COUNTERING DISINFORMATION IN THE UNITED STATES

CSC White Paper #6

UNITED STATES OF AMERICA
CYBERSPACE SOLARIUM COMMISSION

CO-CHAIRMEN
Senator Angus King (I-Maine)
Representative Mike Gallagher (R-Wisconsin)

DECEMBER 2021

CONTENTS

EXECUTIVE SUMMARY

In its March 2020 Final Report, the U.S. Cyberspace Solarium Commission called on the U.S. government to promote digital literacy, civic education, and public awareness in order to build societal resilience to foreign malign cyber-enabled information operations. As the scourge of disinformation swept across the globe and expanded its scope beyond elections, the Commission decided to conduct a deeper examination of cyber-enabled disinformation and propose steps that the United States could take to begin building greater resilience to disinformation, particularly from foreign actors. While many facets of the Commission's original strategy of "layered cyber deterrence" can be applied in the context of combating cyber-enabled disinformation, further action is needed from policymakers and lawmakers to enable the United States to better prevent, withstand, and respond to disinformation.

In the context of disinformation, the United States faces stark foreign threats from nation-state adversaries, including most prominently China, Russia, and Iran. These governments leverage intelligence operators, foreign media outlets, businesses, and expatriates to spread disinformation in an effort to weaken confidence in key institutions, sow civil discord, and undermine U.S. pillars and instruments of power. These malign foreign actors leverage traditional and social media to create and disseminate disinformation to pursue broader geopolitical goals, amplify acute crises, and exploit societal fissures.

Yet even despite this clear and defined threat, the federal government must tread carefully when wading into the fraught world of disinformation. Its role must be defined narrowly and in a way that recognizes the inherent limitations on how a democratic government should influence the information space, including but not limited to the guardrails enshrined in the First Amendment. Further complicating this role is the notion that education—commonly ascribed a high level of importance for building societal resilience to disinformation—is a policy area largely within the purview of states and not the federal government. Still other areas, like the training of journalists, introduce concerns about the appearance of inappropriate government influence and are better addressed by other stakeholders. The federal government must therefore focus on building key partnerships with relevant stakeholders around the country and enabling these partners to do the right thing.

This is not to imply that the federal government is not taking and cannot take important steps to counter disinformation. Indeed, elements of the State Department, the Federal Bureau of Investigation, the Department of Homeland Security, the Department of Justice, the Department of the Treasury, and the Office of the Director of National Intelligence currently engage in programming designed to protect the American people from the adverse effects of disinformation. Congress too has recognized the need for action, and members have introduced dozens of bills that seek to confront the challenge of disinformation. The federal government, working with key partners, must chart a path forward that brings coherence to national efforts by prioritizing those threats that are most harmful and then taking steps to address them.

This white paper sets out seven recommendations to both reduce the prevalence of disinformation in the information ecosystem and build greater individual and societal resilience to disinformation and malign foreign influence:

- Recommendation 1: Congress should establish a Civic Education Task Force, enable greater access to civic education resources, and raise public awareness about foreign disinformation.

- Recommendation 2: Congress should ensure material support to nongovernmental disinformation researchers

- Recommendation 3: Congress should fund the Department of Justice to provide grants to nonprofit centers seeking to identify, expose, and explain malign foreign influence campaigns to the American public

- Recommendation 4: Congress should create a capability within the Department of Homeland Security to actively monitor foreign disinformation

- Recommendation 5: Congress should create a grants program at the Department of Homeland Security designed to equip state and local governments with the personnel and resources necessary to identify foreign disinformation campaigns and incorporate countermeasures into public communications strategies

- Recommendation 6: Congress should reform the Foreign Agents Registration Act and direct the Federal Communications Commission to introduce new regulations in order to improve media ownership transparency in the United States

- Recommendation 7: Congress should grant a federal entity the authority to publish and enforce transparency guidelines for social media platforms

This white paper is the result of research and deliberation by Commission staff and commissioners. It seeks to explain how the Commission's original recommendations and strategy of layered cyber deterrence can be applied in the context of disinformation and contributes a set of comprehensive policy recommendations that lay a firm foundation upon which the United States, working with allies and partners, can build to combat disinformation and protect our most valuable democratic institutions.

INTRODUCTION – WHY DISINFORMATION IS A CYBERSPACE ISSUE

The United States Cyberspace Solarium Commission (CSC) was created by Congress in the National Defense Authorization Act (NDAA) for Fiscal Year 2019 to answer two fundamental questions: What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy? While disinformation is considered by some an issue largely separate from cybersecurity or network security,[1] the Commission addressed disinformation in the very narrow context of elections in its final report in March 2020. As the COVID-19 pandemic swept across the globe, the Commission revisited the issue, this time in the context of disinformation about the pandemic itself, noting, "Our adversaries' disinformation campaigns focused on the pandemic illustrate that disinformation activities can reach far beyond the political and electoral contexts with which Americans are best acquainted."[2]

Over the course of the intervening months, the Commission received demand signals from constituents within Congress and the executive branch to treat the topic of disinformation and potential policy recommendations more extensively. The Commission has previously been reluctant to delve deeply into the topic of disinformation for two reasons.

First, disinformation as a policy issue, unlike many aspects of cybersecurity policy, has been marked by a strong partisan divide. Researchers have identified an association between strong partisanship and vulnerability to misinformation;[3] more than two-thirds of U.S. citizens believe that Republicans and Democrats disagree about basic facts;[4] and while U.S. citizens in both major parties agree that disinformation is a problem, they disagree about who is responsible for it and what ways to tackle the threat are appropriate.[5] Although this partisan divide persists today, it is the sense of the members of the Commission that there is room to reach some agreement on core issues.

Second, as noted above, disinformation is seen by many as an issue largely separate from cybersecurity and cyber policy in the United States. While the Commission understands this view, continuing to bifurcate these issues has become untenable. From a strategic perspective, the United States and its policymakers do themselves a disservice by continuing to differentiate between the two when our adversaries do not.[6]

In order to craft a comprehensive strategy to defend the United States from cyberattacks of significant consequence, policymakers must account for the entire arsenal employed by adversaries to cause harm in cyberspace, including information. It is also important to take a more operational or risk management perspective: disinformation campaigns waged against the United States by foreign actors are often carried out by many of the same threat actors as are active in cyberspace and are often the consequence of cyberattacks.

For these reasons, members of the Commission believe that elements of the topic of disinformation are within our mandate. This white paper is the result of deep research, interviews with experts, and deliberations by the Commission. It seeks to explain how the Commission's proposed strategy of layered cyber deterrence applies to combating disinformation and contributes a set of policy recommendations to better position the United States to prevent, counter, and withstand the consequences of disinformation launched against it.

SECTION I: THE COMMISSION'S STRATEGIC APPROACH AND RECOMMENDATIONS AS THEY PERTAIN TO DISINFORMATION

Layered cyber deterrence, the strategic approach proposed by the U.S. Cyberspace Solarium Commission in its March 2020 Final Report, combines a number of traditional deterrence mechanisms and extends them beyond the government to develop a whole-of-nation approach. By shaping behavior, denying benefits, and imposing costs on adversaries, the approach seeks to reduce the frequency and severity of cyberattacks of significant consequence. In combating disinformation, the United States should adopt the same approach, and several CSC recommendations from the March 2020 Final Report pertain to disinformation.

In the March Report, for example, the CSC made recommendations aimed at ensuring robust U.S. capability to respond to cyberattacks using cyber and non-cyber tools, including through defend forward operations and law enforcement action. These same recommendations can be applied in the disinformation context. The executive branch should clarify the concept of "defend forward" and its applicability in preventing and responding to adversary disinformation campaigns, and Congress should strengthen non-military response tools. Further, the CSC recommended that "the U.S. government develop a multitiered signaling strategy aimed at altering adversaries' decision calculus and addressing risks of escalation."[7] In addition to signaling about cyber, such a strategy should seek to communicate capability and resolve, delineate thresholds of behavior that will trigger a response, and convey intent behind U.S. actions in the information space.

The report also emphasized the importance of resilience in managing cyber risks. Such management includes strengthening public resilience against the pernicious messaging promoted by disinformation. The complete elimination of disinformation, like the elimination of all traditional cyber threats, is not a realistic outcome. Understanding the malicious actor's or nation's strategic objectives and finding ways to deny those objectives, regardless of the means being used, provides a sustainable and agile approach that can mitigate harm even as the adversary changes tactics. This was the thinking behind the CSC recommendation on teaching digital literacy and reinvigorating civic education to counter the erosion of trust in democracy and democratic institutions that is so often the goal of disinformation.

Still other recommendations from the CSC's subsequent white papers may also apply to combating disinformation in the United States. For example, in its May 2020 "Cybersecurity Lessons from the Pandemic" white paper, the CSC recommended that the Office of the Director of National Intelligence create the Social Media Data and Threat Analysis Center (DTAC) to act as a convening and sponsoring authority for social media companies and other third parties that will cooperate in collating social media data to facilitate analysis of foreign threat networks, analysis of foreign influence operations, and information sharing.[8] While policymakers are still debating the institutional home of the DTAC, this center should be created and staffed to carry out its mandate. Further, in the same white paper, the CSC advocated for improving the capacity of nongovernmental organizations (NGOs)to identify and counter foreign disinformation and influence campaigns. This recommendation remains as compelling as before.

To date, however, the CSC has neither fully treated nor proposed a suite of complementary recommendations aimed directly at the challenge of combating disinformation. Before doing so, it is critical to grasp the intricacies of the United States' information environment, including the threats and soft targets, and to understand existing government efforts aimed at addressing disinformation in the U.S. information ecosystem.

SECTION II: THE UNITED STATES' INFORMATION ECOSYSTEM

The question of how best to describe harms in the information environment has been the subject of scholarly disagreement,[9] and terms like "disinformation," "misinformation," "malinformation," "information operations," "influence operations," "information warfare," and "malign influence," to name just a few, are all used in various contexts by experts. It is important not to use them interchangeably, because they describe specific phenomena, each of which requires a different policy solution. The CSC focuses on the problems of disinformation, or "false information that is deliberately created or disseminated with the express purpose to cause harm," and misinformation, or "information that is false, but not intended to cause harm."[10] Both disinformation and misinformation are tools used in the broader context of "influence operations," which the RAND Corporation defines as "the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent."[11] In many cases, the information activities of adversaries involve explicitly false information; in others, such activities rely on misleading information, taken out of context or presented in an inflammatory manner, and employ a kernel of truth to conceal the otherwise malign actions. The CSC concentrates on disinformation and misinformation as elements of broader influence operations because this focus creates a more narrow and appropriate scope for federal action.

Adversaries of the United States, operating out of both foreign and domestic locations, conduct operations to spread both disinformation and misinformation in the United States in an effort to undermine public confidence in core democratic institutions, sow discord and polarize the population, and place the health and safety of Americans at risk. While the elections of the past decade have newly drawn attention to the issue of disinformation in the United States, the malady is not confined to the context of elections. Adversaries of the United States have taken advantage of dis- and misinformation campaigns to weaken public trust in all our institutions, undermine public health (both during and before the COVID-19 pandemic), and create friction or confusion during U.S. military and diplomatic engagements abroad.

A. THREATS

Adversaries of the United States leverage influence operations and disinformation campaigns in an effort to degrade confidence in key institutions, sow civil discord, and undermine U.S. pillars and instruments of power. Although most states and, increasingly, many non-state actors deploy information as a means of influence over other states, foreign adversaries using disinformation campaigns to undermine U.S. national security interests include Russia, China, and Iran. In taking such actions, each of these countries seeks not only to undermine U.S. objectives but also to pursue their own diplomatic, military, and economic objectives. In addition, within our own borders, domestic political actors wittingly and unwittingly wield or amplify disinformation in furtherance of political goals.

1. Russia

Russia employs a mix of methods to muddy the information environment in pursuit both of long-term objectives, including undermining the instruments of U.S. power and trust in democratic institutions, and of short-term objectives, such as cultivating civil tension over specific issues like race relations or influencing elections.[12] In the United States, Russia draws on print, online, television, radio, and social media to construct divisive narratives and spread mistruths. The three primary

Russian intelligence agencies—the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), and the Main Directorate of the General Staff of the Armed Forces (GRU)—each conduct information operations that impact the U.S. information environment.[13] In addition, the Russian government distributes propaganda and disinformation through official channels, like those issuing official government statements; through state-funded entities, including foreign-facing media like Russia Today; and through proxy sources, including Russia-aligned outlets with global reach and English-language outlets such as the Strategic Culture Foundation, Global Research, New Eastern Outlook, and Geopolitica.ru.[14] Many of these proxy outlets obfuscate their Russian state connections by employing American or other Western authors and academics. Peace Data, for example, was a Russian site that paid real journalists to produce content in order to lend it legitimacy even as it was producing false and misleading content.[15]

In furtherance of their information objectives, Russian influence operators have become adept at leveraging social media networks and fringe websites to infiltrate communities of interest in the United States using false personas, to stand up campaigns to undermine institutions, and to amplify protests or broader civil discord.[16] Russia also routinely conducts cyber operations in order to steal sensitive private information and leak it to the press.[17] While such information is not necessarily false, it does saturate the media ecosystem and distract public attention from other issues, thereby shaping public opinion. All in all, Russia's disinformation efforts have focused on volume, leading RAND Corporation analysts to coin the expression "firehose of falsehoods" to describe how Russian disinformation is inundating the media environment.[18]

2. China

China, like Russia, is involved in a long-term strategic influence operation aimed at shifting values around the world and positioning itself as a new ideologue.[19] During the COVID-19 pandemic, China began operating an increasingly comprehensive international influence apparatus, using both overt and subtle tactics in an attempt to erode U.S. and partner countries' influence. These efforts have included propaganda related to the coronavirus and to the United States' handling of the outbreak.[20] In some of the most egregious cases, they have also involved attempts to stop European government sources from reporting on its COVID-19 misinformation efforts.[21] However, its disinformation campaigns are not confined to the issue of COVID-19; they have extended to areas such as the state's treatment of Uighurs in Xinjiang, technology competition, the U.S.-China relationship, and pro-democracy protests in Hong Kong.[22] These campaigns have been fueled by the aggressive use of social media (the same social media to which China denies its citizens access) as Chinese government officials promote narratives favorable to the Chinese Communist Party (CCP).[23]

Overtly, a new class of vocal and vitriolic diplomats, colloquially referred to as "Wolf Warriors," often take the lead in propagating conspiracy theories via official Twitter accounts, interviews, and press releases.[24] In addition to the push by individual high-level diplomats, a dedicated community of state-paid internet users, often called the "50 cent party," echoes these talking points amid praise of the CCP across the internet.[25] At a more subtle and subversive level, China's COVID-era escalation of its disinformation campaign against the United States continued during the 2020 presidential election with the use of fake Twitter accounts to push out misleading videos, which were then echoed by Chinese bots. Most notably, Chinese-linked accounts published footage purporting to show a man burning ballots marked for Donald Trump, which then received upward of 1.2 million views.[26] Such tactics are similar to those pioneered and deployed by Russia in the 2016 election campaign and point toward the CCP's increasingly active and hostile disinformation posture.

China's Propaganda Efforts in Xinjiang

In 2017, growing attention began to focus on China's repression and forced detention of Uighurs, members of an ethnically Muslim minority who live primarily in China's western Xinjian province, under the guise of antiterrorism efforts.[27] Since then, journalists have obtained piles of evidence documenting the mass detentions.[28] Estimates in 2019 were that more than 1 million Uighurs were being held in internment camps;[29] and even as leaders claimed that the program was "winding down," the construction of new camps has continued.[30]

As international criticism has mounted,[31] China has engaged in a global propaganda campaign to deflect attention from its practices by criticizing the human rights practices of other countries,[32] co-opting ordinary citizens into its efforts to reshape the narrative,[33] and amplifying social media content in favor of its version of events.[34]

In one notable action detailed by the *New York Times*, Chinese authorities have facilitated the production of hundreds of videos from supposedly ordinary citizens extolling the freedom they enjoy in Xinjiang.[35] These videos are uploaded to Chinese platforms like Pomegranate Cloud or Douyin and then recirculated on YouTube and Twitter in an apparently coordinated campaign. Some of the Twitter accounts pushing these videos have been suspended for violating the site's policies regarding spam and platform manipulation.

3. Iran

Iran is a smaller but still powerful player focused on gaining regional influence, controlling its citizens' access to information, and preserving its national image.[36] Researchers who have studied and tracked Iran's efforts have focused on the use of sockpuppets (false online identities) to launder information and push distorted narratives, especially with respect to Israel and Saudi Arabia.[37] Iran's propaganda and disinformation efforts heavily feature a sense of exaggerated moral authority. For example, following the U.S. government's killing of Qassem Soleimani in early 2020, Iran mounted a propaganda campaign that promised vengeance or retaliation.[38] Pervasive Iranian disinformation efforts continue to address the Israeli-Palestinian conflict and the possibility that the United States might reenter the Joint Comprehensive Plan of Action (JCPOA).[39] A recently declassified report by the Director of National Intelligence evaluated with high confidence that Iran launched a multipronged disinformation campaign connected to the 2020 elections that was aimed at denigrating then-President Trump and sowing discord domestically.[40] In one of its more brazen efforts, Iranian actors sent threatening emails to voters in Florida in an attempt to make them change their votes. While Iran's efforts became more frequent, its tactics remained technically unsophisticated. The report concludes that in their efforts, Iranian actors relied mainly on low-cost cyber tools supplemented with information operations (including spearfishing campaigns). Further analysis indicated that multiple actors within the Iranian government took part in the disinformation campaign, suggesting that Ayatollah Khomeini prioritized a "whole-of-government" approach.[41] Much like both Russia and China, Iran is seeking in these campaigns to subvert trust in democratic institutions and sow discord between political parties around the world.

B. VECTORS

In the context of disinformation, vectors represent the ways in which information spreads. In the United States, any discussion of disinformation necessarily involves social media platforms.[42] This attention is largely merited as, according to Pew Research Center, 53 percent of American adults read the news on social media.[43] In Q2 of 2020, Facebook alone removed more than 7 million posts that contained fake news and labeled 98 million posts with "warning notices about coronavirus misinformation."[44] in the following quarter, sites producing provably false content generated 1.8 billion interactions on

Facebook.[45] However, while social media plays an important role in amplifying disinformation and is a primary vector through which disinformation spreads, disinformation existed long before the advent of social media. Online sources—including websites (like the Russian proxy websites) with links to or run by foreign intelligence agencies—print media, television, radio, and in-person networks all contribute heavily to the creation and dissemination of disinformation in the U.S. media ecosystem.

How Disinformation Spreads across Platforms

While researchers have called for greater access to social media data so that they may fully understand the spread of disinformation across platforms including Facebook, Twitter, and YouTube,[46] some studies and anecdotal evidence have already demonstrated how disinformation appears on fringe platforms, migrates to more mainstream social media platforms, and finally is picked up by traditional media sources in newspapers and television.[47]

For example, fringe platforms, social media, and mainstream media have all been involved in the spread of conspiracy theories about COVID-19 and the safety of COVID-19 vaccines.[48] Fringe platforms like 4chan and 8kun showed a spike in conversations about the Pfizer COVID-19 vaccine in November 2019, following the company's announcement of positive results from its Phase III clinical trials. Many of these conversations relied on links to known conspiracy sites and affiliate sites, which are used to launder information,[49] as well as to Russian state media and sites known to push pro-Kremlin narratives. These links then spread to Facebook and Twitter, in some cases generating thousands of interactions.

The proliferation of misinformation about COVID-19 vaccines has generated sustained media attention, as mainstream news outlets attempt to assure Americans of the vaccines' safety and efficacy.[50] Even though much of this coverage focuses on debunking conspiracy theories and misinformation, experts describe it as a win for the perpetrators, whose main goal is amplification.[51]

C. DISINFORMATION AS A TOOL TO AMPLIFY ACUTE CRISES AND EXPLOIT SOCIETAL FISSURES

Disinformation threatens to broadly undermine public confidence in the United States government's ability to govern effectively. Different threat actors leverage different topics to sow discord, create confusion, and damage trust in the U.S. government, society, and economy. While adversaries often find and focus on targets of opportunity, many campaigns share the goal of weakening faith in democracy and seek to exploit public anxiety regarding race relations, economic inequality, and public health. No system of government is perfect, and adversaries exploit citizens' frustration with democratic outcomes and the sometimes slow and messy process by which democracies fashion their policies. By contrast, autocratic adversaries like Russia and China—unimpeded by basic protections for citizens' rights or by processes that involve hashing out disagreements among competing interests—are able to place stricter controls on information, silence opposition, and, if need be, respond with great flexibility to populist impulses swayed by disinformation. These advantages do not make autocracy preferable to democracy: the features that make democracies uniquely vulnerable to disinformation perpetrated by adversary nations are precisely the features worth protecting. But the need to operate within the constraints of democracy does introduce unique challenges for countries seeking to compete with comparatively untrammeled adversaries.

Disinformation can represent a sharp tool with which key adversaries can create or exacerbate acute crises related to health, safety, and security. China, for example, has relied heavily on disinformation to push narratives throughout the COVID-19

pandemic, focusing efforts on undermining democratic responses to the pandemic, disputing the origins of the virus, and causing widespread panic by amplifying false messages.[52] However, the targeting of public health issues in the United States is not limited to the context of COVID-19. For the better part of two decades, the Russian state has sought to undermine the American public's confidence in vaccinations. This effort has involved using Russian content polluters to sow discord about vaccines, which researchers suggest may damage public health because "normalizing these debates may lead the public to question long-standing scientific consensus regarding vaccine efficacy."[53] Some have therefore concluded that the Russian government believes in "the anti-vaxxer/pro-vaccination debate as one of the fissures within American society that it can exploit."[54] The intent of this misinformation is to undermine the American public's faith in U.S. institutions, a decline that would in turn weaken the United States and our ability to counter the Kremlin.

In addition, other wedge issues, such as race relations, have provided fertile ground for disinformation campaigns to take root. As Americans took to the streets in June 2020 to protest police brutality and racism in the United States, foreign media outlets in Russia and China "piggybacked onto hashtags linked to George Floyd . . . to push divisive messages and criticize Washington's handling of the unfolding crisis."[55] This tactic prompted the Department of Homeland Security to issue an intelligence bulletin to law enforcement agencies containing the assessment that foreign adversaries had sought to capitalize domestic political tensions for geopolitical goals.[56] Perpetrators of disinformation sought to impersonate black Americans by using fake social media profiles and to leverage content focused on Black Lives Matter protests to express support and criticism of both presidential candidates, Biden and Trump.[57] Though foreign actors latched on to the recent protests to push disinformation, these tactics were not new: according to a Senate report after Russia's interference in the 2016 presidential election, black Americans were the largest target of Russian social media disinformation.[58] Domestic racial tensions are just one arena in which foreign adversaries have used existing divisions or ongoing events to sow chaos.

Further, Russia is among the adversaries that have actively manufactured and spread disinformation to reduce the influence of the United States and its allies in the international arena.[59] Over the past decade in particular, Russia has used disinformation to undermine various arms control norms and institutions. An ongoing disinformation campaign orchestrated by the Kremlin seeks to conceal the illegal use of chemical weapons by itself and its allies. In 2018, Russia violated the Chemical Weapons Convention by using a nerve agent in an attempt to assassinate Sergei Skripal, a former Russian spy, in the United Kingdom.[60] Subsequently, the Russian state is alleged to have employed its disinformation machine to deflect its responsibility for the attempted murder of the Russian opposition leader Alexei Navalny via a Novichok-class nerve agent.[61] After German doctors confirmed that a nerve agent was responsible for Navalny's illness, Russia immediately denounced the accusations, calling the announcement a "smear campaign" against Russian authorities.[62]

Finally, military service members and veterans are especially ripe targets for disinformation, and adversaries like Russia have focused their efforts on these individuals. A 2019 report by Vietnam Veterans of America "documented persistent, pervasive, and coordinated online targeting of American servicemembers, veterans, and their families by foreign entities who seek to disrupt American democracy."[63] An earlier report from 2017 detailed Russian attempts to hack, spearphish, and target service members and veterans with disinformation, relying on tactics such as "posing as attractive young women to gather intelligence" and distributing propaganda on social media after friending service members on Facebook.[64] The same report suggests that Russia uses platforms targeted at veterans in order to push pro-Russia propaganda and partner with other Russian front organizations.[65] In addition to targeting service members and veterans, adversaries have made the U.S. military the object of disinformation campaigns and conspiracy theories: during the pandemic, Russian and Chinese news sources sought to stoke fear regarding martial law and the National Guard's role in response to the pandemic.[66] Other disinformation episodes, seeking to undermine NATO exercises in Europe, have spread allegations that members of the U.S. Army killed a Lithuanian boy.[67] Some of this targeting may be enabled by online platforms like Facebook that continue to allow

advertisements to target military personnel.[68] In 2019, at a hearing held by the House Veterans' Affairs Committee on online disinformation targeting veterans, one disinformation expert testified that veterans are targeted because they "are highly respected members of society who positively influence their country and their community."[69] The goal of these particular foreign disinformation campaigns is the same as that of others: "to further amplify and exploit the existing frustrations in the veteran community" and, in so doing, "to wear away veterans' faith in the U.S. system."[70]

SECTION III: THE FEDERAL GOVERNMENT'S ROLE

Subsequent sections of this white paper discuss current federal efforts under way to deal with the problem of disinformation and propose specific recommendations for the federal government, but it is important to note at the outset the limitations and unique circumstances of the U.S. federal government as it seeks to address disinformation. Protected by the First Amendment, freedom from government interference in speech and access information is a fundamental American value. In addition, the United States is home to many of the world's leading media and social media companies, which own and operate much of the information environment not only domestically but also internationally. These realities pose unique challenges and opportunities for the United States, including the need to determine the appropriate scope of the role of the federal government and to manage collaboration between the federal government and the private owners and operators of the information space.

A. RECOGNIZE FEDERAL LIMITATIONS

While the federal government has a diverse set of tools that can be applied to the challenge, not all of these tools are appropriate and should be applied. For example, with few exceptions, in developing policy that involves the content of speech the federal government is constrained by the First Amendment.[71] The protections that amendment affords are the lifeblood of democracy, and censorship is inimical to the values that underpin a healthy, functioning information environment. Furthermore, censorship erodes U.S. strength abroad by undermining American support not just for freedom of speech and the press internationally but for an open information environment more broadly. Platforms themselves can moderate the content that appears online, but the federal government can intervene only in extremely limited circumstances, subject to strict legal scrutiny.[72]

Another constraint arises from the Tenth Amendment, which reserves to states the right to make policy in areas not delegated to the federal government by the Constitution. As a result, state and local governments have had primacy over areas like education, providing greater local control over what is taught in schools. The federal government can and does exercise influence over education policy through instruments like funding.[73] However, it should not dictate the content of the school curricula.[74]

In other areas, federal action must avoid the appearance of inappropriate government influence over parts of society that are better served by other stakeholders. The sphere of journalism, for example, was investigated by the CSC in the course of researching and writing this white paper. The CSC considered recommendations that might bolster the ability of rigorous independent journalism to counter disinformation. Not only can journalists play an important role in providing credible, authoritative information to the American public,[75] but they are also themselves targets of disinformation.[76] However, the

CSC abandoned the idea, in part because of concerns that the government might appear to be supporting certain media outlets or propagandizing. Moreover, the media plays a crucial role in holding the government accountable (as at least two-thirds of both Republicans and Democrats agree),[77] and any government support that compromises the ability or perceived ability of independent journalists to provide neutral and unbiased reporting on its activities does more harm than good. When it comes to countering disinformation by bolstering journalism, other stakeholders from civil society or private industry might be better positioned than the federal government to take the lead.

B. BUILD PARTNERSHIPS

In keeping with the importance of establishing an appropriate scope for the federal government's role, partners will be essential to any national disinformation strategy. Private industry; state and local governments; and civil society are all crucial partners for several reasons. Private industry, such as social media companies and traditional media companies, own and operate the core infrastructure through which disinformation flows. States and localities are critical not only because they are perceived as more trustworthy or reliable sources of information than is the federal government,[78] but also because they have jurisdiction over infrastructure or policies—including education policy and elections administration—that are central to the disinformation challenge. Civil society organizations can provide credible research on the disinformation campaigns spreading across platforms and can work to hold accountable both the private sector and government through rigorous journalism and fact-checking.[79] Each of these actors brings resources and expertise to bear on the problem, and they expand the set of tools available for countering disinformation.

These partners can also help expand access to authoritative information and counter false or misleading narratives with greater credibility than the federal government. A Pew Research Center survey from the fall of 2020 reported that the proportion of Americans who trust the federal government, which has not passed 30 percent since 2007, has fallen to just 20 percent.[80] And while the percentage of Americans who trust their state governments has also declined since the early 2000s, it has consistently remained above its lowest point (51 percent, in 2010).[81] In 2018, fully 63 percent of Americans expressed trust in state government and 72 percent expressed trust in local government.[82] These statistics show that state and local agencies can better serve as trusted sources for information than their federal counterparts and are, therefore, essential partners in the effort to provide authoritative information regarding topics such as election integrity or COVID-19.

SECTION IV: CURRENT FEDERAL GOVERNMENT EFFORTS

Over the past several years, the federal government has made strides in addressing the problem of online disinformation, but important structural barriers to effective progress in this area remain. Efforts suffer from a lack of strategy, coordination, and prioritization. Leadership on the issue is lacking, in part because there is no clearly designated department, agency, or office around which all efforts should coalesce. Much as in the case of cybersecurity, multiple departments and agencies have resources and expertise that come to bear on the problem of disinformation. And much as in the case of cybersecurity before the creation of the Office of the National Cyber Director, no single federal entity has the oversight, authority, or resources to assume ownership for countering disinformation; nor is it clear that a single federal entity should assume

such ownership. As a result, federal executive agencies including the Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) have created a number of centers, task forces, and initiatives meant to deal with the problem of foreign influence and disinformation.

Still, there is cause for optimism regarding the federal appetite to address cyber-enabled disinformation, particularly when it emanates from foreign entities. Every National Defense Authorization Act since 2017 has made reference to the subject and authorized federal action.[83] Both the executive branch and Congress have demonstrated a willingness to respond to foreign interference campaigns, particularly those affecting elections. The Department of Justice has indicted operatives tied to disinformation campaigns—notably, those associated with the Russian Internet Research Agency.[84] The Department of the Treasury has also sanctioned Russian and Iranian entities and individuals engaged in election interference,[85] using the powers granted by Executive Orders 13757 and 13848.[86]

A. FEDERAL AGENCY INITIATIVES

On the heels of the news that Russia had attempted to interfere in the 2016 presidential election, the Trump administration's 2017 National Security Strategy included a section on "information statecraft" under the heading "Preserve Peace Through Strength."[87] Naming Russia and China among the adversaries seeking to "weaponize information" for strategic gain and control the information available to their own publics, the document recognized that "U.S. efforts to counter the exploitation of information by rivals have been tepid and fragmented. U.S. efforts have lacked a sustained focus and have been hampered by the lack of properly trained professionals."[88] Similarly, although the Biden administration has not yet released its National Security Strategy, the interim guidance published in March 2021 identified mis- and disinformation as among the tools used by adversary nations to "exploit perceived weaknesses and sow division within and among free nations, erode existing international rules, and promote alternative models of authoritarian governance."[89]

Reflecting the emphasis of current and former administrations on countering the threat of cyber-enabled disinformation, federal initiatives have sought to increase information-sharing among federal agencies and between the government and the general public on ongoing disinformation campaigns. They have also focused on public diplomacy and providing technical assistance to foreign publics that may be affected by disinformation campaigns. The following list is not exhaustive but rather provides an overview of some of the most notable ongoing efforts by federal departments and agencies.

1. Rumor Control

In the run-up to the 2020 election, the Cybersecurity and Infrastructure Security Agency (CISA) launched rumorcontrol.gov to prebunk—that is, to preemptively warn of and expose[90]—disinformation related to the integrity of the election by providing authoritative information on election protection efforts.[91] Some federal messaging campaigns have focused on reaching specific audiences—CISA partnered with the Vietnam Veterans of America on the #Protect2020 campaign, similarly designed to combat disinformation regarding the integrity of the election.[92] In an attempt to replicate the success of CISA's website, other federal departments and agencies have created similar sites to address coronavirus-related disinformation. The Federal Emergency Management Agency and Department of Defense, for example, both have "rumor control" sites to help "distinguish between rumors and facts regarding the response to the Coronavirus (COVID-19) pandemic," and both aggregate links to the pages of other federal departments and agencies involved in coronavirus response.[93] The Department of Justice's website also provides information on how to spot coronavirus-related scams, as does the Federal Trade Commission's.[94] States, too, have followed this model. Maryland, for example, established its own rumor control sites

addressing the election and the coronavirus, as did Colorado.[95] And in April 2021, a bipartisan group of 11 secretaries of state asked the Department of Homeland Security to expand its efforts to push back against foreign disinformation campaigns and thanked the department for its efforts during the 2020 election.[96]

2. Mis-, Dis-, and Malinformation Team

The Countering Foreign Influence Task Force, established in 2018 within CISA's predecessor agency, became in 2021 the Mis-, Dis-, and Malinformation (MDM) team, which "work[s] in close coordination with interagency and private sector partners, social media companies, academia, and international partners on a variety of projects to build resilience against malicious information activities."[97] In its approach to public awareness, the MDM team focuses on three stakeholder groups: (1) subject-matter experts who enhance understanding of the threat, (2) "trusted voices" that can help amplify messaging, and (3) the general public for which the team's informational materials are designed. The team also seeks to "rout[e] disinformation concerns to appropriate social media platforms and law enforcement." These public awareness efforts have included two graphic novels focused on identifying disinformation.[98]

3. Foreign Influence Task Force

In the fall of 2017 the FBI established its own task force, focused on the threat of foreign influence, which is intended to coordinate the Counterintelligence, Cyber, Criminal, and Counterterrorism Divisions.[99] Its work deals largely with investigations, information-sharing, and private-sector partnerships.

4. Protected Voices Initiative

The FBI, DHS, and ODNI work together to run the Protected Voices Initiative and provide resources to political campaigns desiring to protect themselves from cyberattacks and foreign influence campaigns.[100] Their videos and materials have covered topics such as business email compromise, cloud-based services, ransomware, multi-factor authentication, and social media literacy. They provide tips and best practices for "protect[ing] your digital devices, social media accounts, and private information from cyberattacks."[101]

5. Global Engagement Center (GEC)

The Global Engagement Center (GEC) was established in 2016 by Executive Order 13721 for the purpose of coordinating governmentwide communications to foreign publics on terrorist narratives.[102] Section 1287 of the FY17 NDAA amended the GEC's mandate, so that it now leads federal efforts "to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests."[103] GEC's functions include "identify[ing] current and emerging trends in foreign propaganda and disinformation in order to coordinate and shape the development of tactics, techniques, and procedures to expose and refute foreign misinformation and disinformation and proactively promote fact-based narratives and policies to audiences outside the United States."[104] So far, the GEC has released a report on Russia's propaganda and disinformation efforts;[105] its Technology Engagement Team "leads U.S. Government innovation efforts by convening technology experts and programmatic authorities from the public and private sectors," and "has developed a dedicated effort for the U.S. Government to identify, assess, test and implement technologies against the problems of foreign propaganda and disinformation."[106]

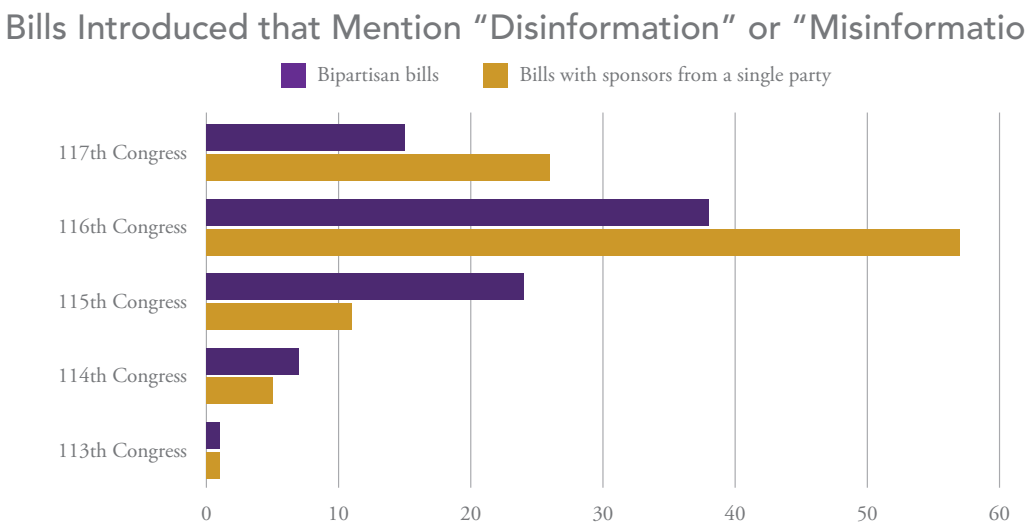
6. Office of the Director of National Intelligence

In April 2021, ODNI announced the creation of the Foreign Malign Influence Center to focus on "coordinating and integrating intelligence pertaining to malign influence, drawing together relevant and diverse expertise to better understand and monitor the challenge."[107] The center builds on existing efforts run through ODNI, including a series of Intelligence Community Assessments on disinformation, mainly focused on elections.[108] In addition, the 2021 Intelligence Authorization Act required the creation of the Social Media Data and Threat Analysis Center to facilitate public-private cooperation on countering disinformation.[109] The intelligence community plays an important role in bringing the broader strategic context to conversations about foreign disinformation, highlighting the ways in which our adversaries leverage disinformation in pursuit of their larger diplomatic, national security, and economic objectives.

B. CONGRESSIONAL PROPOSALS

In the 117th Congress alone, legislators in both chambers have introduced more than 40 bills that contain the word "misinformation" or "disinformation." Dozens of other bills address similar topics of relevance to this white paper, including foreign influence, civic education, media and advertising, and social media regulation, though without specific reference to the problem of disinformation.. The breadth of the proposed legislation demonstrates that there is congressional appetite to make progress on this issue. Like the recommendations contained in this report, these proposals attempt to address the problem of disinformation and foreign influence over the American public using a variety of different tools. However, partisanship is rampant: as shown below, nearly two-thirds of the disinformation-relevant bills introduced so far during the 117th Congress lack bipartisan co-sponsorship.

Congressional interest in addressing disinformation has risen since 2016, when Russian efforts to undermine the integrity of the presidential election generated public anxiety about its role. During the 113th Congress (2013–14), just two bills were introduced that contained the term "misinformation," and none contained the word "disinformation." Interest in the topic rose steadily, however, and during the 116th Congress (2019–21), nearly 100 bills were introduced that referred to "misinformation" or "disinformation." That session also marked an important shift: for the first time, less than half the bills pertaining to the topic had bipartisan support. Currently, just over a quarter of the way through the 117th Congress, legislators are on pace to introduce a record number of bills related to disinformation and misinformation.



C. SANCTIONS AND LAW ENFORCEMENT ACTION

Federal responses to ongoing disinformation campaigns have largely focused on law enforcement action and sanctions against actors attempting to interfere in the media environment in the context of elections. The primary targets have been Russian actors, though recently the Department of Justice charged an American citizen with election interference.[110] In the most notable case, a grand jury indicted 13 individuals and three companies associated with the Internet Research Agency—a Russian operation that attempted to interfere in the 2016 presidential election—for criminal conspiracy to defraud the United States, conspiracy to commit wire fraud and bank fraud, and aggravated identity theft.[111] In a more recent action, the Department of Justice charged a Florida resident with interfering in the 2020 presidential election by using social media to knowingly disseminate false information about voting.[112]

The Department of the Treasury has also levied sanctions against actors using cyber-enabled means to interfere in elections, relying on two executive orders (EOs) and one piece of legislation. In 2016, President Obama signed EO 13757, an amendment to an earlier EO on cyberattacks,[113] to authorize the imposition of sanctions against those "tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions."[114] In 2018, President Trump signed EO 13848 to authorize sanctions against those determined to have "directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a United States election."[115] Both of these EOs enable the Department of the Treasury to freeze the assets and block the transactions of individuals who have been added to the Office of Foreign Assets Control's Specifically Designated Nationals list because they have behaved in the ways specified above. Both EOs also enable Treasury to sanction those who "materially, financially, or technologically assist" others who engage in such behavior.

To date, Treasury has taken action pursuant to these EOs against more than 100 individuals for election-related interference and cyber-enabled disinformation. Some of these actions have built on the above-mentioned indictments of Russian individuals involved in efforts to interfere in the 2016 presidential election or have targeted Russian nationals and companies involved in interference in the 2018 midterm elections.[116] Others have involved Iranian actors and entities, including a number of Iranian government organizations, because of their interference in the 2020 presidential election.[117] The Department of Justice has also used its authorities pursuant to the Foreign Agent Registration Act and the International Emergency Economic Powers Act to seize domains used by Iran to target Americans and influence public opinion.[118]

SECTION V: RECOMMENDATIONS FOR COMBATING DISINFORMATION

Through intelligence and information-sharing programs, public diplomacy efforts, and a variety of cost imposition measures, federal efforts have sought to shape the behavior of actors attempting to spread disinformation, and Congress has responded to disinformation with a variety of approaches. What these federal efforts lack, however, is an underlying strategy to combat disinformation and a clear articulation of roles and responsibilities for addressing different aspects of the problem. As the federal government attempts to take on disinformation, it must pay attention to the interplay between digital and analog systems. Disinformation is neither new nor unique to the online environment: it predates the Internet,[119] and it spreads across radio, television, and print sources.[120] Moreover, U.S. citizens consume news from a range of outlets. While social media is an increasingly popular source of information, with slightly more than half of Americans reporting they get news "sometimes" or "often" from digital platforms,[121] more than 40 percent of Americans still prefer to get their news instead from television, radio, and print sources and regard news on social media with skepticism.[122] These statistics vary across age groups, as more than half of adults age 50 and older say they "often" receive their news from television.[123]

Not all threats in the information environment are equally harmful. Nor does the federal government have the resources to treat all threats as equally harmful. An effective approach to disinformation must enable the federal government to identify and prioritize those threats that are most dangerous, while ignoring those that are not likely to have a significant impact. The strategy and recommendations outlined in this white paper prioritize those threats that are most likely to do significant harm either to democratic institutions or to health and human safety. In the past year alone, the American public has been faced with disinformation campaigns that threaten both of these targets, demonstrating that dangerous threats are real and pervasive.

In addition to identifying and prioritizing the threats that are most harmful, the federal government must develop a comprehensive strategy to deal with those threats. To date, the federal government has not crafted a coherent strategy for the information environment, one that recognizes the unique vulnerabilities of democratic societies to disinformation and their unique strengths in responding to it. Nor has the government developed a strategy that contends with the difficulty of reconciling the United States' respect for and promotion of free speech and access to information (including from abroad) with the need to protect the American people from disinformation threats that undermine national security.

Recommendation 1: Congress should establish a Civic Education Task Force, enable greater access to civic education resources, and raise public awareness about foreign disinformation

Disinformation robs democracies of the informed and engaged citizenry necessary for a government of, by, and for the people. Along with providing recommendations to counter other kinds of malicious cyber activity, the Commission recognizes that the most sustainable way to mitigate the impact of disinformation is to build public resilience against the pernicious messages that are being promoted. Our adversaries, often amplifying and amplified by domestic voices, hope to so thoroughly muddle the truth that Americans give up trying to distinguish lies; to portray democracy and its institutions as so broken that Americans give up on the prospect for change and reform; to so severely exacerbate divisions that Americans lose sight of our fundamental shared values and sense of civic identity and civic responsibility. To counter these efforts, the United States needs to reinvigorate civic education, thereby restoring a sense of shared values and empowering citizens to be

more effective agents of change through constitutional means. A renewed emphasis on civic education should also include media and digital literacy initiatives to help people become more discerning consumers of information and develop the skills needed to understand the concept of civic responsibility in the digital age. It is a national security imperative for the U.S. government to "promote and reinvigorate American understanding of the importance of democracy and our democratic institutions, as a bulwark against foreign efforts to exploit divisions and complacency."[124]

Civic education is also essential for developing the sense of civic responsibility necessary to meet national security challenges. People who understand the Constitution and founding documents of the United States and feel a sense of responsibility to their community and nation are more likely to make an effort to avoid sharing disinformation. Traditional cybersecurity, too, is a shared responsibility between government, business, and individuals. However, if Americans do not have instilled in them a sense of civic responsibility, they are far less likely to appreciate their role, at work and at home, in protecting the cyber ecosystem. Similar concerns arise in the context of COVID-19 and other public health issues.

In support of the need to promote citizens' engagement, Congress is considering bipartisan, bicameral legislation to reinvigorate civic education.[125] Congress should move forward, with the urgency dictated by the national security imperative, to put in place resources and programs that provide appropriate federal support for civic education at all ages. An assessment by the Campaign for the Civic Mission of Schools revealed that the federal government annually spends roughly $54 per student on STEM education (science, technology, engineering, and math) and only 5 cents per student on civics;[126] as a result, according to the last National Assessment, only 25 percent of eighth graders test as "proficient" in civics.[127]

Without overriding the principle that curricular content should be determined at the state and local levels, there is much that the federal government can and should do to help remedy the shocking decline in civic education and meet our national security needs. These actions include funding for state and local educational entities, grant programs, challenge programs, and resource development, as well as other steps to enable greater access to civic education resources for students and adults, to train teachers, to encourage excellence in civic education, and to raise public awareness about the threat of disinformation. In all these efforts, Congress should prioritize and support programs and projects that build an understanding of, and appreciation for, our Constitution and founding documents.

Civic Education Task Force

Congress should establish a bipartisan Civic Education Task Force at the Department of Education to design and make publicly available civic education and digital and media literacy courses for the military, civil servants, and the broader adult population. Courses should focus on the importance of our Constitution, founding documents, and the federal government's structure; on how the federal government interacts with all stakeholders, including state and local governments; and on digital literacy and media literacy. The task force should include representatives from state and local governments and government organizations, subject matter experts, and representatives from expert organizations, including, but not limited to, academic organizations, nonprofits, and private-sector organizations.

To drive the widespread adoption of courses designed by the task force, the Department of Homeland Security and Department of Justice should implement mandatory completion of civic education and digital literacy courses for employees of state and local entities that receive federal funding, including state and local law enforcement. The Office of Management and Budget should implement mandatory completion of similar civic education and digital literacy courses for federal government employees. The Department of Defense should implement mandatory completion of civics and digital literacy

training for members of the military regarding the role, structure, and organization of the military and the federal government as an element of initial session training and as part of the Transition Assistance Program.

Civic Education Clearinghouse

Congress should authorize and appropriate funds for the Department of Education to create a clearinghouse of resources for voluntary use by K-12 educators teaching civic education, applied civics, and service learning. In developing the clearinghouse, the Department of Education should be empowered to consult with state and local governments and government organizations, subject matter experts, and nonprofit organizations, and it should place a particular emphasis on our Constitution and founding documents, as well as on media and digital literacy. The Department of Education should also produce a strategy for working with external partners to distribute the resources made available through the clearinghouse. The clearinghouse should highlight the recipients of the award and recognition program and include information about the Civic Education Fund, described below.

Student and Teacher Awards Program

Congress should authorize and appropriate funds for the Secretary of Education to create an award and recognition program to highlight both excellence by students and excellence by teachers in delivering and teaching civic education, applied civics, and service learning.

Civic Education Fund

Congress should create a Civic Education Fund and provide an initial investment of $500 million and commit $200 million each year to state educational agencies (SEAs), local educational agencies (LEAs), institutions of higher education (IHEs), and nonprofit organizations to enable grantees to develop and implement best practice curricula that incorporate civic education, applied civics, and service learning across K-12 education and to provide teacher development opportunities in civic education, applied civics, and service learning, with a particular emphasis on our Constitution and founding documents. Congress should create an Office of Civic Education responsible for overseeing and administering the Civic Education Fund and coordinating other civic education and service-learning initiatives of the federal government. The director of the office should be confirmed by the Senate.

National Disinformation Awareness Outreach Program

Congress should direct the Department of Homeland Security to create the National Disinformation Awareness Outreach Program to promote broader public awareness about disinformation through government-sponsored public service announcement (PSA) campaigns run by nongovernmental organizations. The program should not develop the PSA material itself, but instead administer a fund to which nonprofit organizations producing PSAs may apply. The sponsored PSAs should focus on building awareness about how disinformation spreads and how it affects the general public, not the specifics of recent disinformation campaigns.

Partner Approaches: Media Literacy in Finland

Finland has invested heavily in media literacy programs that ultimately aim to counter disinformation and build societal resilience. As of 2021, Finland continues to lead the European media literacy index rankings,[128] which measure a country's resistance to disinformation. Because of collaboration across different sectors, Finnish schools have been able to actualize a comprehensive media literacy education program.[129] In order to develop specialized curricula focused on media literacy and civics and implement Finnish national media education policy, media education professionals work with the National Audiovisual Institute and the Ministry of Education and Culture.[130] The Department for Media Education and Audiovisual Media (MEKU) is legally tasked with promoting media education, improving youth media skills, and fostering a safe media environment for children;[131] moreover, MEKU serves as the primary coordinator for media education at the national level.[132] Finnish civil society is also involved in creating curricula to bolster the media literacy of Finnish students. An NGO-run fact-checking service called Faktabaari adapts professional fact-checking methods for use in schools, and provides digital literacy "toolkits" that emphasize research and critical thinking skills.[133] The government works closely with the media, business, and higher education sectors in both formulating and implementing these programs.

Finland's media literacy curriculum is integrated into a variety of subjects, helping students to better understand how the concept applies to all types of engagement with information. For example, in a math lesson, "pupils learn how easy it is to lie with statistics" and are brought to understand the importance of producing and analyzing data with integrity and nuance. In an art class, students see how an image's meaning can be manipulated or changed with photo-editing software.[134] In history lessons, students "analyze notable propaganda campaigns" and their consequences, while in language courses, "teachers work with them on the many ways in which words can be used to confuse, mislead, and deceive."[135] Students are taught fact-checking skills and reliable-source selection practices—not only while writing term papers but also in lessons that specifically address social media and news. Ultimately, these more specific skills translate to improvements in students' critical thinking and ultimately to greater voter literacy: rather than focusing on debunking false claims or specific disinformation narratives, media literacy workshops emphasize the development of both a strong national narrative and a well-informed, critical student within that national narrative.

Recommendation 2: Congress should provide funding for nongovernmental disinformation researchers

The federal government alone cannot address the complex set of questions regarding the nature and impact of foreign disinformation campaigns affecting the United States. Academic institutions, think tanks, nonprofits, and corporate entities have all played important roles in the effort to identify and expose online disinformation campaigns, and the federal government can support the work of these organizations by providing funding and research opportunities in conjunction with the Social Media Data and Threat Analysis Center.[136] The research task is multifold, and nongovernmental organizations can help create richer understandings of disinformation campaigns, analyze medium- and long-term trends in the content and structure of disinformation campaigns, develop taxonomies and common definitions to enable further research, and study the effectiveness of countermeasures aimed at diminishing the impacts of disinformation. This type of research is central both to creating a more informed, resilient public by raising awareness of potential and ongoing threats and to building the evidence base upon which future policy solutions to the disinformation challenge can be developed.

Congress should provide funding for disinformation researchers through grants programs and legislation that ensures nongovernmental researchers access to data on disinformation.

Disinformation Research Grants

Congress should enhance funding to the National Science Foundation (NSF) to provide grants for rigorous research on foreign disinformation. Congress should boost funding to the Divisions of Behavioral and Cognitive Sciences, Social and Economic Sciences, Computer and Network Systems, and Information and Intelligent Systems in support of further research on:

- The actions of adversary nations in the information environment and their effect on the perceptions of U.S. citizens and attitudes toward democracy;
- The economics of disinformation and how federal action can reduce incentives for the creation and propagation of disinformation;
- The impact of manipulated media (also known as "deepfakes") on the perceptions, attitudes, and behaviors of online users; and
- Technical solutions for verifying the provenance of images, audio, and text in order to help identify, label, and contextualize manipulated media that appears online.[137]

In addition, Congress should fund DHS, in consultation with ODNI, to provide grants for priority areas established annually, and eligible grant applicants should be encouraged to work with the DTAC. Initial priorities should be building baseline understandings of the threat landscape in the information environment and of the impact of information threats on democratic publics—researchers should develop taxonomies of threat, identify metrics for evaluating the impact of disinformation campaigns, and identify metrics for evaluating the impact of countermeasures.

Congressional Research Service Study

Congress should task the Congressional Research Service with producing a study on federal laws that govern the sharing of social media data, both analyzing how existing legislation constrains the ability of social media companies to lawfully share those data in support of rigorous scientific research on disinformation and identifying potential solutions (either through amendments to existing legislation or the drafting of new legislation) so that independent research on disinformation, its spread across social media platforms, its impact on behaviors and attitudes of the American public, and the effectiveness of countermeasures against disinformation can be carried out.

Ensuring Data Availability

Congress should task the National Institute of Standards and Technology (NIST) with working with social media companies and researchers to develop a voluntary standardized data transfer format for social media data, thereby enabling both data portability for social media users and research on disinformation that crosses multiple social media platforms. "Data portability" means the ability to take data from specific services and take it elsewhere.[138] Although several major social media companies have launched a Data Transfer Project to make it easier for users to move their data across platforms, privacy concerns have hindered robust data portability efforts.[139] Standardized data transfer formats and data portability could benefit both consumers seeking to take their data elsewhere and, by making it easier to compare data across platforms, researchers studying disinformation.[140]

Recommendation 3: Congress should fund the Department of Justice to provide grants to nonprofit centers seeking to identify, expose, and explain malign foreign influence campaigns to the American public

As the damage caused by COVID-19-related disinformation makes clear, in addition to undertaking long-term public education initiatives, it is imperative that the United States possess the capacity in real time to identify highly dangerous disinformation activities and make them known both to the platforms that enable the activities and to the general public. Civil society must also maintain a robust nongovernmental capability to identify these disinformation activities and their malign infrastructure. It is critical that the U.S. government help ensure that social media companies, other media outlets, and stakeholders in the private sector and civil society continue building the expertise and credibility necessary to sound the alarm when disinformation campaigns pose an urgent threat to the American public.

To help bolster the nongovernmental capability to recognize and publicize such operations, Congress should fund the Department of Justice to provide grants through the Office of Justice Programs (which may be administered through a component of that office), in consultation with the Department of Homeland Security and the National Science Foundation, to nonprofit centers seeking to identify, expose, and explain malign foreign influence campaigns to the American public while putting those campaigns in context to avoid amplifying them. The CSC included this recommendation in the May 2020 white paper, "Cybersecurity Lessons from the Pandemic,"[141] and the continued spread of disinformation related to the pandemic and the safety of vaccines reaffirms its importance.

Recommendation 4: Congress should create a capability within the Department of Homeland Security to actively monitor foreign disinformation

The U.S. government should help identify, highlight, and shine light on foreign propaganda efforts and disinformation in the U.S. media environment and present the American public with factual information. However, as researchers at the Center for Strategic and International Studies note, "the intelligence community is limited in what it can do inside the United States, particularly regarding influence operations. The FBI is focused on the counterintelligence aspects but not leading a proactive public campaign, nor would we expect it to. The Department of Homeland Security (DHS) may be a logical choice but has not been given the mission."[142] To effectively shine light on and communicate about these operations, attribution is helpful, in the same way that some responses to cyber campaigns require the federal government to identify the perpetrators. The public's resilience against disinformation may be heightened if the disinformation is credibly linked to a specific malicious actor. The federal government should ensure that it has the capabilities and resources necessary to appropriately and reliably attribute disinformation campaigns in order to increase the effectiveness of policy responses and enhance public resilience.

Congress should task the Secretary of Homeland Security, in consultation with the Director of National Intelligence and the Director of the FBI, with creating a capability within DHS to actively monitor foreign propaganda narratives, terrorist propaganda narratives, and violent extremist narratives in the U.S. media and social media environment; to inform the public of their contents; and to present factual information on topics treated in such propaganda.

Creation of Capability

Congress should task the Secretary of Homeland Security, in coordination with the Director of National Intelligence, with creating a capability within DHS to identify foreign state-sponsored propaganda narratives and violent extremist narratives that affect the American public and with developing a Rapid Alert System to inform the public of the contents of such narratives and present scientific, statistical, and empirical information on relevant topics.[143] The capability should sit within DHS but consist of personnel from DHS, ODNI, the FBI, and the Department of State, and it should be empowered to collaborate across the federal government, as necessary. The capability should serve as a clearinghouse for information sharing and joint efforts across the federal government in combating foreign propaganda, terrorist propaganda, and violent extremist narratives. The capability should be authorized to enter agreements with social media platforms to share information in both directions on foreign propaganda, terrorist propaganda, and violent extremist propaganda narratives and efforts.

Relationship with the Global Engagement Center

The capability should also be empowered to share information with and receive information from the State Department's Global Engagement Center, which focuses on identifying, analyzing, and countering foreign propaganda affecting U.S. foreign policy interests as well as the interests of partner and allied nations. Congress should amend the FY17 NDAA to clarify the GEC's role and relationship to a DHS-housed capability for monitoring and countering domestic disinformation. The GEC should focus its efforts on identifying and countering disinformation likely to affect foreign perceptions of U.S. foreign policy or the health of foreign media environments, providing targeted financial support and training to foreign media outlets and organizations aimed at identifying and exposing propaganda put forward by adversarial nations such as Russia, China, and Iran. DHS should have primary responsibility communicating to policymakers and the public about foreign-backed disinformation designed to affect U.S. domestic policy or the social and political stability of the United States.

Data Sharing with Private Stakeholders

Congress should direct DHS, in consultation with ODNI and the FBI, to develop a plan for using data from such sources as major social media platforms, open-source intelligence companies, and other private investigative bodies to inform and increase public confidence in government-provided attribution. In producing the plan, DHS should develop and coordinate a public-private process to facilitate the voluntary sharing of information with the federal government for the purpose of attributing foreign and extremist disinformation campaigns and should develop options to swiftly impose consequences. In addition, the plan should provide a blueprint for coordinating with partners and allies to promote multidirectional information sharing between partner governments, the U.S. government, state and local governments, academia, and the private sector.

Partner Approaches: The United Kingdom's RESIST Disinformation Toolkit

The United Kingdom has recognized disinformation as a national security threat since at least 2019.[144] In response to the threat, the government has pursued several different mechanisms, including the development and publication of a RESIST Disinformation toolkit.[145] The toolkit is intended for government professionals, policy officers, special advisors, and other public-sector communications professionals, regardless of agency, role, or issue. RESIST offers a step-by-step guide to aid organizations and individuals in developing a response when disinformation affects the organization or individual directly. In doing so, the toolkit is intended to (1) build resilience to disinformation and (2) prevent the spread of disinformation by equipping government communicators with the skills and information necessary both to anticipate the impact of disinformation on their work and to reorient messaging strategies in response to ongoing disinformation campaigns.

Broadly speaking, the RESIST toolkit aims to provide a systemic and efficient approach to countering disinformation that harms U.K. society and its national interests by helping civil servants "Recognise disinformation" by highlighting objectives and principles of disinformation, and then providing "Early warning" through media monitoring and analytical tools, "Situational insight" to make early warning more actionable, and "Impact analysis" to assess the likely goals, impacts, and reach of disinformation. The toolkit finally offers "Strategic communication" guidance and helps policymakers "Track outcomes." The RESIST toolkit supports the "dissemination of reliable, truthful information that underpins . . . democracy," while ensuring that core democratic principles such as freedom of speech are protected. Notably, the toolkit emphasizes that organizations must continue to deliver effective positive communications to the public on important issues, regardless of a current disinformation presence, and offers methods for doing so.

Recommendation 5: Congress should create a grants program at the Department of Homeland Security designed to equip state and local governments with the personnel and resources necessary to identify foreign disinformation campaigns and incorporate countermeasures into public communications strategies

Given the relatively high levels of trust in state and local governments as compared to the federal government, one of the most effective ways in which the federal government can counter disinformation is to enable state and local governments to take the lead in some public communications. But like their counterparts in federal departments and agencies, the public affairs teams in state and local government agencies are often underfunded and lack the capability to educate the public about disinformation affecting state and local policy issues. The federal government should also ensure that state and local governments, including state and local election officials and courts, can apply for funding to equip their communications teams with additional personnel and the tools to identify and counter disinformation in areas likely to affect health and human safety or the integrity of democratic institutions.

Congress should authorize the creation of a grant program administered by the Department of Homeland Security and should appropriate sufficient funding for the program to equip state and local governments with the personnel and resources necessary to identify disinformation campaigns and incorporate countermeasures into public communications strategies as government plans or policies affecting health and human safety or the integrity of democratic institutions are rolled out.

Allocation and Purpose

Grants should be allocated to those state government entities primarily responsible for plans and policies that affect health and human safety or democratic processes and institutions, including, but not limited to, health departments and organizations administering elections or state and local courts. Grants should be used to hire or train personnel or to acquire the tools necessary to identify disinformation campaigns and incorporate counter-messaging strategies into communications plans.

Use of Grants

Organizations applying for grants should submit detailed plans for the use of funds administered through the grant program, and after receiving a grant they should report on the actual use of funds and associated outcomes. Such plans should incorporate strategies for identifying and countering not only digital foreign disinformation but also foreign disinformation circulating in broadcast or print media. Communications plans developed through the grant program should focus, to the extent practicable, on evidence-based strategies for countering disinformation and on disseminating authoritative scientific or statistical information in support of government plans and policies. Grant recipients should be empowered to consult with local intermediary organizations, with the goal of identifying trusted community members with which they can partner and gain help in reaching the populations most vulnerable to disinformation.

Duration and Evaluation

Congress should appropriate funds for the grant program to be distributed over two years, with grants awarded on a quarterly basis for a period lasting no longer than one year. The Secretary of Homeland Security should submit to Congress an annual report on the funds administered through the grant program and, to the extent possible, provide metrics for evaluating the program's outcomes. The second of these annual reports submitted to Congress, after the grant program concludes, should make recommendations regarding whether the grant program should be continued and what modifications to the program, if any, would enable it to better accomplish its purpose of equipping state and local government communicators with the resources necessary to anticipate and counter disinformation affecting health and human safety or the integrity of democratic institutions.

Recommendation 6: Congress should reform the Foreign Agents Registration Act and direct the Federal Communications Commission to introduce new regulations in order to improve media ownership transparency in the United States

The level of trust in the ability of mass media to report the news "fully, accurately, and fairly" is falling. In 2000, 12 percent of the adult population in the United States rated their trust level in mass media as "not at all"; by contrast, 51 percent had either a great deal of trust or a fair amount of trust. In 2020, 33 percent of American adults had no trust in mass media, while only 40 percent had a great deal or fair amount of trust.[146] Many factors affect overall levels of trust in the media, but American news consumers should be empowered to understand the sources of information in their news environment. When media outlets are foreign-owned and operated, transparency regulations are crucial to ensuring that American news consumers are aware of the foreign actors attempting to influence public opinion. When media outlets are domestic, transparency rules are still crucial, for they help American news consumers contextualize the information they receive.

Competition in media markets is important for more than purely economic reasons—it is also central to ensuring that a diverse array of voices and perspectives can be heard and that local news markets are responsive to local concerns.

Congress should strengthen the Department of Justice's ability to investigate potential violations of the Foreign Agents Registration Act (FARA) by foreign media companies, remove exemptions for foreign media companies registered under the Lobbying Disclosure Act (LDA), and clarify how FARA's requirements to file "informational materials" every six months relate to social media and email content. Congress should also direct the Federal Communications Commission (FCC) to promulgate new regulations on media ownership transparency for all media companies operating within the United States.

Foreign Agents Registration Act Reform

Congress passed the Foreign Agents Registration Act in 1938 in response to Nazi propaganda,[147] with the intent not to censor foreign propaganda but to promote transparency regarding the sources of information being disseminated to the American public.[148] Under the law, foreign agents are required to register with the DOJ and regularly file information regarding their activities in the United States, including copies of "informational materials" disseminated in the course of such activities. The law gives the DOJ the authority to investigate potential FARA violations, and to date, the DOJ has taken action under FARA against certain foreign-owned media, including the Russian-owned RT media outlet.[149] However, current law stipulates that an individual or entity registered under the Lobbying Disclosure Act need not register under FARA, unless the individual or entity is acting on behalf of a foreign government or foreign political party.[150] Because of this exemption, the records collected under FARA contain an incomplete picture of individuals operating as foreign agents within the United States.

Congress should therefore amend FARA to remove from the LDA exemption those foreign organizations that produce media content for consumption by the public, including political advertisements, and ensure that filing requirements for FARA registrants are sufficiently robust for the digital age. This narrowing of the exemption should be designed in such a way that it does not require all foreign-owned private companies to register as foreign agents under FARA—exemptions should continue to apply to foreign car manufacturers, for example, that register under the LDA. Furthermore, the amendment should stipulate a process whereby media organizations from allied countries may apply for a license allowing them to maintain the exemption.

Congress should also update FARA reporting requirements by amending the definition of "informational materials" to make clear that social media and email communications are covered, specifying which types need to be included in FARA filings. Several proposals to amend the law in this manner have been put forward by members of Congress, but none has yet been adopted.[151] In amending the definition, Congress should ensure that the DOJ adopts a records system that allows the social media posts that are filed to be maintained in a dynamic form, along with comments, while preserving appropriate privacy protections.[152]

Finally, Congress should grant the DOJ greater authority to investigate FARA violations, improve FARA compliance, and enforce FARA disclosure requirements. A bill introduced in 2017, titled the Disclosing Foreign Influence Act,[153] could serve as a template for these reforms. The bill would grant the DOJ civil subpoena authority to investigate possible FARA violations, would remove FARA exemptions for those that register under the LDA, would require the development of a FARA enforcement strategy, and would require reports from the DOJ Inspector General and the Government Accountability Office (GAO) on the enforcement strategy and effectiveness of the new law.[154] A similar bill introduced in 2021, the Chinese Communist Party Influence Transparency Act, would remove LDA exemptions for all Chinese corporations.[155]

Mandate Media Ownership Transparency

Congress should amend the Telecommunications Act of 1996[156] to task the FCC with developing new regulations on media ownership transparency. The FCC currently regulates foreign ownership of broadcast media;[157] moreover, it requires foreign media outlets to submit reports on their activities.[158] The FCC also has numerous rules in place regarding media ownership to ensure competition within American media markets, and by law, the FCC must review these rules every four years to determine whether they are still necessary.[159] But no regulation currently requires domestic media companies to disclose their ownership, and as a result American news consumers often lack reliable information about the corporate entities that own and operate local, regional, or national news outlets. Congress should task the FCC with developing new rules regarding ownership transparency for all media outlets in order to empower Americans in evaluating the sources of their news.

Recommendation 7: Congress should grant a federal entity the authority to publish and enforce transparency guidelines for social media platforms

Social media platforms have changed how people consume information. While not the sole purveyors of information, platforms are leveraged by peddlers of mis- and disinformation to "provoke and amplify political and social discord in the United States."[160] Because of their unique position in the information ecosystems, platforms can exert positive influence over the media and information environment. Policymakers and lawmakers should resist the impulse to regulate content outside of what is already exempted from First Amendment protections.[161]

Congress should direct the Biden administration to report back within 90 days with a plan to task an entity with establishing clear transparency guidelines for social media companies. This entity should not moderate content but should be tasked with developing rules pertaining to requirements for:

- Transparency reporting regarding content moderation policies and takedowns;
- Transparency and labeling of advertisements on platforms;
- Transparency requirements for information-sorting algorithms on platforms;
- Labeling of content created by FARA-registered agents;
- Labeling of bot accounts and content spread by bots; and
- Policies and processes to be developed by social media companies to disclose the use of bots and other such tools.

CONCLUSION

Disinformation is a challenging policy issue. It touches on individual freedom and liberty. It involves foreign intervention in our democracy while affecting national security and the foundations of U.S. democracy. It is inherently political in that it sways hearts and minds. It weaves deftly through modern society and networks—visible only sometimes but always threatening. The recommendations contained in this white paper are equally challenging, and policymakers will find it more difficult to implement some—like regulation of social media companies—than others. While the recommendations are to an extent interconnected, they can be implemented individually—and each would represent progress in the fight to combat disinformation.

ABBREVIATIONS

CCP	Chinese Communist Party
CISA	Cybersecurity and Infrastructure Security Agency
COVID	coronavirus disease
CSC	Cyberspace Solarium Commission
DHS	Department of Homeland Security
DOJ	Department of Justice
DTAC	Social Media Data and Threat Analysis Center
EO	executive order
FARA	Foreign Agents Registration Act
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
GEC	Global Engagement Center
IHE	institution of higher education
LDA	Lobbying Disclosure Act
LEA	local educational agency
MDM team	Mis-, Dis-, and Malinformation team
MEKU	[Finnish] Department for Media Education and Audiovisual Media
NATO	North Atlantic Treaty Organization
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NGO	nongovernmental organization
ODNI	Office of the Director of National Intelligence
PSA	public service announcement
SEA	state educational agency

ENDNOTES

1 Laura Rosenberger and Lindsay Gorman, "How Democracies Can Win the Information Contest," Washington Quarterly 76, no. 2 (2020): 75–96; Ashish Jaiman, "Disinformation Is a Cybersecurity Threat," Medium, January 30, 2021, https://medium.com/swlh/disinformation-is-a-cybersecurity-threat-335681b15b48; Jonathon Morgan and Renee DiResta, "Information Operations Are a Cybersecurity Problem: Toward a New Strategic Paradigm to Combat Disinformation," Just Security, July 10, 2018, https://www.justsecurity.org/59152/information-operations-cybersecurity-problem-strategic-paradigm-combat-disinformation/; Laura Fichtner, "What Kind of Cyber Security? Theorising Cyber Security and Mapping Approaches," Internet Policy Review 7, no. 2 (May 15, 2018), https://policyreview.info/articles/analysis/what-kind-cyber-security-theorising-cyber-security-and-mapping-approaches.

2 U.S. Cyberspace Solarium Commission, "Cybersecurity Lessons from the Pandemic," CSC White Paper #1 (May 2020), 11, available at https://www.solarium.gov/public-communications/pandemic-white-paper.

3 Dimitar Nikolov, Alessandro Flammini, and Filippo Menczer, "Right and Left, Partisanship Predicts (Asymmetric) Vulnerability to Misinformation," *Harvard Kennedy School Misinformation Review*, February 15, 2021, https://misinforeview.hks.harvard.edu/article/right-and-left-partisanship-predicts-asymmetric-vulnerability-to-misinformation/.

4 Aaron Smith, "How Americans View Tech Companies," Pew Research Center, June 28, 2018, https://www.pewresearch.org/internet/2018/06/28/public-attitudes-toward-technology-companies/.

5 Amy Mitchell et al., "Many Americans Say Made-Up News Is a Critical Problem That Needs to Be Fixed," Pew Research Center, June 5, 2019, https://www.pewresearch.org/journalism/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/.

6 Laura Rosenberger and Lindsay Gorman, "How Democracies Can Win the Information Contest," *Washington Quarterly* 43, no. 2 (2020): 75–96.

7 U.S. Cyberspace Solarium Commission, Report of the United States of America Cyberspace Solarium Commission (March 2020), 34, available at https://www.solarium.gov/report.

8 CSC, "Cybersecurity Lessons from the Pandemic," 12–13.

9 A Wanless and J Pamment, "How Do You Define a Problem Like Influence?," *Journal of Information Warfare* 18, no. 3 (2019): 1–14.

10 Claire Wardle, "Information Disorder, Part 1: The Essential Glossary," *First Draft Footnotes* (blog), July 9, 2018, https://medium.com/1st-draft/information-disorder-part-1-the-essential-glossary-19953c544fe3.

11 "Information Operations," RAND, 2021, https://www.rand.org/topics/information-operations.html.

12 Renee DiResta and Shelby Grossman, "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019," November 12, 2019, available at https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks.

13 Conor Cunningham, "A Russian Federation Information Warfare Primer," Henry M. Jackson School of International Studies, November 12, 2020, https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/.

14 U.S. Department of State, *GEC Special Report: Russia's Pillars of Disinformation and Propaganda* (August 2020), *United* https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

15 Alicia Wanless and Laura Walters, "How Journalists Become an Unwitting Cog in the Influence Machine," Carnegie Endowment for International Peace, October 13, 2020, https://carnegieendowment.org/2020/10/13/how-journalists-become-unwitting-cog-in-influence-machine-pub-82923.

16 U.S. Department of State, *GEC Special Report: Russia's Pillars of Disinformation and Propaganda*.

17 James Shires, "Hack-and-Leak Operations and U.S. Cyber Policy," *War on the Rocks*, August 14, 2020, https://warontherocks.com/2020/08/the-simulation-of-scandal/.

18 Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It," RAND Corporation, July 11, 2016, available at https://www.rand.org/pubs/perspectives/PE198.html.

19 Joshua Kurlantzick, "China's Global Information and Influence Campaign," Council on Foreign Relations, 2021, https://www.cfr.org/project/chinas-global-information-and-influence-campaign.

20 Edward Wong, Matthew Rosenberg, and Julian E. Barnes, "Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say," *New York Times*, April 22, 2020; updated January 5, 2021, https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html.

21 Matt Apuzzo, "Pressured by China, E.U. Softens Report on Covid-19 Disinformation," *New York Times*, April 24, 2020, https://www.nytimes.com/2020/04/24/world/europe/disinformation-china-eu-coronavirus.html.

22 Daniel Wood, Sean McMinn, and Emily Feng, "China Used Twitter to Disrupt Hong Kong Protests, But Efforts Began Years Earlier," *NPR*, September 17, 2019, https://www.npr.org/2019/09/17/758146019/china-used-twitter-to-disrupt-hong-kong-protests-but-efforts-began-years-earlier; James Griffiths, "From Cover-up to Propaganda Blitz: China's Attempts to Control the Narrative on Xinjiang," CNN, April 17, 2021, https://www.cnn.com/2021/04/16/china/beijing-xinjiang-uyghurs-propaganda-intl-hnk-dst/index.html; Erika Kinetz, "Anatomy of a Conspiracy: With COVID, China Took Leading Role," *AP News*, February 15, 2021, https://apnews.com/article/pandemics-beijing-only-on-ap-epidemics-media-122b73e134b780919cc1808f3f6f16e8; Dexter Roberts, "China's Disinformation Strategy: Its Dimensions and Future" (Atlantic Council, December 2020), https://www.atlanticcouncil.org/wp-content/uploads/2020/12/CHINA-ASI-Report-FINAL-1.pdf.

23 Erika Kinetz, "Army of Fake Fans Boosts China's Messaging on Twitter," *AP News*, May 28, 2021, https://apnews.com/article/asia-pacific-china-europe-middle-east-government-and-politics-62b13895aa6665ae4d887dcc8d196dfc.

24 Joshua Kurlantzick, "How China Ramped Up Disinformation Efforts During the Pandemic," Council on Foreign Relations, September 10, 2020, https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic; Sulmaan Wasif Khan, "Wolf Warriors Killed China's Grand Strategy," Foreign Policy, May 28, 2021, https://foreignpolicy.com/2021/05/28/china-grand-strategy-wolf-warrior-nationalism/.

25 Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 3 (2017): 484–501, available at https://gking.harvard.edu/files/gking/files/50c.pdf?m=1463587807; "The China Deep Dive: A Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China," U.S. House of Representatives Permanent Select Committee on Intelligence, September 30, 2020, https://intelligence.house.gov/uploadedfiles/hpsci_china_deep_dive_redacted_summary_9.29.20.pdf.

26 "Hundreds of Fake Twitter Accounts Linked to China Sowed Disinformation Prior to the US Election—Report," Cardiff University: News, January 28, 2021, https://www.cardiff.ac.uk/news/view/2491763-hundreds-of-fake-twitter-accounts-linked-to-china-sowed-disinformation-prior-to-the-us-election,-with-some-continuing-to-amplify-reactions-to-the-capitol-building-riot-report.

27 Gerry Shih, "AP Exclusive: In Western China, Thought Police Instill Fear," *AP News*, December 17, 2017, https://apnews.com/article/china-religion-10207e125d564897934a27288855e34d.

28 Austin Ramzy and Chris Buckley, "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims," *New York Times*, November 16, 2019, https://www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html.

29 Chris Buckley and Amy Qin, "Muslim Detention Camps Are Like 'Boarding Schools,' Chinese Official Says," *New York Times*, March 12, 2019, https://www.nytimes.com/2019/03/12/world/asia/china-xinjiang.html.

30 Emma Graham-Harrison, "China Has Built 380 Internment Camps in Xinjiang, Study Finds," *The Guardian*, September 23, 2020; https://www.theguardian.com/world/2020/sep/24/china-has-built-380-internment-camps-in-xinjiang-study-finds.

31 Emily Rauhala, "U.S., E.U., Canada and Britain Announce Sanctions on China over the Abuse of Uyghurs," *Washington Post*, https://www.washingtonpost.com/world/xinjiang-sanctions-european-union/2021/03/22/1b0d69aa-8b0a-11eb-a33e-da28941cb9ac_story.html.

32 Ken Moritsugu, "China Bashes US over Racism, Inequality, Pandemic Response," ABC News, March 24, 2021, https://abcnews.go.com/US/wireStory/china-bashes-us-racism-inequality-pandemic-response-76648636.

33 Jeff Kao et al., "'We Are Very Free': How China Spreads Its Propaganda Version of Life in Xinjiang," *New York Times*, June 23, 2021, https://www.nytimes.com/interactive/2021/06/22/technology/xinjiang-uyghurs-china-propaganda.html.

34 Eva Xiao, "China Used Twitter, Facebook More Than Ever Last Year for Xinjiang Propaganda," *Wall Street Journal*, March 30, 2021, sec. World, https://www.wsj.com/articles/china-used-twitter-facebook-more-than-ever-last-year-for-xinjiang-propaganda-11617101007

35 Jeff Kao et al., "'We Are Very Free': How China Spreads Its Propaganda Version of Life in Xinjiang," *New York Times*, June 23, 2021, sec. Technology, https://www.nytimes.com/interactive/2021/06/22/technology/xinjiang-uyghurs-china-propaganda.html.

36 Sonja Swanbeck, "How to Understand Iranian Information Operations," Lawfare, February 19, 2021, https://www.lawfareblog.com/how-understand-iranian-information-operations.

37 Emerson T. Brooking and Suzanne Kianpour, "Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century" (Atlantic Council, 2020), https://www.atlanticcouncil.org/wp-content/uploads/2020/02/IRAN-DIGITAL.pdf.

38 @DFRLab, "Tensions Escalate on Social Media Platforms after Soleimani's Death," *DFRLab* (blog), January 4, 2020, https://medium.com/dfrlab/tensions-escalate-on-social-media-platforms-after-soleimanis-death-48f295ecec5e.

39 "Exclusive: Iran Steps Up Efforts to Sow Discord Inside the U.S.," *Time*, June 7, 2021; updated June 9, 2020, https://time.com/6071615/iran-disinformation-united-states/.

40 National Intelligence Council, "Intelligence Community Assessment: Foreign Threats to the 2020 U.S. Federal Elections" (March 10, 2021), I, 5–7, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

41 Ibid., 6.

42 Ana Lucía Schmidt et al., "Anatomy of News Consumption on Facebook," *Proceedings of the National Academy of Sciences* 114, no. 12 (2017): 3035–39, https://www.pnas.org/content/114/12/3035.

43 Elisa Shearer, "More Than Eight-in-Ten Americans Get News from Digital Devices," Pew Research Center, January 12, 2021, https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/.

44 Rachel Lerman, "Facebook says it has taken down 7 million posts for spreading coronavirus misinformation," *Washington Post*, August 11, 2020, https://www.washingtonpost.com/technology/2020/08/11/facebook-covid-misinformation-takedowns.

45 Karen Kornbluh, Eli Weiner, and Adrienne Goldstein, "New Study by Digital New Deal Finds Engagement with Deceptive Outlets Higher on Facebook Today Than Run-up to 2016 Election," German Marshall Fund of the United States, October 12, 2020, https://www.gmfus.org/news/new-study-digital-new-deal-finds-engagement-deceptive-outlets-higher-facebook-today-run-2016.

46 Jacob N. Shapiro, Natalie Thompson, and Alicia Wanless, "Research Collaboration on Influence Operations between Industry and Academia: A Way Forward" (Carnegie Endowment for International Peace, December 2020), available at https://carnegieendowment.org/2020/12/03/research-collaboration-on-influence-operations-between-industry-and-academia-way-forward-pub-83332.

47 Though this trend has been documented in case studies of specific disinformation campaigns, a team of researchers supported by the Carnegie Endowment for International Peace that surveyed existing academic literature on the subject found a notable gap in studies surveying cross-platform influence operations and their impact on the beliefs and behaviors of audiences; Jon Bateman et al., "Measuring the Effects of Influence Operations: Key Findings and Gaps from Empirical Research," Carnegie Endowment for International Peace, June 28, 2021, https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824. See also Claire Wardle, "5 Lessons for Reporting in an Age of Disinformation," First Draft, December 27, 2018, https://firstdraftnews.org/articles/5-lessons-for-reporting-in-an-age-of-disinformation/.

48 Seb Cubbin, "Banned Sites and Pro-Russian Networks Are Driving Anti-Pfizer Vaccine Disinformation," First Draft, March 31, 2021, https://firstdraftnews.org/articles/anti-pfizer-vaccine-narratives/.

49 "Anatomy of a Disinformation Empire: Investigating NaturalNews" (ISD, 2020), https://www.isdglobal.org/wp-content/uploads/2020/06/20200620-ISDG-NaturalNews-Briefing-V4.pdf.

50 Shannon Bond, "'The Perfect Storm': How Vaccine Misinformation Spread to the Mainstream," *NPR*, December 10, 2020, https://www.npr.org/2020/12/10/944408988/the-perfect-storm-how-coronavirus-spread-vaccine-misinformation-to-the-mainstrea; Geoff Brumfiel, "Anti-Vaccine Activists Use a Federal Database to Spread Fear about COVID Vaccines," *NPR*, June 14, 2021,

https://www.npr.org/sections/health-shots/2021/06/14/1004757554/anti-vaccine-activists-use-a-federal-database-to-spread-fear-about-covid-vaccine.

51 Wardle, "5 Lessons for Reporting in an Age of Disinformation"; Yariv Tsfati et al., "Causes and Consequences of Mainstream Media Dissemination of Fake News: Literature Review and Synthesis," *Annals of the International Communication Association* 44, no. 2 (2020): 157–73, available at https://www.tandfonline.com/doi/full/10.1080/23808985.2020.1759443.

52 Kurlantzick, "How China Ramped Up Disinformation Efforts During the Pandemic."

53 David A. Broniatowski et al., "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate," *American Journal of Public Health* 108, no. 10 (October 2018): 1378–84, available at https://ajph.aphapublications.org/doi/pdf/10.2105/AJPH.2018.304567.

54 Justin Anderson and Sarah Jacobs Gamberini, "Infodemic: Russian Disinformation Campaigns, Public Health, and COVID-19," Inkstick, March 25, 2020, https://inkstickmedia.com/infodemic/

55 Mark Scott, "Russia and China Target U.S. Protests on Social Media," Politico, June 1, 2020, https://www.politico.com/news/2020/06/01/russia-and-china-target-us-protests-on-social-media-294315.

56 Josh Margolin and Lucien Bruggeman, "Intel Bulletin Warns of 'Malign Actors' Targeting US over George Floyd Fallout," ABC News, June 11, 2020, https://abcnews.go.com/US/intel-bulletin-warns-malign-actors-targeting-us-george/story?id=71184163.

57 Craig Timberg and Isaac Stanley-Becker, "Black Voters Are Being Targeted in Disinformation Campaigns, Echoing the 2016 Russian Playbook," *Washington Post*, August 26, 2020, https://www.washingtonpost.com/technology/2020/08/26/race-divisions-highlighted-disinformation-2016/; Craig Timberg and Shane Harris, "Chinese Network of Fake Accounts Targets Trump with English-Language Videos," *Washington Post*, August 12, 2020, https://www.washingtonpost.com/technology/2020/08/12/china-video-network-trump/.

58 *Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, vol. 2, *Russia's Use of Social Media with Additional Views* (2019), available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

59 Sarah Jacobs Gamberini, "Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns," Joint Forces Quarterly 99 (2020): 4–13, available at https://wmdcenter.ndu.edu/Portals/68/Documents/jfq/jfq-99/jfq-99_4-13_Gamberini.pdf?ver=Yoes_BQSvex7rNRLXvI08Q%3d%3d.

60 Alicia Sanders-Zakre, "Russia Blocks Consensus at CWC Conference," Arms Control Association, January/February 2019, https://www.armscontrol.org/act/2019-01/news/russia-blocks-consensus-cwc-conference.

61 "Putin Is Running a Disinformation Campaign on Navalny's Poisoning," editorial, *Washington Post*, October 2, 2020, https://www.washingtonpost.com/opinions/global-opinions/putin-is-running-a-disinformation-campaign-on-navalnys-poisoning/2020/10/02/0889ef54-0411-11eb-897d-3a6201d6643f_story.html.

62 Ibid.

63 Kristofer Goldsmith, "VVA Investigative Report," September 17, 2019, executive summary of *An Investigation into Foreign Entities Who Are Targeting Servicemembers and Veterans Online*, https://vva.org/trollreport/.

64 Ben Schreckinger, "How Russia Targets the U.S. Military," *Politico Magazine*, June 12, 2017, https://www.politico.com/magazine/story/2017/06/12/how-russia-targets-the-us-military-215247/.

65 Ibid.

66 Paul Merklinger and Ryan Orsini, "Disinformation Disruption and Distance: Public Confidence in the U.S. Military in the COVID-19 Era," *Strategy Bridge*, July 28, 2020, https://thestrategybridge.org/the-bridge/2020/7/28/disinformation-disruption-and-distance-public-confidence-in-the-us-military-in-the-covid-19-era.

67 Andrius Sytas, "Lithuania Sees Fake News Attempt to Discredit NATO Exercises," *Reuters*, June 13, 2018, https://www.reuters.com/article/us-nato-russia/lithuania-sees-fake-news-attempt-to-discredit-nato-exercises-idUSKBN1J92FC.

68 Lily Hay Newman, "Facebook Ad Services Let Anyone Target US Military Personnel," *Wired*, January 28, 2021, https://www.wired.com/story/facebook-ad-targeting-us-military/.

69 *Hijacking Our Heroes: Exploiting Veterans Through Disinformation on Social Media: Hearing of the House Committee on Veterans' Affairs*, 116th Cong. (2019) (statement of Dr. Vlad Barash, Science Director at Graphika), https://www.congress.gov/116/meeting/house/110183/witnesses/HHRG-116-VR00-Wstate-BarashV-20191113.pdf.

70 Suzanne Spaulding, "Why the Kremlin Targets Veterans," CSIS, November 8, 2019, https://www.csis.org/analysis/why-kremlin-targets-veterans.

71 For example, defamation—false statements that damage a person's reputation—is considered to possess little First Amendment value and can lead to civil liability and even criminal punishment if intentional.

72 Kathleen Ann Ruane, "Freedom of Speech and Press: Exceptions to the First Amendment" (Congressional Research Service, September 8, 2014), https://fas.org/sgp/crs/misc/95-815.pdf .

73 Brendan Pelsue, "When It Comes to Education, the Federal Government Is in Charge of . . . Um, What?," *Ed.: Harvard Ed. Magazine*, Fall 2017, https://www.gse.harvard.edu/news/ed/17/08/when-it-comes-education-federal-government-charge-um-what.

74 Andrew Ujifusa, "GOP Leader: Biden Grant Plan Referencing Anti-Racism, 1619 Project Is 'Divisive Nonsense,'" *Education Week*, April 30, 2021, https://www.edweek.org/teaching-learning/gop-leader-biden-grant-plan-referencing-anti-racism-1619-project-is-divisive-nonsense/2021/04.

75 Darrell M. West, "How to Combat Fake News and Disinformation," Brookings, December 18, 2017, https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/

76 Wanless and Walters, "How Journalists Become an Unwitting Cog in the Influence Machine."

77 Media Insight Project, "Holding Power Accountable: The Press and the Public," chapter 2 of *How the Press and Public Can Find Common Purpose* (American Press Institute, December 18, 2019), https://www.americanpressinstitute.org/publications/reports/survey-research/holding-power-accountable-the-press-and-the-public/.

78 A Pew Research survey suggests just 20 percent of Americans trust the federal government: "Americans' Views of Government: Low Trust, but Some Positive Performance Ratings," Pew Research Center, September 14, 2020, https://www.pewresearch.org/politics/2020/09/14/americans-views-of-government-low-trust-but-some-positive-performance-ratings/.

79 For fact-checking, see, for example, the International Fact-checking Network run by the Poynter Institute, https://www.poynter.org/ifcn/. Nonprofit organizations working on the disinformation challenge and on supporting journalists include First Draft News (https://firstdraftnews.org/), the Digital Forensics Research Lab at the Atlantic Council (https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/), the Internet Observatory at Stanford University (https://cyber.fsi.stanford.edu/io/io), and the Commission on Information Disorder at the Aspen Institute (https://www.aspeninstitute.org/programs/commission-on-information-disorder/).

80 "Public Trust in Government: 1958–2021," Pew Research Center, May 17, 2021, https://www.pewresearch.org/politics/2021/05/17/public-trust-in-government-1958-2021/.

81 Justin McCarthy, "Americans Still More Trusting of Local Than State Government," Gallup, October 8, 2018, https://news.gallup.com/poll/243563/americans-trusting-local-state-government.aspx.

82 Ibid.

83 National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, 130 Stat. 2000 (2016), https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf; National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283 § 1287 (2017), https://www.govinfo.gov/content/pkg/PLAW-115publ91/pdf/PLAW-115publ91.pdf; John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 § 1239 (2018), https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf; National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, 133 Stat. 1198 § 1282 (2019), https://www.govinfo.gov/content/pkg/PLAW-116publ92/pdf/PLAW-116publ92.pdf; William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 567 (2020), https://www.congress.gov/bill/116th-congress/house-bill/6395/text.

84 "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," press release, United States Department of Justice, February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

85 "Treasury Sanctions Iranian Entities for Attempted Election Interference," press release,. U.S. Department of the Treasury, October 22, 2020, https://home.treasury.gov/news/press-releases/sm1158; "Treasury Takes Further Action against Russian-Linked Actors," press release, U.S. Department of the Treasury, January 11, 2021, https://home.treasury.gov/news/press-releases/sm1232.

86 Exec. Order No. 13757, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," 82 Fed. Reg. 1 (January 3, 2017), https://www.federalregister.gov/documents/2017/01/03/2016-31922/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious; Exec. Order No. 13848, "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," 83 Fed. Reg. 46843 (September 14, 2018), https://www.federalregister.gov/documents/2018/09/14/2018-20203/imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election.

87 The White House "National Security Strategy of the United States of America" (December 2017), 34–35, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

88 Ibid., 35.

89 The White House, "Interim National Security Strategic Guidance" (March 2021), 7, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

90 Jon Roozenbeek, Sander van der Linden, and Thomas Nygren, "Prebunking Interventions Based on the 'Inoculation' Theory Can Reduce Susceptibility to Misinformation across Cultures," *Harvard Kennedy School Misinformation Review*, February 3, 2020, https://misinforeview.hks.harvard.edu/article/global-vaccination-badnews/.

91 "Election Security Rumor vs. Reality," Cybersecurity and Infrastructure Security Agency, September 23, 2021, https://www.cisa.gov/rumorcontrol.

92 "#PROTECT2020: Disinformation Stops with You," 2021, https://vva.org/protect2020.

93 Quotation from "Coronavirus Rumor Control," Federal Emergency Management Agency, July 6, 2021, https://www.fema.gov/disasters/coronavirus/rumor-control; see also "Coronavirus: DOD Response," U.S. Department of Defense, October 27, 2021 [frequent updates], https://www.defense.gov/Explore/Spotlight/Coronavirus/Rumor-Control.

94 "Coronavirus Response," United States Department of Justice, October 27, 2021[frequent updates], https://www.justice.gov/coronavirus; "Coronavirus (COVID-19) Pandemic: The FTC in Action," Federal Trade Commission, 2021, https://www.ftc.gov/coronavirus.

95 "Rumor Control for the 2022 Election," Maryland State Board of Elections, 2021, https://elections.maryland.gov/press_room/rumor_control.html; "Maryland Coronavirus (COVID-19): Rumor Control," Maryland.gov, https://govstatus.egov.com/md-coronavirus-rumor-control; "Rumor Control," Colorado Department of Public Health & Environment / Colorado State Emergency Operations Center," September 23, 2020, https://covid19.colorado.gov/rumor-control.

96 Benjamin Freed, "Secretaries of State Ask DHS to Expand Anti-disinformation Fight," *StateScoop*, April 19, 2021, https://statescoop.com/secretaries-state-dhs-expand-anti-disinformation-fight.

97 "Mis, Dis, Malinformation: MDM Mission Overview," Cybersecurity and Infrastructure Security Agency, October 25, 2021, https://www.cisa.gov/mdm.

98 "Resilience Series Graphic Novels," Cybersecurity and Infrastructure Security Agency, n.d., https://www.cisa.gov/resilience-series-graphic-novels.

99 "What We Investigate: Combating Foreign Influence," Federal Bureau of Investigation, n.d., https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

100 "What We Investigate: Protected Voices," Federal Bureau of Investigation, n.d., https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices.

101 Ibid.

102 Exec. Order No. 13721, "Developing an Integrated Global Engagement Center To Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584," 81 Fed. Reg. 14685 (March 17, 2016), https://www.federalregister.gov/documents/2016/03/17/2016-06250/developing-an-integrated-global-engagement-center-to-support-government-wide-counterterrorism.

103 National Defense Authorization Act for Fiscal Year 2017, §1287(a)(2).

104 Ibid., §1287(b)(4).

105 "GEC Special Report: Russia's Pillars of Disinformation and Propaganda" (U.S. Department of State, August 2020), available at https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report.

106 "Technology Engagement Team," U.S. Department of State, n.d., https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/technology-engagement-team.

107 Olivia Gazis, "U.S. Intelligence Community to Create Center to Address Foreign Malign Influence," CBS News, April 26, 2021, https://www.cbsnews.com/news/intelligence-community-foreign-malign-influence.

108 See, for example, National Intelligence Council, "Intelligence Community Assessment: Foreign Threats to the 2020 US Federal Elections" (ODNI, March 10, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

109 Intelligence Authorization Act for Fiscal Year 2021, S. 3905, 116th Cong., §307 (2020), incorporated into the National Defense Authorization Act for Fiscal Year 2021, §5323(c).

110 "Social Media Influencer Charged with Election Interference Stemming from Voter Disinformation Campaign," press release, United States Department of Justice, January 27, 2021, https://www.justice.gov/opa/pr/social-media-influencer-charged-election-interference-stemming-voter-disinformation-campaign.

111 "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies." The Justice Department later dropped its charges against two of the companies initially named in the indictment. See Ken Dilanian, Pete Williams, and Tom Winter, "Why Did the Justice Department Drop Its Prosecution of 2 Firms Linked to a Putin Associate?" NBCNews, March 17, 2020, https://www.nbcnews.com/politics/justice-department/why-did-justice-department-drop-its-prosecution-2-firms-linked-n1161886.

112 "Social Media Influencer Charged with Election Interference Stemming from Voter Disinformation Campaign," press release, United States Department of Justice, January 27, 2021, https://www.justice.gov/opa/pr/social-media-influencer-charged-election-interference-stemming-voter-disinformation-campaign.

113 Exec. Order No. 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 80 Fed. Reg. 18077 (April 2, 2015), https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities.

114 Exec. Order No. 13757, "Taking Additional Steps to Address the National Emergency," 1.

115 Exec. Order No. 13848, "Imposing Certain Sanctions in the Event of Foreign Interference," 46844.

116 "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," press release, U.S. Department of the Treasury, March 15, 2018, https://home.treasury.gov/news/press-releases/sm0312; "Treasury Targets Assets of Russian Financier Who Attempted to Influence 2018 U.S. Elections," press release, U.S. Department of the Treasury, September 30, 2019, https://home.treasury.gov/news/press-releases/sm787.

117 "Treasury Sanctions Iranian Entities for Attempted Election Interference," press release, U.S. Department of the Treasury, October 22, 2020, https://home.treasury.gov/news/press-releases/sm1158.

118 "United States Seizes 27 Additional Domain Names Used by Iran's Islamic Revolutionary Guard Corps to Further a Global, Covert Influence Campaign," press release, United States Department of Justice, November 4, 2020, https://www.justice.gov/opa/pr/united-states-seizes-27-additional-domain-names-used-iran-s-islamic-revolutionary-guard-corps.

119 Richard Tilley, "The Kremlin's Return to Active Measures," Lawfare, October 20, 2020, https://www.lawfareblog.com/kremlins-return-active-measures.

120 Center of Excellence on Democracy, Human Rights, and Governance, "Disinformation Primer" (United States Agency for International Development, February 20210, 1, https://pdf.usaid.gov/pdf_docs/PA00XFKF.pdf.

121 Elisa Shearer and Amy Mitchell, "News Use across Social Media Platforms in 2020," Pew Research Center, January 12, 2021, https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020.

122 Shearer, "More Than Eight-in-Ten Americans Get News from Digital Devices"; Elisa Shearer, and Katerina Eva Matsa, "News Use across Social Media Platforms 2018," Pew Research Center, August 27, 2020, https://www.pewresearch.org/journalism/2018/09/10/news-use-across-social-media-platforms-2018/#most-social-media-news-consumers-are-concerned-about-inaccuracy-but-many-still-see-benefits.

123 Shearer, "More Than Eight-in-Ten Americans Get News from Digital Devices."

124 Suzanne Spaulding and Eric Goldstein, "Countering Adversary Threats to Democratic Institutions: An Expert Report" (Center for Strategic and International Studies, February 2018), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180214_Spaulding_CounteringAdversaryThreats_Web2.pdf?EzqGtMwOAjQIIH8eRNNoZ10T49OV63lh.

125 Civics Secures Democracy Act of 2021, H.R. 1814, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/1814/actions (House version); Civics Secures Democracy Act, S. 879, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/879 (Senate version)

126 Kimberly Adams, "What Federal Funding for Civics Reveals about American Political Discourse," Marketplace, November 6, 2019, https://www.marketplace.org/2019/11/06/what-federal-funding-for-civics-reveals-about-american-political-discourse.

127 "NAEP Report Card: Civics," The Nation's Report Card, [2019], https://www.nationsreportcard.gov/civics/results/achievement.

128 "Media Literacy Index 2021," Open Society Institute Sofia, March 14, 2021, https://osis.bg/?p=3750&lang=en.

129 Audrey Quicke, "Media Literacy Education in Finland," Australia Institute | Nordic Policy Centre, November 12, 2020, https://www.nordicpolicycentre.org.au/media_literacy_education_in_finland.

130 National Audiovisual Institute, Finnish Ministry of Education, homepage, https://kavi.fi/en; Ministry of Education and Culture, Finnish Government, homepage, https://minedu.fi/en/frontpage.

131 "Finnish Centre for Media Education and Audiovisual Media (MEKU)," United Nations Alliance of Civilizations: Media and Literacy, September 30, 2013, https://milunesco.unaoc.org/mil-organizations/finnish-centre-for-media-education-and-audiovisual-media-meku/.

132 "Media Literacy in Finland: National Media Education Policy" (Ministry of Education and Culture, 2019), https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf.

133 "Welcome to Faktabaari," FaktaBaari homepage, https://faktabaari.fi/in-english/; Emma Charlton, "How Finland Is Fighting Fake News—in the Classroom," World Economic Forum, May 21, 2019, https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom.

134 Quicke, "Media Literacy Education in Finland."

135 Ibid., quoting Jon Henley, "How Finland Starts Its Fight against Fake News in Primary Schools," *The Guardian*, January 29, 2020, https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news.

136 National Defense Authorization Act for Fiscal Year 2020, §5323(c).

137 Daniel Kilman et al., "Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations" (Center for a New American Security, May 2020), 1–36, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Dangerous-Synergies-May-2020-DoS-Proof.pdf?mtime=20200506164642.

138 Gennie Gebhart, Bennett Cyphers, and Kurt Opsahl, "What We Mean When We Say 'Data Portability,'" Electronic Frontier Foundation, September 13, 2018, https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability.

139 Data Transfer Project homepage, https://datatransferproject.dev; Lauren Feiner, "Facebook Calls for Data Portability Laws as It Expands the Types of Info Users Can Transfer to Other Services." CNBC, April 19, 2021, https://www.cnbc.com/2021/04/19/facebook-expands-the-types-of-data-users-can-transfer-to-other-services.html; Mark R. Warner, "Potential Policy Proposals for Regulation of Social

Media and Technology Firms" (August 20, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0048-d-0104-155263.pdf.

140 Shapiro, Thompson, and Wanless, "Research Collaboration on Influence Operations between Industry and Academia."

141 CSC, "Cybersecurity Lessons from the Pandemic," 13.

142 Spaulding and Goldstein, "Countering Adversary Threats to Democratic Institutions," 13.

143 *United States Efforts to Counter Russian Disinformation and Malign Influence: Hearing of the United States House Committee on Appropriations—Subcommittee on State, Foreign Operations, and Related Programs*, 116th Cong. (2019) (statement of Dr. Alina Polyakova), https://www.brookings.edu/wp-content/uploads/2019/07/Alina-Polyakova-House-Appropriations-Testimony-July-10-2019.pdf.

144 House of Commons, Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Final Report* (House of Commons, February 18, 2019), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

145 James Pamment et al., "RESIST: Counter Disinformation Toolkit," Government Communication Service, 2019; updated August 24, 2021, https://gcs.civilservice.gov.uk/publications/resist-counter-disinformation-toolkit/. All descriptions of the toolkit are taken from this webpage, which includes a link to the pamphlet.

146 Amy Watson, "Level of Trust in the Mass Media to Report the News Fully, Accurately, and Fairly among Adults in the United States from 2000 to 2021," Statista, October 13, 2021, https://www.statista.com/statistics/471240/perceived-objectivity-mass-media-usa.

147 Jacob R. Straus, "Foreign Agents Registration Act (FARA): Background and Issues for Congress" (Congressional Research Service, June 30, 2020), https://sgp.fas.org/crs/misc/R46435.pdf.

148 Joshua R. Fattal, "The Justice Department's New, Unprecedented Use of the Foreign Agents Registration Act," Lawfare, December 18, 2019, https://www.lawfareblog.com/justice-departments-new-unprecedented-use-foreign-agents-registration-act.

149 Josh Gerstein, "DOJ Told RT to Register as Foreign Agent Partly Because of Alleged 2016 Election Interference," Politico, December 21, 2017, https://www.politico.com/story/2017/12/21/russia-today-justice-department-foreign-agent-election-interference-312211.

150 "FARA Frequently Asked Questions," United States Department of Justice, n.d., https://www.justice.gov/nsd-fara/frequently-asked-questions#22.

151 Foreign Agents Registration Modernization and Enforcement Act, H.R. 2811, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/2811; Foreign Agents Registration Modernization and Enforcement Act, S.625, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/senate-bill/625. See Straus, "Foreign Agents Registration Act (FARA): Background and Issues for Congress."

152 Straus, "Foreign Agents Registration Act (FARA): Background and Issues for Congress"; Daniel Fried and Alina Polyakova, "Democratic Defense against Disinformation" (Atlantic Council, February 2018), https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf.

153 Disclosing Foreign Influence Act, S.2039, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/senate-bill/2039/text.

154 "Disclosing Foreign Influence Act: Summary of Legislation," Senate Committee on the Judiciary, October 31, 2017, https://www.judiciary.senate.gov/imo/media/doc/FARA,%2010-31-17,%20Disclosing%20Foreign%20Influence%20Act%20-%20Summary.pdf.

155 Chinese Communist Party Influence Transparency Act, H.R.3390, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/3390/text?r=14&s=1.

156 Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996), https://www.govinfo.gov/content/pkg/STATUTE-110/pdf/STATUTE-110-Pg56.pdf#page=1.

157 "The Public and Broadcasting," Federal Communications Commission, September 2021, https://www.fcc.gov/media/radio/public-and-broadcasting.

158 "United States–Based Foreign Media Outlets," Federal Communications Commission, September 10, 2021, https://www.fcc.gov/united-states-based-foreign-media-outlets.

159 "FCC Commences 2018 Quadrennial Review of Media Ownership Rules," Federal Communications Commission, December 13, 2018, https://www.fcc.gov/document/fcc-commences-2018-quadrennial-review-media-ownership-rules-0.

160 Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2 vols. (Washington, D.C.: U.S. Department of Justice, March 2019), 1:4, https://www.justice.gov/archives/sco/file/1373816/download.

161 Ruane, "Freedom of Speech and Press: Exceptions to the First Amendment."

COMMISSIONERS

CO-CHAIRMEN

Angus S. King Jr., U.S. Senator for Maine

Michael "Mike" J. Gallagher, U.S. Representative for Wisconsin's 8th District

COMMISSIONERS

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Thomas A. "Tom" Fanning, Chairman, President, and Chief Executive Officer of Southern Company

James R. "Jim" Langevin, U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Benjamin E. "Ben" Sasse, U.S. Senator for Nebraska

Suzanne E. Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

STAFF

STAFF
Mark Montgomery
Deb Grays
Laura Bate
Erica Borghard
Tasha Jhangiani
Robert Morgus

WHITE PAPER LEAD WRITERS
Robert Morgus
Natalie Thompson

SENIOR ADVISORS
Tatyana Bolton
Benjamin Jensen
Shawn Lonergan
Brandon Valeriano

LEGAL ADVISORS
Stefan Wolfe, General Counsel
David Simon, Chief Counsel for Cybersecurity and National Security

PRODUCTION STAFF
Alice Falk, Editor
Laurel Prucha Moran, Graphic Designer


U.S. CYBERSPACE SOLARIUM COMMISSION
E PLURIBUS UNUM