scholars have studied, achieving a 99.63% accuracy rate in rumor detection with a false positive rate of only 0.13% (Rani et al., 2022). In a comparative analysis of recent works regarding the accuracy of other rumor detection models, the next most accurate deep learning model had an accuracy rate of 97.0% (Tida et al., 2022). The

dataset used to test the model consisted of news articles from 2016. 12,600 real-world news articles were labeled 'truthful' as the articles were sourced from Reuters, a reputable news outlet and 12,600 news articles were categorized as 'fake' as they were sourced from unreliable websites according to the fact-checking organization Politifact. Though this research focuses on how blockchain technologies and deep learning techniques can detect rumors and inauthentic information online, there is little to no discussion about how these digital identity verification policies can prevent exposure to distorted content online or lessen the volume of disinformation individuals come across.

Alternative Narratives and Fact-Checking Tags

Potential solutions to Russia's disinformation campaign could target the distribution channels and circulation methods of propaganda supported by the Kremlin. Russia uses a variety of tactics across different mediums to disseminate false narratives and disinformation targeting the U.S. justice system, including traditional news media; state-funded global media outlets; proxy websites and sources; and social media (Matthews et al., 2021; Paul & Matthews, 2016; Vladimir Putin's Historical Disinformation, 2022). The literature discussing interventions that focus on reducing the spread of disinformation content considers the usage of fact-checking tags in media. The effects of fact-check tags attached to social media posts and general warnings on belief in false stories, specifically Facebook, was studied in a randomized controlled experiment (Clayton et al., 2020). The study's findings provide evidence that false headlines are viewed as less accurate as users are exposed to general warnings about misinformation on social media. This effect of lower perceived accuracy holds when "Disputed" or "Rated false" tags accompany headlines, reducing the share of users believing the fake news by 10 percentage points (Clayton et al., 2020). The experimental results are consistent across the political views of participants, though the magnitude of both effects only modestly reduced trust in the false news (Clayton et al., 2020). The literature also discusses evidence surrounding the effectiveness of fact-checking labels relative to the timing of the fact-check. In a study conducted by Brashier et al. (2021), participants' who were exposed to fact-checking tags immediately after viewing a story headline saw a reduction of misclassifying a headline one week later by 25.3%, relative to a 5.7% reduction when the fact-check tags were shown prior to the headline.

The consistency of causal claims from the literature discussing policy solutions targeting the dissemination channels of disinformation is somewhat mixed and varies depending on the specific nuances of the intervention. While Clayton et al. (2020) provide evidence that fact-checking tags on social media can help prevent the intended effects of disinformation from taking hold, other scholarly works are more skeptical and suggest that further research is needed. One section of the literature offers up the following line of thinking: if audiences encounter content that is flagged, then they will cease to believe in, share, and be influenced by the false or inaccurate information to which they had viewed (Matthews et al., 2021). Yet, there is a strong body of social psychology research studying the encoding of beliefs individuals hold. The findings from this body of research state that this assumption about flagged content does not hold

and that individuals can still be influenced by false narratives (Lewandowsky et al., 2012).

In three individual experiments conducted between August 2011 and November 2012, Thorson (2016) randomly assigned participants to be exposed to negative political information in news articles where the information was later discredited. The experimental results across all three studies found that being exposed to negative political information increased the negative attitudes participants had toward that politician, even when the negative information was effectively discredited (Thorson, 2016). Thorson (2016) calls these effects 'belief echoes.' These belief echoes persisted even in the case when false information was immediately corrected. Relatedly, Lewandowsky et al. (2012) point to a plethora of research that has consistently found that issuing a retraction fails to eliminate the influence of false or inaccurate information, even after persons believe, comprehend, and later recall the retraction. They state that at best, a retraction will cut in half the quantity of references to false information and that, at worst, a retraction will not reduce the number of references at all (Johnson & Seifert, 1994; Lewandowsky et al., 2012).

These findings from Thorson (2016) and Lewandowsky et al. (2012) address what is known in social psychology as the Continued Influence Effect. The Continued Influence Effect is a phenomenon where obsolete and discredited information continues to impact beliefs and behaviors (Kan et al., 2021). To effectively counter the continued influence effects of disinformation, Kan et al. (2021) conducted a randomized controlled trial that consistently found that providing an alternative narrative to causally explain a correction reduced the persistent reliance on misinformation. Previous work from Lewandowsky et al. (2012) supports their empirical findings, noting that issuing preexposure warnings to individuals, repeating information and story corrections to bolster efficacy, and providing an alternative explanation within the correction to plug causal gaps can help reduce continued influence effects.

Targeting Content Consumption: Inoculation & Media and Information Literacy Interventions

The final defensive practice in combating disinformation specifically targets how content is consumed online. This strategy looks to educate and increase the awareness of consumers about disinformation itself, as doing so mitigates the subversive narratives and undermining of democratic values that Russian disinformation looks to instill in American citizens. Audience inoculation methodologies and media literacy programs are a few of the promising solutions to educate consumers and disrupt disinformation operations.

Strategies to inoculate audiences are based on the theory that exposing individuals to diluted arguments or weakened oppositional statements contrary to one's beliefs can increase resistance to potentially stronger, more persuasive attacks in the future (Compton et al., 2016; Dillingham & Ivanov, 2016). In Banas & Rains' (2010) meta-analysis examining the effectiveness at conferring resistance of inoculation theory, the

results across 54 cases found that inoculated persons had increased resistance to future persuasive attacks by 0.43 standard deviations relative to persons who were not inoculated. The magnitude of the effect size, however, was moderate (Cohen's d =0.43) based on J. Cohen's (2013) standards of magnitude (small effect size: d =0.10-0.20; medium effect size: d =0.21-0.50; large effect size: d =0.51-0.80). In addition, inoculation effects maintained resistance to persuasive attacks for long periods of time between initial inoculation and encountering a persuasive attack. While initial research about inoculation effects to disinformation treatment looks promising, future research is needed to scale treatment effects on larger sets of individuals (Matthews et al., 2021).

Media and information literacy (MIL) education encapsulates a large array of tactics and techniques that aim to improve the skills and knowledge of consumers when processing media content (Matthews et al., 2021). Overall, studies of the education interventions fundamental to MIL programs have been found to increase media knowledge and reduce negative attitudes or behaviors that are aggravated by the media (Matthews et al., 2021). In a national sample of over 600,000 American citizens conducted in 2017, Jones-Jang et al. (2021) found evidence that information literacy interventions significantly increased how accurately participants identified fake news. While some of the research on the effectiveness of MIL education has found these inoculation interventions to be effective in the long-run (Maertens et al., 2021), there is no clear consensus yet in the literature, and other scholars have called for additional inquiry into these

Policy Alternatives

This section considers policy alternatives raised in the literature that could be implemented to address the threat Russian disinformation poses to the perceived legitimacy and integrity of the U.S. justice system. Three options are considered: a public threat awareness campaign paired with MIL education programming; disinformation rapid response teams focused on monitoring, publicly identifying, and responding to justice system-targeted disinformation; and expanding public-private partnerships between the federal government and social media and technology companies.

1) Public awareness campaign and MIL education

A campaign to engage the public and raise awareness about how disinformation targets justice system personnel and institutions could be implemented to safeguard the legitimacy of judicial institutions as well as the physical safety of court officials. This public awareness and community engagement campaign would be a nationwide effort supported by and coordinated with appropriate federal entities, namely the Department of Justice's (DOJ) National Security Division (NSD), Community Relations Service (CRS), and the GEC at DOS. While the threat awareness campaign would occur on a national scale, it would be operationally carried out at the state level by state court system officials. Specifically, state court systems could use their Public Information Officer (PIO) to lead the campaign and liaise with community members and local leaders. State court PIOs would coordinate information-sharing efforts throughout their state and facilitate community outreach engagements to educate the public about the role of the courts in the justice system and dismantle the false narratives Russian disinformation strives to advance.

Information sharing and public warning communications about disinformation targeting the justice system could be distributed to the public through television and radio messages, while in-person community engagement could be facilitated at state courthouses, local schools, and community centers. The campaign would also implement in-person and virtual learning programs, such as media and information literacy training and disinformation inoculation interventions, both of which have shown promising effects in countering the belief in disinformation narratives (Banas & Rains, 2010; Jones-Jang et al., 2021; Matthews et al., 2021). MIL education programming and inoculation training could also be posted online to the official website of each state's court system, thereby providing an online toolkit that citizens could conveniently access on their own and that judicial personnel could refer the public toward, similar to the Cybersecurity and Infrastructure Security Agency's (CISA) COVID-19 Disinformation Toolkit (COVID-19 Disinformation Toolkit | CISA, n.d.).

The duration and initiation of the public awareness campaign could vary across states as any decisions regarding timelines may be better served by letting state court officials determine how to phase in the campaign to best serve the citizens of their state. This could lead to some states being early adopters of the threat awareness campaign while others may come along later, though the federal government could incentivize states to be early adopters by authorizing federally-funded pass-through funds from DOJ to state court systems to pay for MIL education initiatives from the campaign. Federal pass-through funds would give states discretion in allocating money to cover campaign costs, offering greater flexibility than competitive federal grants and allowing each state court system to receive a share of the funds, granted that they adhere to any associated federal requirements.

2) Rapid Response Teams

The establishment of a rapid response team focused on countering disinformation which specifically targets the legitimacy of the U.S. justice system could be implemented to address the threat Russian disinformation narratives pose toward the overall integrity of democratic institutions. As noted in a 2022 report from the Arizona Supreme Court's Task Force on Countering Disinformation (TFCD), time is a critical factor whenever disinformation enters the public discourse, be it via social media or through another medium. With time being of the essence, it is imperative to not only swiftly discredit false stories with accurate information, but also provide an alternative narrative to causally explain a correction as evidence from the literature suggests doing so reduces the continued influence effects of disinformation (Kan et al., 2021; Lewandowsky et al., 2012). A rapid response team could be implemented to secure the timely supply of accurate information and alternative/explanatory narratives in a time of crisis, thus working to counter disinformation and the harmful beliefs it looks to engender. These beliefs include holding the view that the U.S. justice system is flat out corrupt, an instrument manipulated by political elites, and serves without integrity.

Because of the need for judicial institutions and personnel to remain independent, so as to uphold their credibility and legitimacy, rapid response communication teams would be comprised of individuals from organizations familiar with court proceedings and judicial issues but not directly employed by the courts themselves. Organizations such as the American Bar Association (ABA), American Board of Trial Advocates (ABOTA), National Judicial College (NJC), and the National Center for State Courts (NCSC) could offer the necessary infrastructure and human capital to support the operations of disinformation rapid response teams. Using Arizona's TFCD recommendation for staffing a rapid response communications unit as a template, teams would be comprised of attorneys, media members, academics, and retired judges (Goldstein, 2021).

While the coordination in establishing rapid response units could be supported by local and regional federal partners, such as DOJ's U.S. Attorney Offices, individual teams would be implemented at the state level across every state. A combination of public and private funding would be necessary for each rapid response team to execute its duties.

Funding support from non-government entities could come from sources such as non-profit legal organizations; academic institutions, such as law schools; and private sector law firms from whom the lawyers on each team practice law. Attorneys participating on rapid response teams from private law firms would work pro bono, while non-profits and academic institutional sponsors of rapid response teams would allocate funds from their personal budgets to the effort. Public funding from the government to support rapid response teams could be allocated in the form of federal and state grants; the National Science Foundation (NSF) has issued grants related to research about disinformation rapid response capabilities in the past (*$2.25 Million in National Science Foundation Funding Will Support Center for an Informed Public's Rapid-Response Research of Mis- and Disinformation*, 2021).

3) Expanding public-private partnerships

Expanding public-private partnerships and coordination between institutions of justice and social media companies could be implemented to strengthen public confidence in and the perceived legitimacy of the U.S. justice system. While disinformation can be disseminated across a host of mediums, social media platforms have been a key avenue in how Russia, as well as other foreign actors, have spread maligning narratives attacking the integrity of the justice system. The expanding partnership would have two main components, requiring action from both the federal government as well as private social media and technology companies.

The first component would be a federal interagency campaign to educate and raise awareness about disinformation that targets the American judicial system. The campaign would primarily target executives and leaders from major social media platforms (i.e., Facebook, Twitter, Snapchat, Instagram, Reddit, etc.) and other big technology companies, such as Amazon, Apple, Google, and Microsoft. In addition, the campaign's secondary audience would be any public sector leaders in the interagency who may not know or fully appreciate the current threat landscape of the justice system. The federal agency in charge of leading this awareness campaign would be the GEC at DOS, as the scope of the campaign falls under GEC's mandated mission ("About Us - Global Engagement Center," n.d.). GEC could host virtual or in-person roundtable discussions where attendees would learn how disinformation specifically harms the justice system and organizations could share best practices for combatting disinformation on social media platforms. While many social media and technology companies may be aware about disinformation on their platforms from past high-profile instances (i.e., during elections, the COVID-19 pandemic, and Russia's invasion of Ukraine), the campaign would highlight how the justice system is vulnerable to disinformation attacks.

The second component would be the implementation of a voluntary code of conduct formulated by private sector companies in the social media and technology industry. The code could stipulate universal policies for addressing disinformation that which specifically targets the justice system. Following the federal education campaign, social media platforms would move to formulate a self-governing code of conduct to address

disinformation on their platforms. Policies of the voluntary code could include committing to authenticating the identity of accounts, taking down fake accounts, identifying content spread by bot accounts, providing digital literacy trainings for users, and flagging content with fact-checking tags. To meet these commitments, social media platforms could contract out to independent third-party companies who would be responsible for executing the commitments in the Code of Conduct or they could hire staff internally to maintain their commitments. While some companies already make use of these practices (R. S. Cohen et al., 2021), a code of conduct would provide a universal framework across platforms for countering disinformation. There is also some evidence in the literature that fact-checking tags attached to social media posts are effective at reducing the spread of disinformation (Clayton et al., 2020). Furthermore, there is precedent for this type of code of conduct as the European Commission's "Code of Practice on Disinformation" is a EU-wide voluntary commitment signed by 34 social media and technology companies to combat disinformation. Each company is responsible for upholding expectations the Code sets and the Commission does not have any regulatory or enforcement authority in monitoring if companies are abiding by the Code (The 2022 Code of Practice on Disinformation | Shaping Europe's Digital Future, 2023).

The timeline for the two-pronged, federally-led awareness campaign and voluntary code of conduct could vary. GEC could carry out the campaign on an annual basis, each year looking to reach a wider audience of appropriate public and private sector leaders. Developing and implementing the code of conduct would be determined by the signatory companies, though the code would stay in place following its establishment. Given that the code would be on a voluntary basis, some companies may commit to sign up earlier than others though the variability in who and when between these early and late adopters is difficult to determine.

Evaluating Alternatives

This section evaluates each of the three alternatives—public awareness campaign/MIL education, rapid response teams, and expanding public-private partnerships—against three criteria: direct cost, effectiveness, political feasibility, and practical feasibility. Appendix A describes how each criterion was measured. Appendix B explains the calculations for projecting direct costs over a five-year implementation period.

Alternative 1: Public Awareness Campaign and MIL Education

Direct Cost - $503.8 million

In estimating the cost of an education and awareness campaign about disinformation targeting the US justice system, I used cost data sourced from the New York City Department of Health and Mental Hygiene (DOHM) in a study examining the return on investment of New York City's COVID-19 Vaccination Campaign. The study examined the time between December 14, 2020 through January 31, 2022 and estimated that the direct costs of advertisement and community outreach of the vaccination campaign totaled $243,390,758.20, reported in 2021 USD (Sah et al., 2022). Separately during the summer of 2020, the Office of the Assistant Secretary for Public Affairs in the Department of Health and Human Services (HHS) led a national $265 million public education and awareness campaign promoting COVID-19 vaccinations and prevention efforts (*COVID-19 Information on HHS's Public Education Campaign*, 2022). A significant amount of the funding for the HHS public education campaign went toward developing public service announcements for multiple forms of mass media, such as television, radio, digital, out-of-home, and print (*COVID-19 Information on HHS's Public Education Campaign*, 2022). I assume that this alternative would be active for a two-year period, at which point there after the alternative would no longer receive funding. Based on the funding figures from the New York City and HHS case studies, I estimate baseline costs of this alternative to be roughly $260 million (USD 2023). Though the duration for this alternative is only two years, I project direct costs of this alternative over a five-year period, to include actions such as community outreach, media and information and literacy programming, and disinformation pre-bunking messaging. In total, I estimate the direct cost of funding a disinformation awareness campaign and MIL education initiative to be roughly $503.8 million[1].

Effectiveness – High (3)

The effectiveness of public awareness and disinformation education campaigns, to include MIL programs as well as disinformation pre-bunking methods, receives a high score. Encouraging results are seen in a number of studies. Dame Adjin-Tettey (2022) saw over 70% of study participants that received MIL training accurately identify inauthentic news stories, compared to 46% for participants who received no training. A meta-analysis of MIL interventions found statistically significant positive effects on

[1] See Appendix B for cost calculations

information consumption where the intervention increased measured outcomes such as "media knowledge, criticism, perceived realism, influence, behavioral beliefs, self-efficacy, and behavior" by 0.37 standard deviations (Jeong et al., 2012). Jeong, Cho, and Hwang's (2012) meta-analysis demonstrates how MIL trainings can be effective tools to combat the mal effects disinformation renders on the knowledge, beliefs, and attitudes of individuals exposed to disinformation. Another study conducted by Jones-Jang, Mortensen, and Liu (2021) saw a 11.9 percentage point increase ($p<0.001$) in respondent's ability to correctly identify fake news stories for every additional correct answer respondents scored on a five-question baseline information literacy assessment.

In addition to raising both general disinformation threat awareness and MIL interventions, other pre-bunking strategies based in inoculation theory have shown promising mitigatory effects (Banas & Rains, 2010; Ecker et al., 2022; Kavanagh & Rich, 2018; Matthews et al., 2021; van der Linden, 2022). Coupled with a body of empirical research, real world cases of pre-bunking and media literacy initiatives that have been heralded for their success in countering disinformation include media literacy education in Europe, such as Ukraine's efforts against Russian disinformation and Sweden's youth education system (Treyger et al., 2022a). Still, the long-term effectiveness of proactive-leaning policies and interventions to address disinformation deserve additional study as questions linger about not only overall efficacy, but also treatment effects targeting large audiences (Ecker et al., 2022; Matthews et al., 2021).

Political Feasibility – High (3)

Raising public awareness and education, engaging the community, and stressing the importance of media and information literacy ranks high on the scale of political feasibility. At the national and state levels, there is political precedent for the government to advance public education campaigns related to mis- and disinformation as seen in the HHS vaccination campaign to respond to COVID-19. Media and information literacy advocacy organizations, such as Media Literacy Now, have also seen success in passing legislation at the state level supporting MIL programming in K-12 school curriculums (Ali, 2022). Among key political leaders and relevant government officials, President Joe Biden signed the Consolidated Appropriations Act, 2023 into law on December 29th, 2022 which tripled federal funding in civics education and included $50 million in additional funding for building media and digital literacy skills for students (*FACT SHEET*, 2023).

Practical Feasibility – Medium (2)

The practical feasibility of a public education/awareness campaign coupled with media and information literacy education programming is medium. Significant coordination would be required across the federal, state, and local government levels to execute the proposed policy alternative. While it is possible one agency or department at the federal level could lead the effort, robust execution of the alternative would necessitate interagency coordination and leadership from at least three key cabinet departments, specifically the GEC, DHS, and the Department of Education (ED). Legal and practical

concerns regarding the propagandizing or even the appearance of propagandizing of the American public could arise with DOS involvement as well.

Even with the aforementioned practical challenges, government has demonstrated the institutional capacity to perform public education initiatives, such as the COVID-19 vaccine education initiative from HHS or the "Click It or Ticket" and "Drive Sober or Get Pulled Over" mobilizations from the National Highway Traffic Safety Administration (NHTSA). Public information sharing and education initiatives are also inherently scalable by virtue of targeting mass audiences. Even MIL education has shown the ability to be implemented at scale in K-12 schools though targeting other specific populations who may be more susceptible to online disinformation, such as senior citizens, could prove to be a greater practical challenge.

Alternative 2: Rapid Response Teams

Cost - $12.3 million

To operationalize the cost of establishing disinformation rapid response teams, I relied on budget data from Canada and the international Group of Seven (G7). The G7 is an unofficial group of countries that include Canada, France, Germany, Italy, Japan, the United Kingdom (UK), and the United States. The European Union also serves as a member of the G7. Launched in 2018, the G7 uses a Rapid Response Mechanism (RRM) to share information, identify, and coordinate response efforts to disinformation and foreign threats to democracy (Canada, 2021). Canada leads the G7 RRM through RRM Canada, and in March 2022 Canadian Prime Minister Justin Trudeau announced additional funding for RRM Canada totaling $13.4 million over the next five years (*Disinformation and Russia's War of Aggression against Ukraine*, 2022). To estimate the direct costs for this alternative, I first calculated the annual costs of the additional funding for RRM Canada by dividing the total funding allocation over the number of years the funding would be distributed, giving me an annual cost of $2.68 million ($13.4 million in funding divided by five years). Converting this appropriated funding into 2023 USD, I estimate baseline costs to be roughly $2.75 million. After projecting costs of the alternative over a five-year period, I estimate total direct costs of establishing disinformation rapid response teams to be roughly $12,300,000[2].

Effectiveness – Medium (2)

Evidence suggests that disinformation monitoring and rapid response capabilities are moderately effective at addressing inaccurate knowledge and beliefs that individuals hold after they have been exposed to and influenced by disinformation. Clayton et al. (2020) found a statistically significant ($p < 0.01$) yet small (Cohen's $d = 0.08$) effect size where general warnings reduced perceived belief accuracy in false headlines by 0.08 standard deviations. The same study found medium effect sizes for reducing belief in false headlines through "Disputed" and "Rated False" tags, decreasing false beliefs by 0.26 and 0.38 standard deviations, respectively (Clayton et al., 2020). Another study found that accuracy flags attached to social media posts moderately increased the correct identification of real and fake news among participants ranging between 0.65-0.80 standard deviations ($d = 0.651$-0.800) (Gaozhao, 2021). Fact-checking was also seen to increase the correct identification of political misinformation by 0.29 standard deviations (Cohen's $d = 0.29$, $p < 0.005$) (Walter et al., 2020).

Other studies have also shown positive effects in reducing the continued influence effects of mis- and disinformation by flagging content, employing fact-checking tags, and providing a causal alternative narrative when issuing a correction statement (Ecker et al., 2022; Kan et al., 2021; Matthews et al., 2021; van der Linden, 2022). One such study was conducted by Ecker, Lewandowsky, and Tang (2010), which found that showing a specific warning about the continued influence effect and the provision of an

[2] See Appendix B for cost calculations

alternative narrative for retracted information reduced study participants' average number of references to misinformation by 2.94 references (a 58.1% decrease) and 2.84 references (a 56.1% decrease), respectively, relative to study participants who were not shown any form of a retraction. When participants were exposed to both the specific warning and alternative narrative treatments, the average number of participants' references to misinformation decreased by 3.60 references (a 77.6% decrease) relative to individuals who were not exposed to any form of retraction.

Monitoring and rapid response capabilities have also been hailed as successes at countering disinformation in places such as the UK and EU (R. S. Cohen et al., 2021; Vilmer, 2021). Yet, the long-term effectiveness and staying power of such measures remains questionable at best when looking to impact the beliefs and knowledge of individuals at a group level, especially given the nuanced-process needed to successfully debunk the beliefs and knowledge rooted in disinformation messaging (Ecker et al., 2022; Johnson & Seifert, 1994; Lewandowsky et al., 2012).

Political Feasibility – Medium (2)

Creating rapid response teams focused on addressing disinformation targeting the U.S. justice system and its institutions scores a medium on the political feasibility criterion scale. While rapid response teams may coordinate and share information for situational awareness with court systems and relevant personnel within the U.S. justice system, much of their monitoring, identification, and response operations could be independent of official court systems. Acting separately from the U.S. justice system, such as by sharing information with the public via a third-party website, could offer critical political coverage to judges, prosecutors, and other court personnel directly employed by and affiliated with the justice system. Organizations, such as the ABA and NCSC, have already signaled a willingness for undertaking such an effort. An example of this willingness is evidenced by the ABA issuing disinformation rapid response guidelines and best practices (*Rapid Response to Fake News, Misleading Statements, and Unjust Criticism of the Judiciary*, 2018).

Still, the political climate for instituting rapid response teams could vary significantly on a state-to-state basis. As of March 30th 2023, 11 states have divided governments, 22 states have Republican trifectas, and 17 states have Democratic trifectas whereby a trifecta consists of a single political party holding the governorship, majority in the state house, and majority in the state senate (*State Government Trifectas*, n.d.). The enactment and operational execution of disinformation rapid response teams could prove to be easier or harder in states with trifecta governments depending on the political leanings of that state and the party in power at the time. Regardless of the specific politics of a state, court systems will likely continue to be concerned with and look to maintain both their credibility and legitimacy by remaining impartial and not engaging in partisan debates outside of their institutional scope.

Practical Feasibility – High (3)

The practicality of standing up a rapid response team with disinformation monitoring, information sharing, and coordinated response capabilities scores high. National organizations, like the ABA and the NCSC, have provided best practices guidance to support the formation of rapid response teams in court systems and localities across the country, boosting an overall ability to scale (*Rapid Response to Fake News, Misleading Statements, and Unjust Criticism of the Judiciary*, 2018). While some legal barriers may exist on a case-by-case basis, that has not stopped certain states from moving forward in creating rapid response teams focused on combatting disinformation. This has been the case in Arizona, where upon the recommendation from the Arizona Supreme Court's TFCD, the "Arizona Judges Association (AJA) agreed to establish a Rapid Response Team for Arizona's judiciary" (*Disinformation Task Force Concluding Report*, 2022).

Alternative 3: Expanding Public-Private Partnerships

Cost - $59.6 million

In quantifying the expansion of public-private partnerships, I used cost estimates based on funding appropriated by the European Union's Commission. The European Digital Media Observatory (EDMO), an initiative started in 2020 that combats disinformation by supporting independent academic researchers and fact-checkers in collaboration with social media companies and other relevant stakeholders, received 11 million Euros (roughly $11,957,550 USD) in May 2021 in grant funding to establish eight regional EDMO centers across different Member States (*Funded Projects in the Fight against Disinformation*, n.d.). As part of the larger EU "Code of Practice on Disinformation" which serves as an example of governments partnering with private social media and tech companies, I use the EDMO initiative to estimate the direct costs of a similar partnership in the United States. Converting EDMO funding into 2023 USD, I estimate baseline costs to be roughly $13,275,000. After projecting costs of the alternative over a five-year period, I estimate total costs of expanding public-private partnerships to be roughly $59,600,000[3].

Effectiveness – Low (1)

The effectiveness of expanding public-private partnerships scores low. One aspect of expanding public-private partnerships between social media companies and the federal government would be standardizing fact-checking practices across different companies. As has been previously discussed, there is some empirical evidence showing that fact-checking and the flagging of false content online can reduce beliefs in mis- and disinformation and improve the accurate identification of authentic news, ranging in effect size from 0.29-0.80 standard deviations (Clayton et al., 2020; Gaozhao, 2021; Walter et al., 2020). However, other research has found no evidence that the warning and fact-checking practices employed by some social media platforms significantly reduces the circulation of false content compared to the absence of any warning message (Ross et al., 2018).

Coupled with the mixed empirical support of self-regulated fact-checking, anecdotal evidence from other countries supporting the effectiveness of expanding partnerships to combat disinformation is weak. Outcomes to date of such partnerships have been poor as disinformation continues to spread and threaten institutions of justice. This poor effectiveness is seen in the case of Twitter, which did not follow through on the commitments it made to advance fact-checking efforts in the EU's Disinformation Code of Conduct (Lomas, 2023). Social media companies are also profit-seeking entities with a global presence, characteristics which could make them apprehensive about expanding their relationship with the government for fear of damaging their user base and adversely impacting their bottom line (Cohen et al. 2021). This apprehension, informed in part by profit-seeking motivations, limits the overall effectiveness this alternative has

[3] See Appendix B for cost calculations

at countering the beliefs, knowledge, and positions disinformation looks to advance in the online users of social media platforms.

Political Feasibility – Low (1)

The political feasibility of expanding partnerships between government and private social media companies to address the threat to legitimacy disinformation creates for the justice system is mixed. While the EU has successfully implemented policies that establish operational infrastructure which secures and expands these partnerships (*Funded Projects in the Fight against Disinformation*, n.d.; *The 2022 Code of Practice on Disinformation | Shaping Europe's Digital Future*, 2023), similar domestic efforts to counter online disinformation have experienced blowback. This was the case during the spring of 2022 when DHS announced that its new, three-week old Disinformation Governance Board would be put on pause following public and political criticism (Lorenz, 2022). Though the Board was created only to examine best practices at countering the effects of disinformation and had no regulatory authority over the speech and content on social media platforms, it drew the political ire from a host of critics with many referencing George Orwell's "1984" by dubbing the Board the "Ministry of Truth." Based on the timeline of these events, the present willingness of the Biden administration to support this alternative looks bleak.

Moreover, many social media and big tech companies have had a history of strained relations with Congress and political leaders. The federal government has brought antitrust lawsuits against Google and Meta while Congress has discussed legislation that would impose reforms on the tech industry, though that legislation and the possibility of near-term reforms was effectively killed in December 2022 thanks to big tech lobbying efforts (*FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate*, 2021; *Justice Department Sues Google for Monopolizing Digital Advertising Technologies*, 2023; Kelly, 2022). Still, these events signal how the overall relationship between policymakers and social media companies may be more adversarial than amicable. Republican lawmakers, having expressed concerns about online censorship and holding a majority in the House of Representatives, introduced a bill in January 2023 that makes some tech policy experts worried about the prospects the federal government partnering with companies to effectively counter Russian disinformation online (*GOP Bill to Protect Speech on Social Media May Gag Officials*, 2023).

Practical Feasibility – Medium (2)

The practical feasibility of any strategy expanding a partnership between government and social media companies is medium. Though many tech and social media companies are well-resourced and generate billions of dollars in revenue annually, they have also slashed significant amounts of their workforce, exacerbating their inability to combat disinformation on their platforms (Conger et al., 2022; Myers & Grant, 2023). These layoffs could signal an unwillingness or inability to expand any relationship between these private companies and the government, as establishing such a partnership would likely require additional staff to manage greater coordination efforts. Evidenced in the

case of the EU, scaling public-private partnerships is possible yet also presents significant coordination challenges. Expanding public-private partnerships to include greater collaboration with the federal government and other technology firms could further strain coordination, while the resources and institutional capacity would likely vary from company to company.

Evaluation Matrix

Evaluation Criteria	Policy Alternatives		
	Public Awareness Campaign and MIL Education	**Rapid Response Teams**	**Expanding Public-Private Partnerships**
Direct Cost	$503,800,000	$12,300,000	$59,600,000
Effectiveness	High	Medium	Low
Political Feasibility	High	Medium	Low
Practical Feasibility	Medium	High	Medium
Overall Feasibility	Medium to High	Medium to High	Low to Medium

Recommendation

Based on its score against the evaluative criteria, I recommend the implementation of a network of state-level disinformation rapid response teams that focus on monitoring, publicly identifying, and responding to disinformation that specifically targets the U.S. justice system. While the effectiveness and political feasibility of rapid response teams are only moderate, the direct cost of establishing and operating rapid response teams is $12.3 million, which is significantly lower than the direct costs of the other two policy alternatives ($503.8 million and $59.6 million, respectively).

Next Steps: Implementation Consideration

Establishing disinformation rapid response teams with monitoring, information sharing, and public communication and warning capabilities will only be successful in addressing the problem if implemented effectively. For the recommendation to have the greatest chance at success, I highlight the main stakeholders involved in the implementation process, each of their perspectives on the recommended policy, and potential challenges that could arise during the implementation stage.

Stakeholders: Roles and Perspectives

Non-Governmental Legal Organizations

Non-governmental legal organizations are primary stakeholders in the implementation of disinformation rapid response teams, as they would take an operational role in the initial implementation and long-term execution of rapid response teams. Many of these organizations exist at the national scale, such as the ABA, the NCSC, and ABOTA. In addition, university law schools, private attorneys, retired judges, and media outlets are stakeholders who would likely be heavily involved in the operations of disinformation rapid response teams as well as the advocacy component for their initial establishment. Several of these non-governmental legal organizations, such as the ABA and NCSC, already recognize the threat disinformation poses to the justice system and the need to take measures to combat it (American Bar Association Standing Committee on the American Judicial System, 2018; NCSC, 2022). With this inherent awareness of the disinformation threat, it is reasonable to believe that this stakeholder group would be supportive of implementing disinformation rapid response teams.

Federal Government

The federal government would be a key stakeholder in facilitating the implementation of disinformation rapid response teams, namely the GEC, DOJ, DHS, and the federal court system. GEC, DHS, and DOJ would likely assume major support roles in a rapid response team's operations. This support role could include the provision of disinformation subject matter expertise as well as technological and logistical assets to secure effective coordination and information sharing capabilities. The federal government may also be involved in funding efforts for disinformation rapid response teams. While the operational function of teams would be led by private, non-governmental, non-profit, and/or academic legal organizations, the federal government could offer tax breaks, subsidies, and/or grants to these organizations to incentivize and facilitate the establishment and capabilities of rapid response teams. Under the current Biden administration, there is a recognition of the threat disinformation poses to both the justice system and widely held democratic values. However, the administration could be hesitant to support any implementation efforts following the botched rollout and subsequent dissolution of DHS' Disinformation Governance Board back in the spring of 2022 (Lorenz, 2022).

State Government

State governments are another set of stakeholders that would be critical to the successful implementation of disinformation rapid response teams. State court systems, legislatures, and governors would hold multiple roles in the implementation process. These roles could include serving in an advisory capacity as to how rapid response teams function, being a source for possible funding, and acting as a gatekeeper in coordination efforts. The gatekeeping coordination role is characterized by state governments' ability to strengthen or weaken the ability of rapid response teams to operate, as governors and state legislatures could be in favor of or against the recommended policy based on the politics of their respective states. As the recommended policy aims to establish multiple rapid response teams at the state level, taking this approach based on recommendations found in a 2022 report by the Arizona Supreme Court's TFCD, policymakers in state government, such as governors and state legislators, would hold significant sway over the potency of rapid response teams due to the operational coordination and communication required in their relationship with state court systems. Thus, support for implementing the recommendation could vary greatly on a state-by-state basis.

Challenges and Mitigation Strategies

Challenges

A major challenge my client, CSIS, faces in facilitating the implementation of the recommendation is making the problem salient to leaders and policymakers. While many leaders within government and civil society are aware of disinformation and how it threatens democratic values, from concerns about election interference to Russia's invasion of Ukraine to the January 6th Capitol insurrection, there is a lack of awareness and an inherent understanding of how disinformation targets the justice system and the subsequent harm that is caused. Another challenge to implementing disinformation rapid response teams is securing both adequate funding and the political buy-in to get the policy up and running. Putting in place the framework to even have the opportunity to fund and execute the recommendation is likely to require significant energy, as issuing funding avenues such as tax incentives or grants for the policy could be a long and complicated process.

Mitigation Methods

The following list includes courses of action that CSIS has already and continues to implement in addition to other next steps that could be taken to move the recommended policy forward:

1. Continue to directly engage in workshops, roundtables, and discussions with non-governmental legal organizations about disinformation targeting the justice system.
2. Educate and raise the issue with policymakers at the national and state levels to promote greater awareness about the disinformation threat to the justice system and how the recommended policy would serve to neutralize the threat.
3. Continue to directly engage and raise the issue with the public, as making the issue salient to them could help raise the issue with leaders and policymakers. Educating the public about the issue directly could also serve to make the public more resilient to disinformation targeting the justice system as a whole.

Conclusion

Outcomes to date from the harmful and manipulative effects of Russian disinformation targeting the U.S. justice system have already shown how public confidence and trust in democratic institutions can be undermined, consequentially weakening overall faith in government (Spaulding et al., 2019). As Russian aggression in pursuit of its foreign policy objectives increasingly strains international security and heightens tensions with the U.S., defending intuitions of justice is an ever more vital measure to safeguard national security.

This report identified and evaluated three evidence-based policy alternatives to address the vulnerabilities of the U.S. justice system's perceived legitimacy and integrity to attacks from Russian disinformation: a public awareness campaign including MIL education, disinformation rapid response teams, and expanding public-private partnerships. While a threat awareness campaign paired with MIL education programming holds promise as an effective response to the malign beliefs and knowledge disinformation looks to sow, the associated high direct cost of executing the policy may pose too large of an obstacle to enact. Disinformation rapid response teams, however, ranked as the best policy alternative when viewed across the entire catalog of evaluative criteria, including direct cost, effectiveness, political feasibility, and practical feasibility. Moving forward, CSIS could continue to facilitate discussions with appropriate decision-makers about the threat Russian disinformation poses to the justice system and American democratic institutions as a whole, while also stressing how disinformation rapid response units could work to diminish the threat. In any next steps CSIS takes, it is essential that the consequences of inaction be explicitly highlighted for policymakers, as doing so could galvanize their support for an effective policy response.

Appendix A: Evaluative Criteria Rubric

Cost: This criterion will consider the direct costs associated with a proposed alternative. U.S. dollars (USD) is the unit of measurement used to evaluate costs. Cost estimate data for a proposed alternative is drawn from various sources, including case studies from foreign countries and international organizations.

Effectiveness: This criterion will consider the degree to which a proposed alternative alters two primary outcomes of interest: beliefs and knowledge. Belief outcomes capture any change in an individual's opinions, convictions, or worldview (Shapiro, 2021). Survey data from the body of literature studying disinformation and misinformation is used to measure beliefs. Survey instrument measures include asking respondents questions about their opinions on a host of issues, such as perceived credibility. Knowledge outcomes capture any change in an individual's understanding or awareness of a topic (Shapiro, 2021). Just as belief outcomes, survey data from the literature on disinformation is leveraged to measure knowledge. These surveys include questions focused on examining the memory and recall ability of participants.

Wherever possible, I apply Cohen's standards of magnitude for effect size in this criterion to inform the effectiveness evaluation of each alternative in impacting belief and knowledge outcomes. Those standards state that small effect size: d =0.10-0.20 standard deviations; medium effect size: d =0.21-0.50 standard deviations; large effect size: d =0.51-0.80 standard deviations. In addition, in the absence of empirical data regarding beliefs and knowledge outcomes, the criterion will leverage case studies examining outcomes where similar policy interventions to the proposed alternative were implemented.

Feasibility: This criterion will consider the viability of implementing a proposed alternative, as any alternative that lacks the capacity to be implemented offers little utility in addressing the problem. The criterion has two separate components that are independently evaluated: political feasibility and practical feasibility. Each component is equally weighted and defined below.

1. **Political Feasibility**: Political feasibility considers the degree of political support a proposed alternative would garner relative to the current political climate. Political feasibility is informed by factors such as support from relevant elected and/or public officials, the number of agents required to approve the implementation of a proposed alternative, and public sentiment. The criterion is measured on a linear 1-3 scale (low = 1, medium = 2, high = 3).
2. **Practical Feasibility**: Practical feasibility considers factors such as the legal barriers, scalability, and organizational/institutional capacity necessary to implement a proposed alternative. The fewer barriers, greater ability to scale, and more resources an organization has to implement an alternative, the higher that alternative's practical feasibility. Just as the political feasibility criterion, practical feasibility is measured on a liner 1-3 scale (low = 1, medium = 2, high = 3).

	High (3)	Medium (2)	Low (1)
Effectiveness	-Is the alternative supported by strong empirical evidence? Yes -Have other countries implemented & hailed the alternative as a success? Yes	-Is the alternative supported by strong empirical evidence? Somewhat -Have other countries implemented & hailed the alternative as a success? Yes	-Is the alternative supported by strong empirical evidence? No -Have other countries implemented & hailed the alternative as a success? No
Political Feasibility	-Key political leaders, government officials, and relevant stakeholders would likely support the policy alternative -The alternative would likely have few political detractors -There is strong political precedent for the alternative	-Key political leaders, government officials, and relevant stakeholders would likely be somewhat supportive of the policy alternative -The alternative would likely have a consequential amount of political detractors -There is some political precedent for the alternative	-Key political leaders, government officials, and relevant stakeholders would likely not support the policy alternative -The alternative would likely have a large amount of political detractors -There is little to no political precedent for the alternative
Practical Feasibility	-The alternative is scalable -One organization/department/entity would be primarily responsible for implementing, coordinating, and operating the alternative -The organization/department/entity primarily responsible for the alternative is well-resourced	-The alternative is somewhat scalable -Two organizations/departments/entities would be primarily responsible for implementing, coordinating, and operating the alternative -The organizations/departments/entities primarily responsible for the alternative have some resources	-The alternative is difficult to scale -Three or more organizations/departments/entities would be primarily responsible for implementing, coordinating, and operating the alternative -The organizations/departments/entities primarily responsible for the alternative have few resources

Appendix B: Projecting Direct Costs

I project out the total direct costs associated with each policy alternative to compare each alternative against one another with respect to the direct cost criterion. For each year of implementation over a five-year period, I calculate the total direct cost of each alternative based on budgets and fiscal appropriations of similar programs and policy interventions from foreign nations as well as from domestic case studies. First I convert all direct cost figures into 2023 USD. I then use forecasts from the Office of Management and Budget's (OMB) to discount future costs (*OMB Circular No. A-94 Appendix C*, 2022). OMB forecasts the 5-year nominal discount rate at 1.6%, which I use to discount future costs. Calculations for each policy alternative are listed below.

Alternative 1: Public Awareness Campaign & MIL Education Discounted Costs (1.6%) $PV=FV/(1+r)^n$						
2023	**2024**	**2025**	**2026**	**2027**	**2028**	**Total**
$260,000,000	$255,905,512	$247,908,960	$0	$0	$0	$503,814,472

Alternative 2: Rapid Response Teams Discounted Costs (1.6%) $PV=FV/(1+r)^n$						
2023	**2024**	**2025**	**2026**	**2027**	**2028**	**Total**
$2,750,000	$2,706,693	$2,622,114	$2,500,175	$2,346,365	$2,167,340	$12,342,688

Alternative 3: Expanding Public-Private Partnerships Discounted Costs (1.6%) $PV=FV/(1+r)^n$						
2023	**2024**	**2025**	**2026**	**2027**	**2028**	**Total**
$13,275,000	$13,065,945	$12,657,659	$12,069,028	$11,326,545	$10,462,342	$59,581,519

Appendix C: Acronyms List

ABA	**American Bar Association**
ABOTA	**American Board of Trial Advocates**
AJA	**Arizona Judges Association**
CISA	**Cybersecurity and Infrastructure Security Agency**
CRS	**Community Relations Service**
CSIS	**Center for Strategic and International Studies**
DHS	**Department of Homeland Security**
DOHM	**Department of Health and Mental Hygiene**
DOJ	**Department of Justice**
DOS	**Department of State**
ED	**Department of Education**
EDMO	**European Digital Media Observatory**
EU	**European Union**
G7	**Group of Seven**
GEC	**Global Engagement Center**
HHS	**Department of Health and Human Services**
IRA	**Internet Research Agency**
MIL	**Media and Information Literacy**
NCSC	**National Center for State Courts**
NHTSA	**National Highway Traffic Safety Administration**
NJC	**National Judicial College**
NSD	**National Security Division**
NSF	**National Science Foundation**
PIO	**Public Information Officer**
RRM	**Rapid Response Mechanism**
TFCD	**Task Force on Countering Disinformation**
UK	**United Kingdom**
U.S.	**United States**
USD	**United States Dollars**
USG	**United States Government**

References

$2.25 million in National Science Foundation funding will support Center for an Informed Public's rapid-response research of mis- and disinformation. (2021, August 15). Center for an Informed Public. https://www.cip.uw.edu/2021/08/15/national-science-foundation-uw-cip-misinformation-rapid-response-research/

About CSIS | Center for Strategic and International Studies. (n.d.). Retrieved April 5, 2023, from https://www.csis.org/about

About Us—Global Engagement Center. (n.d.). *United States Department of State*. Retrieved February 8, 2023, from https://www.state.gov/about-us-global-engagement-center-2/

Ali, S. (2022, March 18). Media literacy is desperately needed in classrooms around the country, advocates say [Text]. *The Hill*. https://thehill.com/changing-america/enrichment/education/598795-media-literacy-is-desperately-needed-in-classrooms/

American Bar Association Standing Committee on the American Judicial System. (2018). *Rapid Response to Fake News, Misleading Statements, and Unjust Criticism of the Judiciary*. https://www.americanbar.org/content/dam/aba/administrative/american-judicial-system/2018-rapid-response-to-fake-news.pdf

Atske, S. (2021, April 7). Social Media Use in 2021. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Banas, J. A., & Rains, S. A. (2010). A Meta-Analysis of Research on Inoculation Theory. *Communication Monographs*, *77*(3), 281–311. https://doi.org/10.1080/03637751003758193

Bowen, A. S., & Welt, C. (2021). *Russia: Foreign Policy and U.S. Relations* (p. 64). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R46761

Brashier, N. M., Pennycook, G., Berinsky, A. J., & Rand, D. G. (2021). Timing matters when correcting fake news. *Proceedings of the National Academy of Sciences*, *118*(5), e2020043118. https://doi.org/10.1073/pnas.2020043118

Brenan, M. (2021, October 7). *Americans' Trust in Media Dips to Second Lowest on Record*. https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx

Canada, G. A. (2021, February 2). *Rapid Response Mechanism Canada: Global Affairs Canada*. GAC. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng#a2

Clayton, K., Blair, S., Busam, J. A., Forstner, S., Glance, J., Green, G., Kawata, A., Kovvuri, A., Martin, J., Morgan, E., Sandhu, M., Sang, R., Scholz-Bright, R., Welch, A. T., Wolff, A. G., Zhou, A., & Nyhan, B. (2020). Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-Check Tags in Reducing Belief in False Stories on Social Media. *Political Behavior*, *42*(4), 1073–1095. https://doi.org/10.1007/s11109-019-09533-0

Cohen, J. (2013). *Statistical Power Analysis for the Behavioral Sciences*. Academic Press.

Cohen, R. S., Beauchamp-Mustafaga, N., Cheravitch, J., Demus, A., Harold, S. W., Hornung, J. W., Jun, J., Schwille, M., Treyger, E., & Vest, N. (2021). *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR4373z1.html

Compton, J., Jackson, B., & Dimmock, J. A. (2016). Persuading Others to Avoid Persuasion: Inoculation Theory and Resistant Health Attitudes. *Frontiers in Psychology*, *7*. https://doi.org/10.3389/fpsyg.2016.00122

Conger, K., Mac, R., & Isaac, M. (2022, November 4). Confusion and Frustration Reign as Elon Musk Cuts Half of Twitter's Staff. *The New York Times*. https://www.nytimes.com/2022/11/04/technology/elon-musk-twitter-layoffs.html

COVID-19 Disinformation Toolkit | CISA. (n.d.). [Official Website of the United States government]. Retrieved February 6, 2023, from https://www.cisa.gov/covid-19-disinformation-toolkit

COVID-19 Information on HHS's Public Education Campaign (p. 27). (2022). United States Government Accountability Office. https://www.gao.gov/assets/720/719781.pdf

COVID-19 Vaccine Misinformation and Disinformation Costs. (n.d.). Johns Hopkins Center for Health Security. Retrieved February 20, 2023, from https://www.centerforhealthsecurity.org/our-work/publications/covid-19-vaccine-misinformation-and-disinformation-costs-an-estimated-50-to-300-million-each-da

Dame Adjin-Tettey, T. (2022). Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. *Cogent Arts & Humanities*, *9*(1), 2037229. https://doi.org/10.1080/23311983.2022.2037229

Defending Democratic Institutions | International Security Program | CSIS. (n.d.). Retrieved April 5, 2023, from https://www.csis.org/programs/international-security-program/defending-democratic-institutions

Derleth, J. (2020). Russian New Generation Warfare Deterring and Winning at the Tactical Level. *Army University Press*, 13.

Dillingham, L. L., & Ivanov, B. (2016). Using Postinoculation Talk to Strengthen Generated Resistance. *Communication Research Reports*, *33*(4), 295–302. https://doi.org/10.1080/08824096.2016.1224161

Disinformation and Russia's war of aggression against Ukraine. (2022, November 3). OECD. https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/

Disinformation Task Force Concluding Report (p. 45). (2022). State of Arizona Supreme Court. https://www.azcourts.gov/Portals/74/DisinformationTaskForceConcludingReport2022_1.pdf

Ecker, U. K. H., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., Kendeou, P., Vraga, E. K., & Amazeen, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology*, *1*(1), Article 1. https://doi.org/10.1038/s44159-021-00006-y

Ecker, U. K. H., Lewandowsky, S., & Tang, D. T. W. (2010). Explicit warnings reduce but do not eliminate the continued influence of misinformation. *Memory & Cognition*, *38*(8), 1087–1100. https://doi.org/10.3758/MC.38.8.1087

FACT SHEET: The Biden-Harris Administration's Abiding Commitment to Democratic Renewal at Home and Abroad. (2023, March 29). The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-the-biden-harris-administrations-abiding-commitment-to-democratic-renewal-at-home-and-abroad/

Freelon, D., & Lokot, T. (2020). Russian Twitter disinformation campaigns reach across the American political spectrum. *Harvard Kennedy School Misinformation Review*, *1*(1). https://doi.org/10.37016/mr-2020-003

FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate. (2021, August 19). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush-competition-after-string-failed

Funded projects in the fight against disinformation. (n.d.). Retrieved February 23, 2023, from https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/funded-projects-fight-against-disinformation_en

Gaozhao, D. (2021). Flagging fake news on social media: An experimental study of media consumers' identification of fake news. *Government Information Quarterly*, *38*(3), 101591. https://doi.org/10.1016/j.giq.2021.101591

GEC Special Report: Russia's Pillars of Disinformation and Propaganda (p. 77). (2020). [Special Report]. U.S. Department of State. https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/

Global Engagement Center. (n.d.). United States Department of State. Retrieved September 25, 2022, from https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/

Goldstein, M. J. (2021). *Disinformation & The Justice System*. Thomson Reuters. https://www.judges.org/wp-content/uploads/2022/05/Disinformation-and-the-Justice-System.pdf

GOP bill to protect speech on social media may gag officials. (2023, January 24). Roll Call. https://www.rollcall.com/2023/01/24/gop-bill-to-protect-speech-on-social-media-may-gag-officials/

Harding, J. (2015, November 15). Russian News, Russian Proxy News Sites And Conspiracy Theory Sites. *To Inform Is to Influence*. https://toinformistoinfluence.wordpress.com/2015/11/15/russian-news-and-russian-proxy-news-sites/

Jeong, S.-H., Cho, H., & Hwang, Y. (2012). Media Literacy Interventions: A Meta-Analytic Review. *The Journal of Communication*, *62*(3), 454–472. https://doi.org/10.1111/j.1460-2466.2012.01643.x

Johnson, H. M., & Seifert, C. M. (1994). Sources of the continued influence effect: When misinformation in memory affects later inferences. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, *20*, 1420–1436. https://doi.org/10.1037/0278-7393.20.6.1420

Jones, J. (2022, July 5). *Confidence in U.S. Institutions Down; Average at New Low*. https://news.gallup.com/poll/394283/confidence-institutions-down-average-new-low.aspx

Jones-Jang, S. M., Mortensen, T., & Liu, J. (2021). Does Media Literacy Help Identification of Fake News? Information Literacy Helps, but Other Literacies Don't. *American Behavioral Scientist*, *65*(2), 371–388. https://doi.org/10.1177/0002764219869406

Justice Department Sues Google for Monopolizing Digital Advertising Technologies. (2023, January 24). https://www.justice.gov/opa/pr/justice-department-sues-google-monopolizing-digital-advertising-technologies

Kan, I. P., Pizzonia, K. L., Drummey, A. B., & Mikkelsen, E. J. V. (2021). Exploring factors that mitigate the continued influence of misinformation. *Cognitive Research: Principles and Implications*, *6*(1), 76. https://doi.org/10.1186/s41235-021-00335-9

Kavanagh, J., & Rich, M. D. (2018). *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2314.html

Kelly, M. (2022, December 20). *Congress blew its last chance to curb Big Tech's power*. The Verge. https://www.theverge.com/2022/12/20/23517807/big-tech-antitrust-bills-congress-omnibus

Kremlin-Funded Mediat: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem (p. 33). (2022). U.S. Department of State Global Engagement Center. https://www.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem/

Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychological Science in the Public Interest*, *13*(3), 106–131. https://doi.org/10.1177/1529100612451018

Lomas, N. (2023, February 9). Musk's Twitter gets "yellow card" for missing data in EU disinformation report. *TechCrunch*. https://techcrunch.com/2023/02/09/elon-musk-twitter-eu-disinformation-code-report/

Lorenz, T. (2022, May 18). How the Biden administration let right-wing attacks derail its disinformation efforts. *Washington Post*. https://www.washingtonpost.com/technology/2022/05/18/disinformation-board-dhs-nina-jankowicz/

Lucas, E., Lamond, J., & Zakem, V. (2022). *Owning the Conversation: Assessing Responses to Russian and Chinese Information Operations Around COVID-19*. Center for European Policy Analysis. https://cepa.mystagingwebsite.com/comprehensive-reports/owning-the-conversation-assessing-responses-to-russian-and-chinese-information-operations-around-covid-19/

Lynch, S. N., & Lynch, S. N. (2022, February 15). U.S. judges faced over 4,500 threats in 2021 amid rising extremism -official. *Reuters*. https://www.reuters.com/world/us/us-judges-faced-over-4500-threats-2021-amid-rising-extremism-official-2022-02-14/

Maertens, R., Roozenbeek, J., Basol, M., & van der Linden, S. (2021). Long-term effectiveness of inoculation against misinformation: Three longitudinal experiments. *Journal of Experimental Psychology: Applied*, *27*, 1–16. https://doi.org/10.1037/xap0000315

Matthews, M., Demus, A., Treyger, E., Posard, M. N., Reininger, H., & Paul, C. (2021). *Understanding and Defending Against Russia's Malign and Subversive Information Efforts in Europe*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR3160.html

Myers, S. L., & Grant, N. (2023, February 14). Combating Disinformation Wanes at Social Media Giants. *The New York Times*. https://www.nytimes.com/2023/02/14/technology/disinformation-moderation-social-media.html

NCSC. (2022, October 9). *Disinformation and the courts*. https://www.ncsc.org/consulting-and-research/areas-of-expertise/communications,-civics-and-disinformation/disinformation/for-courts

Oliker, O. (2015, January 15). Russia's new military doctrine: Same as the old doctrine, mostly. *Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2015/01/15/russias-new-military-doctrine-same-as-the-old-doctrine-mostly/

OMB Circular No. A-94 Appendix C. (2022). Office of Management and Budget. https://www.whitehouse.gov/wp-content/uploads/2022/05/Appendix-C.pdf

Panditharatne, M., Edlin, R., Smith, R., Chen, K., & Urbani, S. (2022, August 2). *Information Gaps and Misinformation in the 2022 Elections | Brennan Center for Justice*. https://www.brennancenter.org/our-work/research-reports/information-gaps-and-misinformation-2022-elections

Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehoods" Propaganda Model*. RAND Corporation. https://www.rand.org/pubs/perspectives/PE198.html

Rani, P., Jain, V., Shokeen, J., & Balyan, A. (2022). Blockchain-based rumor detection approach for COVID-19. *Journal of Ambient Intelligence and Humanized Computing*, 1–15. https://doi.org/10.1007/s12652-022-03900-2

Rapid Response to Fake News, Misleading Statements, and Unjust Criticism of the Judiciary (p. 12). (2018). American Bar Association. https://www.americanbar.org/content/dam/aba/administrative/american-judicial-system/2018-rapid-response-to-fake-news.pdf

Ross, B., Jung, A.-K., Heisel, J., & Stieglitz, S. (2018). *Fake News on Social Media: The (In)Effectiveness of Warning Messages*.

Russian disinformation distorts American and European democracy. (2018, February 22). *The Economist*. https://www.economist.com/briefing/2018/02/22/russian-disinformation-distorts-american-and-european-democracy

Sah, P., Vilches, T. N., Moghadas, S. M., Pandey, A., Gondi, S., Schneider, E. C., Singer, J., Chokshi, D. A., & Galvani, A. P. (2022). Return on Investment of the COVID-19 Vaccination Campaign in New York City. *JAMA Network Open*, *5*(11), e2243127. https://doi.org/10.1001/jamanetworkopen.2022.43127

Salmon, F. (2021, January 21). Trust in media hits new crisis low. *Axios*. https://www.axios.com/2021/01/21/media-trust-crisis

Scheufele, D. A., & Krause, N. M. (2019). Science audiences, misinformation, and fake news. *Proceedings of the National Academy of Sciences of the United States of America*, *116*(16), 7662–7669. https://doi.org/10.1073/pnas.1805871115

Shapiro, J. B., Elonnai Hickok, Laura Courchesne, Isra Thange, Jacob N. (2021, June 28). *Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824

Social Media Fact Sheet. (2021, April 7). Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/fact-sheet/social-media/

Spaulding, S., Nair, D., & Nelson, A. (2019). *Beyond the Ballot HOW THE KREMLIN WORKS TO UNDERMINE THE U.S. JUSTICE SYSTEM* (p. 54). Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190430_RussiaUSJusticeSystem_v3_WEB_FULL.pdf

Spaulding, S., & Rishikof, H. (2018, September 17). *How Putin Works to Weaken Faith in the Rule of Law and Our Justice System*. Lawfare. https://www.lawfareblog.com/how-putin-works-weaken-faith-rule-law-and-our-justice-system

State government trifectas. (n.d.). Ballotpedia. Retrieved March 30, 2023, from https://ballotpedia.org/State_government_trifectas

Suciu, P. (2021, June 24). *Americans Spent On Average More Than 1,300 Hours On Social Media Last Year*. Forbes. https://www.forbes.com/sites/petersuciu/2021/06/24/americans-spent-more-than-1300-hours-on-social-media/

The 2022 Code of Practice on Disinformation | Shaping Europe's digital future. (2023, February 9). https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

The Economic Cost of Bad Actors on the Internet (p. 17). (2019). CHEQ. https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdfhttps://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf

THE GLOBAL ENGAGEMENT CENTER: LEADING THE UNITED STATES GOVERNMENT'S FIGHT AGAINST GLOBAL DISINFORMATION THREAT. (2020). U.S. Government Publishing Office. https://www.govinfo.gov/content/pkg/CHRG-116shrg41862/html/CHRG-116shrg41862.htm

Theohary, C. A. (2018). *Information Warfare: Issues for Congress* (p. 16). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45142

Thorson, E. (2016). Belief Echoes: The Persistent Effects of Corrected Misinformation. *Political Communication*, *33*(3), 460–480. https://doi.org/10.1080/10584609.2015.1102187

Tida, V. S., Hsu, D. S., & Hei, D. X. (2022). *A Unified Training Process for Fake News Detection based on Fine-Tuned BERT Model* (arXiv:2202.01907). arXiv. https://doi.org/10.48550/arXiv.2202.01907

Treyger, E., Cheravitch, J., & Cohen, R. S. (2022b). *Russian Disinformation Efforts on Social Media*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR4373z2.html

Turper, S., & Aarts, K. (2017). Political Trust and Sophistication: Taking Measurement Seriously. *Social Indicators Research*, *130*(1), 415–434. https://doi.org/10.1007/s11205-015-1182-4

van der Linden, S. (2022). Misinformation: Susceptibility, spread, and interventions to immunize the public. *Nature Medicine*, *28*(3), Article 3. https://doi.org/10.1038/s41591-022-01713-6

Vilmer, J.-B. J. (2021). *Effective state practices against disinformation: Four country case studies*. 32.

Vladimir Putin's Historical Disinformation. (2022, May 6). United States Department of State. https://www.state.gov/disarming-disinformation/vladimir-putins-historical-disinformation/

Wagner, T. P. (2014). Using Root Cause Analysis in Public Policy Pedagogy. *Journal of Public Affairs Education*, *20*(3), 429–440. https://doi.org/10.1080/15236803.2014.12001797

Walter, N., Cohen, J., Holbert, R. L., & Morag, Y. (2020). Fact-Checking: A Meta-Analysis of What Works and for Whom. *Political Communication*, *37*(3), 350–375. https://doi.org/10.1080/10584609.2019.1668894

235 McCormick Road
P.O. Box 400893
Charlottesville, VA 22904-4893
434-924-0812 | www.batten.virginia.edu