

Combating Russian Disinformation:

The Case for Stepping Up the Fight Online

PAUL M. BARRETT, TARA WADHWA, AND DOROTHÉE BAUMANN-PAULY

 **NYU | STERN**

Center for Business
and Human Rights

July 2018

Contents

| | |
|---|----|
| Executive Summary | 1 |
| 1. Introduction | 3 |
| 2. ‘Active Measures’ for the Internet Era | 5 |
| 3. Everyday Disinformation in the U.S. | 9 |
| 4. Russian Exploits in Europe..... | 11 |
| 5. Responses by Internet Platforms | 13 |
| 6. Responses by Governments | 19 |
| 7. Recommendations | 23 |
| Endnotes..... | 30 |

Acknowledgments

This report benefited from insights we gained at an off-the-record meeting we co-sponsored in Brussels in early June 2018 along with the European office of Microsoft and the Office of the United Nations High Commissioner for Human Rights. About 50 people participated in the meeting, including representatives of the European Union and European Parliament; a range of civil society groups and academics; and representatives of Facebook, Google, Mozilla, and Microsoft. We wish to acknowledge the support of our co-sponsors in organizing the meeting, especially John Frank, Steve Crown, and Michael Karimian at Microsoft. In preparing this report, we also consulted with a range of experts on U.S. government policies, including Richard Stengel, former Undersecretary of State for Public Diplomacy and Public Affairs; Matthew Olsen, former Director of the National Counterterrorism Center; and Reed Hundt, former Chairman of the Federal Communications Commission. We also have benefited from close collaboration with Laura Rosenberger, Director of the Alliance for Securing Democracy and Senior Fellow at the German Marshall Fund; Ian Vandewalker and Lawrence Norden at the Brennan Center for Justice at New York University Law School; and Eileen Donahoe, Executive Director of the Global Digital Policy Incubator at Stanford University’s Center for Democracy, Development, and the Rule of Law. We are grateful for the financial support we have received from Craig Newmark Philanthropies and the John S. and James L. Knight Foundation. Our thanks also go to Gabriel Ng for research assistance.

NYU Stern Center for Business and Human Rights
Leonard N. Stern School of Business
44 West 4th Street, Suite 800
New York, NY 10012
+1 212-998-0261
bhr@stern.nyu.edu
bhr.stern.nyu.edu

© 2018 NYU Stern Center for Business and Human Rights
All rights reserved. This work is licensed under the Creative
Commons Attribution-NonCommercial 4.0 International
License. To view a copy of the license, visit
<http://creativecommons.org/licenses/by-nc/4.0/>.

Executive Summary

“
Russian disinformation
seeks to undermine
confidence in
democratic institutions
and exacerbate schisms
over such issues as
immigration, race,
and religion.
”

Although they have brought many benefits, the Internet’s social media and search platforms have proven vulnerable to political disinformation—false or misleading “facts” intentionally spread to promote deception and discord. No country in recent years has been more prolific with disinformation than Russia. While Moscow has aimed much of its digital deceit at the U.S., it has also targeted Britain, France, Italy, Germany, Spain, Ukraine, and other European countries. In all of these places, the Kremlin’s divisive narratives seek to undermine confidence in democratic institutions and exacerbate schisms over such issues as immigration, race, and religion.

This report focuses on the particular dangers posed by Russian political disinformation and makes recommendations to governments and Internet platforms like Facebook, Twitter, and Google on how to address these and future threats. The Russian disinformation campaign deserves special attention because it is part of a broader Kremlin strategy to disrupt democracy in the U.S. and Europe. It shows the scale and influence a sovereign state can have promoting disinformation online. It also reveals the governance gaps that currently exist between the platforms and governments in addressing these challenges. Although our recommendations concentrate on the Russian problem, they also suggest an adaptable model for use against other antagonists as they emerge.

The expectation that Moscow will meddle in the 2018 mid-term U.S. elections and 2019 European Parliamentary elections adds urgency to our call for greater attention to Russian disinformation. But this problem goes far beyond interference with elections. Russian-linked trolls and bot accounts are now active on a continual basis in the U.S. and Europe, attempting to intensify conflict over subjects ranging from American school shootings to the cohesiveness of the European Union.

The major platform companies have taken a number of constructive steps in response to Russian disinformation, but they have not gone nearly far enough.

At least two factors may contribute to this hesitancy. First, addressing disinformation thoroughly would require the platforms to reconsider the advertising-based business model that undergirds the Internet industry. Few, if any, platform executives want to go down that path. Second, some inside these companies may fear that moving aggressively against disinformation spread by Russians or other specific parties could erode the crucial legal shield that protects Internet companies against lawsuits over content on their sites.

Governments can respond to Russian disinformation in several ways. One is content regulation: laws that require Internet platforms to block or take down misleading or offensive material, with the threat of pecuniary punishment for failure to do so. In our view, such restrictions on content pose an immediate threat to the basic human right of free speech—and we therefore oppose this approach. But governments can play legitimate roles in response to disinformation. These include enacting regulation that steers clear of content constraints, gathering intelligence and conducting analysis to bolster executive-branch actions, and educating the public to encourage critical thinking by Internet users. Given these options, the U.S. has responded haltingly, while European governments are moving more forcefully, in some ways that are promising and others that are troubling.

Executive Summary: Recommendations

To the Internet Platforms

Create specialized Russian-focused teams

Staffed with experts on Russian language, culture, and Internet practices, these teams would be integrated into each company's existing efforts to address disinformation. As threats from other sources emerge, this model could be applied to them as well.

Realign corporate structure

Beyond creating a Russia team, the companies should elevate and enhance their policy groups to prioritize efforts to address thorny policy questions.

Develop next-generation artificial intelligence

The platforms need to prepare now for combating more potent methods of spreading disinformation, including “deep fake” technology.

Expand third-party fact-checking initiatives

Partnerships with outside organizations devoted to flagging false information are a necessary, if not sufficient, response to Russian disinformation.

Increase industry-wide cooperation

The platforms already collaborate to fight child pornography and terrorist incitement; they should do so for disinformation, too.

De-rank and block suspicious content

Companies can design algorithms to push disinformation down in search results, and familiar verification technology can block automated bots.

Support transparency legislation

Voluntary measures are not enough. The tech industry should lobby for a provision that requires disclosure of buyers of political advertising.

Rethink online business model

Aspects of the current advertising-driven model are producing unintended and problematic consequences. “Whitelisting” websites for advertisers would be a step in the right direction.

To Governments

Make bold public statements

Senior U.S. officials should emulate the sort of public defiance and determination given voice by British Prime Minister Theresa May.

Form new governmental bodies

In the U.S., disinformation deserves the full attention of a new branch of the National Security Council. In Europe, a joint task force between the EU and NATO would help.

Strengthen existing agencies

The U.S. State Department's Global Engagement Center needs resources and direction. A variety of European centers likewise require better leadership and coordination.

Improve information sharing

More cross-pollination among government, the tech industry, and civil society would improve the odds that all will do a better job confronting Russian disinformation.

Increase Russia sanctions

Both Washington and the EU ought to toughen economic sanctions against Russia, ignoring populist calls in Europe to roll back the punishments.

Enact disclosure legislation

The U.S. needs a law mandating disclosure of sources of online political advertising, and the EU should move in the same direction.

Avoid overbroad legislation

Germany's new “hate speech” law, containing draconian financial punishments, could lead to platforms overcompensating and squelching free speech.

1. Introduction

“
We are on the verge
of having something
in the information
area, which will
allow us to talk to the
Americans as equals.

– Russian cyber official
Andrey Krutskikh,
February 2016

”

The Internet, and in particular, social media, increasingly shape people's view of the world. Two-thirds of Americans say they get at least some of their news from sites such as Facebook and Twitter.¹ Beyond keeping users up to date on current events, social media sites offer vital tools to communicate about political and social activity. Recently in the U.S., the #MeToo anti-harassment movement, #NeverAgain gun-control campaign, and #SupportOurTroops call to patriotism have gained momentum as a result of coordination via social media.

But social media platforms have also proven vulnerable to political disinformation—false or misleading “facts” intentionally spread to promote deception and discord. No country in recent years has been more prolific with disinformation than Russia. While Moscow has aimed much of its digital deceit at the U.S., it has also targeted Britain, France, Italy, Germany, Spain, Ukraine, and other European countries. The Russians deploy large numbers of trolls, or individuals sometimes using fake identities to spew inflammatory messages meant to spark online conflict, and swarms of accounts automated to mimic the actions of people, known as bots. These messengers, operating in coordinated networks and sometimes using the platforms' advertising tools, spread divisive narratives that seek to undermine confidence in democratic institutions and exacerbate schisms over such issues as immigration, race, and religion.

Taking advantage of the anonymity available online, President Vladimir Putin coyly denies Kremlin involvement in this corrosive activity. But Moscow's ambitions are not really a secret. In February 2016, a senior Russian government cyber official named Andrey Krutskikh gave a revealing

speech to a Russian information warfare conference. Krutskikh, a Putin adviser, compared his country's newly attained digital capabilities to the atomic bomb the Soviet Union successfully tested for the first time in 1949. Nuclear parity forced Washington to respect Moscow, he said, and history would repeat itself: “We are on the verge of having something in the information area, which will allow us to talk to the Americans as equals.”²

As Krutskikh hinted, the Putin government and some of its proxies carried out what U.S. intelligence agencies have called “an influence campaign” aimed at the 2016 U.S. presidential election and designed “to undermine public faith in the U.S. democratic process.” In addition to nefarious activities by Russian hackers, trolls, and bots, the intelligence agencies cited RT (formerly Russia Today) and Sputnik, describing the two Kremlin-funded news outlets as integral parts of “Russia's state-run propaganda machine.”³ Special prosecutor Robert Mueller's February 2018 indictment of 13 Russian nationals provided more detail on how operatives from the Kremlin-affiliated Internet Research Agency used sham Facebook, Instagram, and Twitter accounts to stir



The Russian disinformation problem goes far beyond elections. Russian-linked trolls and bots continually attempt to intensify conflict over issues ranging from American school shootings to the cohesiveness of the European Union.



discord over injustice against black Americans, white resentment of Latino and Muslim immigrants, and other combustible issues.⁴

Five months later, as we were finishing this report, Mueller elaborated on the hacking part of the Russian attack. A July 2018 indictment accused 12 Russian military intelligence officers of pursuing a vigorous subterfuge operation aimed at undermining the campaign of Hillary Clinton.

In November 2017, our Center published a [report](#), entitled “Harmful Content,” calling on Google, Facebook, and Twitter to take greater responsibility for countering digital material that is detrimental to democracy.⁵ This new paper focuses on the particular dangers posed by Russian political disinformation and makes recommendations to the Internet platforms and governments on how to address these threats. The Russian disinformation campaign deserves special attention because it is part of a broader Kremlin strategy to disrupt democracy in the U.S. and Europe.

Other governments, including those of North Korea and China, have employed hostile tactics online. In countries such

as Myanmar, Sri Lanka, and Egypt, governments have used social media networks to promote propaganda and sow internal division. These are all serious problems and deserve careful attention. This report focuses on the Kremlin’s activities because it has devoted significant resources to fostering disinformation intentionally aimed at fomenting divisions within democratic societies, especially in the West. Accordingly, our recommendations concentrate on the Russian onslaught, although they also suggest an adaptable model for use against other antagonists as they emerge.

Facebook, the largest social media platform with 2.2 billion monthly users, has understandably received the most public attention as the Russians’ preferred vehicle for disinformation. But as we discuss in Section 2, the Russians operate across a variety of platforms, taking advantage of the web’s echo-chamber effect to amplify acrimonious messages. We will look broadly at the social media industry—and to a more limited degree at Google, operator of the premier search engine. (Topics beyond the scope of this report include the fallout from the data breach that led to the harvesting of 87 million Facebook users’ personal information by voter-profiling firm Cambridge Analytica;⁶ Facebook’s sharing of mass user data with device makers, including major Chinese companies;⁷ and the impact of Europe’s new privacy law, the General Data Protection Regulation.)

The expectation of Russian meddling in the 2018 mid-term U.S. elections and 2019 European Parliamentary elections adds urgency to our call for greater attention to Russian disinformation. But as we consider in Sections 3 and 4, this problem goes far beyond interference with elections. Russian-linked trolls and bots are now active on a continual basis in the U.S. and Europe, attempting to intensify conflict over issues ranging from American school shootings to the cohesiveness of the European Union.

In our judgment, the major platform companies have taken only limited steps in response to Russian disinformation. We examine two of the possible reasons for this in Section 5. First, we point out that addressing disinformation thoroughly would require reexamining the advertising-based business model that undergirds the Internet industry. Few, if any, platform executives want to go down that path. Second, we consider why these same executives may resist moving aggressively against Russian disinformation, as it could erode the crucial legal shield that protects Internet companies against lawsuits over content on their sites. In Section 6, we turn to government responses to the Russian threat.

Our recommendations appear in Section 7, where we argue that the major platforms need to institute proactive company-wide policies befitting the nature and scale of the Russian threat. The first step would be to announce publicly the adoption of such policies and the formation of a substantial corporate team dedicated to countering disinformation disseminated by the Russians and any other bad actors that follow their example. While the platforms lately have moved to limit the reach of Russian propaganda, their reform measures too often seem circumscribed or ambiguous. What is called for instead is clarity and unequivocal action that goes beyond what is required by law and focuses broadly on political disinformation generated by the Russian government and its affiliates.

2. ‘Active Measures’ for the Internet Era

“
Putin’s deep commitment to information-based combat reportedly stems in part from his resentment of Western accusations that he rigs elections. He has announced his intention to ‘break the Anglo-Saxon monopoly on the global information streams.’
”

During his long tenure as Russia’s leader, Vladimir Putin has sought to restore the [global reach](#) enjoyed by the former Soviet Union. His tools have included diplomacy, military action, leverage of Russia’s oil and gas, cyber-attacks, and financial support for foreign election campaigns. The objects of his attention have ranged from Ukraine to the U.S. to Syria. In all of these countries, his operatives have updated a Cold War-era technique known as “active measures,” meaning covert attempts to shape public debate and tilt politics in favor of Russia’s interests. Spreading disinformation (*dezinformatsiya*) is one type of active measure. Putin and his lieutenants grasped years ago that digital technology transformed analog disinformation into a speedier, lower-cost, more pervasive method of influence.⁸

Beginning close to home, Putin experimented with updated active measures in Estonia in 2007. Moscow fomented rioting among members of Estonia’s large Russian-speaking minority and then executed a digital attack that temporarily shut down the former Soviet republic’s government and banks. The following year, Russia relied on a mix of conventional and cyber-attacks during a war against Georgia, another former Soviet republic. Methods pioneered in Estonia and Georgia evolved into elements of the “[Gerasimov doctrine](#),” named for General Valery Gerasimov, the chief of the general staff of the Russian military. In writings and speeches, Gerasimov has described Russia’s preference for “hybrid” forms of conflict where “the information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy.”⁹

Putin’s deep [commitment](#) to information-based combat reportedly stems in part from his resentment of Western accusations that he rigs elections and in part from an unsubstantiated fear that the U.S. supports elements in Russian

society seeking to overthrow his regime. According to multiple accounts, he was particularly incensed by what he perceived as Western-instigated protests against suspect parliamentary elections in Russia in 2011. During a subsequent visit to the offices of RT, he announced his intention to “break the Anglo-Saxon monopoly on the global information streams.”¹⁰

In 2014, Putin stepped up his bullying of nations that had once been part of the U.S.S.R. Russia forcibly annexed Ukraine’s Crimea region and backed pro-Russian separatist insurgents in eastern Ukraine. These audacious actions were accompanied by [disinformation](#) disseminated via Facebook and its much smaller Russian equivalent, VKontakte. In a precursor to interference in Western Europe and the U.S., operatives with the Russian military intelligence agency known as the GRU set up fake social media accounts to simulate popular Ukrainian hostility to the pro-Western government in Kiev. The same year, pro-Russian hackers attacked Ukrainian election computers in a narrowly averted bid to hand the presidency to a fringe ultra-right party.¹¹



The Russian disinformation attack in 2016 caught the U.S. unprepared. No single government agency understood the entirety of what was going on or assumed responsibility for addressing it. The major social media platforms minimized the severity of the onslaught until that strategy became infeasible.



While Russia shows no appetite for confronting the U.S. on the conventional battlefield, it has demonstrated its intention to apply digital aspects of the Gerasimov doctrine in the West. Beginning in 2015, Russian hackers **targeted** American and European nuclear power plants and water and electric systems, according to U.S. officials. By 2017, the intruders potentially could have sabotaged vital infrastructure in the West, although they did not do so—this time.¹²

It is in this context of the Russian drive for greater global influence that the Internet platforms and the U.S. and its allies ought to consider Moscow's disinformation campaigns. The 2016 U.S. election story is worth briefly reviewing here to underscore the Russians' ambition and dexterity in this regard. As Clint Watts, a disinformation expert affiliated with the Center for Cyber and Homeland Security at George Washington University, has **put it**: "Within the Kremlin's playbook, each social media platform serves a function,

a role in an interlocking social media ecosystem where Russia infiltrates, engages, influences, and manipulates targeted American audiences."¹³

In one of Russia's main coups in 2016, hackers **penetrated** email accounts of the Democratic National Committee and Hillary Clinton's campaign chairman, John Podesta. WikiLeaks and a Russian-affiliated site called DCLeaks then publicly posted the stolen emails, which divided and distracted the Clinton camp. A suspected Russian GRU front-persona known as Guccifer 2.0 used Twitter to draw the mainstream media's attention to the stolen messages.¹⁴

On another track, the Internet Research Agency (IRA), which employed hundreds of people in St. Petersburg, Russia, carried out a malign social media **operation** allegedly financed by a Putin crony and oligarch named Yevgeny Prigozhin. IRA employees used fake personas to set up accounts on Facebook, Instagram (which Facebook owns), Twitter, and YouTube (which Google owns). The IRA operatives favored Facebook and Instagram for establishing sham activist accounts meant to heighten divisions over immigration, Islam, and police treatment of African Americans. In some cases, IRA employees bought Facebook and Google advertisements to target particular users for incendiary messages. "Ohio Wants Hillary 4 Prison," one ad stated. "Hillary is a Satan," said another. The Russians also purchased Facebook ads to promote anti-Clinton and pro-Donald Trump rallies they organized in Florida, Pennsylvania, and elsewhere. Internally, IRA operatives described their mission as conducting "information warfare against the United States of America."¹⁵

The attack caught the U.S. unprepared. No single government agency understood the entirety of what was going on or assumed responsibility for addressing it. Out of fear of appearing to try to influence the election, the Obama administration hesitated to unilaterally

disclose what it knew. And Republicans in Congress refused to cooperate with a White House proposal to release information on a bipartisan basis.¹⁶ In Silicon Valley, the major social media platforms minimized the severity of the onslaught until that strategy became infeasible.¹⁷

Various Platforms, Diverse Purposes

Between just Facebook and Instagram, nearly 150 million Americans were exposed to Russian disinformation, both via purchased ads and non-paid "organic" traffic. That number comes from Facebook, and it may **understate** the problem. Content from just six IRA-created Facebook pages—Blacktivist, United Muslims of America, Being Patriotic, Heart of Texas, Secured Borders, and LGBT United—was widely shared online, potentially exposing millions of additional users, according to a study by Jonathan Albright, research director of the Tow Center for Digital Journalism at Columbia University.¹⁸

The IRA used various platforms for diverse purposes. It exploited Instagram, a photo- and video-sharing site that boasts 800 million monthly users, for some patently offensive stratagems. The fake Instagram account Woke Blacks, for example, posted a voter-suppression message aimed at African Americans: "Hype and hatred of Trump is misleading the people and forcing Blacks to vote Hillary. We cannot resort to the lesser of two devils. Then we'd surely be better off without voting AT ALL."¹⁹ Albright has called Instagram "a major distributor and redistributor of IRA propaganda that's at the very least on par with Twitter."²⁰

Twitter indicated the extent to which the Russians manipulated its site when it reported that it had shut down more than 3,800 IRA-linked trolling accounts and another 50,300 automated bot accounts. Today, Russian disinformation continues to circulate on Twitter, according to the **Alliance for Securing Democracy**, an initiative housed at the German Marshall Fund.

The Alliance tracks some 600 Twitter accounts with Russian ties and displays their activity on a dashboard called [Hamilton 68](#)—a reference to one of the Federalist Papers attributed to Alexander Hamilton, who discussed the danger of foreign interference in elections. We have relied on Hamilton 68 findings in this report. The content in which the Hamilton 68 network of trolls and bots traffics “is not necessarily produced or created by Russian government operatives, although that is sometimes the case,” the Alliance explains on its website. “Instead, the network often opportunistically amplifies content created by third parties not directly linked to Russia. Common themes include attacks on the U.S. and Europe, conspiracy theories, and disinformation.”²¹ The accounts monitored by Hamilton 68 illustrate how Twitter empowers Russian-linked trolls and bots to react swiftly to controversies chronicled by traditional media. And information flows in both directions: During the 2016 campaign, many mainstream media organizations, including *USA Today*, *The Washington Post*, and *The New York Times*, on occasion [cited](#) Twitter accounts operated by the IRA as evidence of partisan polarization—and thereby inadvertently carried water for Russian disinformation artists.²²

YouTube has served yet another function for the Russians. The Internet’s top site for video sharing, with 1.5 billion users, it has offered RT and Sputnik a ready platform for their Kremlin-financed propaganda. RT has 2.7 million [subscribers](#) on YouTube—more than BBC News, MSNBC, and Fox News.²³ By means of video packaged for YouTube, the government-funded news service overtly participated in the 2016 denigration of Hillary Clinton. RT illustrates how Russian sources of disinformation exploit the designs and business models of the platforms. It uploads videos to YouTube frequently, sprinkling in depictions of disaster—plane crashes, tsunamis, a meteor strike—to earn numerous “likes” and longer watch times from viewers. These

indications of viewer engagement help YouTube sell advertising. At the same time, YouTube automatically rewards RT with better placement among search results and recommendations.²⁴

The Russians have surfaced on other sites, as well. Tumblr, a popular multimedia blogging platform, announced in March 2018 that it had deleted 84 IRA-linked accounts that targeted

specific audiences, including minority groups. Accounts with names such as Ghetta Blasta and Hustle in a Trap tried to attract black users, who were fed anti-Clinton conspiracy theories and invited to phony protests.²⁵ Reddit, another heavily trafficked site that hosts often-contentious forums, said in April 2018 that it purged nearly 1,000 accounts tied to the IRA.

Profile of a Russian Troll Factory

The Internet Research Agency

Special Counsel Robert Mueller has alleged that IRA operatives described their mission as conducting “information warfare against the United States of America.” Here are some basic facts and figures about the organization:

| | |
|---|---|
| Founded | In St. Petersburg in 2014 |
| Financing | Yevgeny Prigozhin, an oligarch and Putin crony |
| Number of employees | Hundreds, of whom more than 80 worked on U.S. interference |
| Preferred social media platforms for disinformation | Facebook, Instagram, YouTube, and Twitter |
| Selected phony Facebook pages designed to sow social discord | Being Patriotic, Blacktivist, United Muslims of America, Army of Jesus, Heart of Texas, LGBT United |
| Favored presidential candidates | Donald Trump, Bernie Sanders |
| Disfavored presidential candidates | Hillary Clinton, Ted Cruz, and Marco Rubio |
| Sample online advertisement | “Donald wants to defeat terrorism... Hillary wants to sponsor it” |
| Wrapped up operations | Late 2016 |
| Names of possible successor troll factories | Glavset and Teka |

Sources: Mueller indictment (United States of America v. Internet Research Agency LLC et al., filed February 16, 2018); *WIRED*; and *The Guardian*.

Ben Nimmo, a senior fellow at the Atlantic Council’s [Digital Forensic Research Lab](#), has noted that the Reddit accounts “spread the Kremlin’s preferred narratives to users who may have missed them elsewhere, working harmoniously with Russian troll accounts on other platforms to spread the message of disharmony.”²⁶








While Russian disinformation travels primarily via social media, it also crops up in response to news searches. Google has faced criticism for including RT and Sputnik in its Google News service, a compilation of supposedly

legitimate news sites. In November 2017, [Eric Schmidt](#), Google’s former executive chairman, said publicly that Google ought to be able to combat Russian disinformation, since it is based on “amplification around a message” that is “repetitive, exploitative, false, [or] likely to be weaponized.” Referring to RT and Sputnik, he added: “My own view is that these patterns can be detected and that they can be taken down or deprioritized.”²⁷ In Section 5, we will see that it is not clear whether Google has deprioritized RT and Sputnik.

As this brisk tour of the Russian disinformation playbook illustrates, “Moscow’s exploitation of social media platforms is expansive, pervasive, and ever-growing.”²⁸ This activity has received attention primarily in connection with the 2016 U.S. presidential election. Equally importantly, it has become a divisive and routine aspect of life in the U.S. and Europe, as the next two sections illustrate.

Diverse Homes for Russian Disinformation

Trolls and bots have used various Internet platforms for a range of aims.

| Platform | Purpose |
|--|---|
|  Facebook | Create thematic pages on divisive themes—for example, Blacktivist, Secured Borders, and Army of Jesus—some of which grew to have hundreds of thousands of online followers each |
|  Instagram | Generate fake accounts, such as Woke Blacks, which urged African Americans not to vote at all, rather than support Hillary Clinton |
|  Twitter | React quickly to events chronicled by traditional media; on occasion, major publications have inadvertently cited Russian tweets as evidence of partisan polarization |
|  YouTube | Serve as a venue for videos from RT and Sputnik, Kremlin-financed news outlets described by U.S. intelligence agencies as integral parts of “Russia’s state-run propaganda machine” |
|  Reddit | Place false accounts said to “spread the Kremlin’s preferred narratives to users who may have missed them elsewhere” |
|  Tumblr | |
|  Google | Provide discordant stories—for example, from RT and Sputnik—which turn up in news searches; it is unclear whether Google deprioritizes disinformation from such sources |

Sources: Tow Center for Digital Journalism, Alliance for Securing Democracy, Digital Forensic Research Lab.

3. Everyday Disinformation in the U.S.

“
Despite Twitter's efforts to remove inauthentic accounts, coordinated troll and bot networks continue to enable individuals or small groups of people to create the illusion of surging trends in public opinion.
”

The current wave of Russian disinformation in the U.S. began with preliminary forays as early as 2014. In that year, numerous troll and bot accounts linked to Russia mounted a campaign about a made-up chemical plant explosion in Louisiana. The effort, organized around the hashtag #ColumbianChemicals, included a multi-platform [hoax](#) using Facebook, Twitter, and Wikipedia. Most of the social media accounts that promoted #ColumbianChemicals had existed since the summer of 2013 and employed tweet-generating services such as Bronislav and Rosislav, which are hosted by an entity with ties to the Internet Research Agency. The Russian network continued to operate in 2015, focusing on such themes as #PhosphorusDisaster (falsely alleging water contamination in Idaho) and #IndianaFedUp (playing on anti-gay sentiment).²⁹

Since the Russian meddling in the 2016 U.S. presidential election, disinformation activity in the U.S. has continued apace. The IRA has receded, but other Russian companies with names like Glavset and Tekka reportedly have picked up the trolling slack.³⁰ Despite Twitter's efforts to remove inauthentic accounts, coordinated troll and bot networks continue to enable individuals or small groups of people to create the illusion of surging trends in public opinion.

Before Trump even took office, Russian-affiliated trolls and bots flooded social media sites to torpedo the potential selection of Mitt Romney as Secretary of State. The #NeverRomney Twitter campaign attacked Romney as a “globalist puppet.” A Facebook group called Being Patriotic promoted an anti-Romney rally outside Trump Tower in Manhattan. “We did NOT fight this hard to get backstabbing Romney as Secretary of State!” the phony group said. Trump ultimately chose Rex Tillerson, a former chief executive

of ExxonMobil who boasted of his “very close relationship” with Putin. Trump removed Tillerson from office in March 2018.³¹

By 2017, Russian-linked Twitter trolls and bots were swarming around all manner of U.S. controversies. During the 2017-2018 National Football League season, the digital horde [descended](#) on the debate over NFL players protesting police brutality by taking a knee during the national anthem. As Trump used Twitter to condemn the sideline demonstrations, Russian-affiliated Twitter accounts advocated on both sides of the issue, promoting hashtags #standfourantheam and #takeaknee.³²

In early 2018, Twitter accounts with Russian ties helped popularize [#releasethememo](#), which referred to a secret House Republican document accusing the FBI and Justice Department of abusing their authority to obtain a warrant to spy on a former Trump campaign adviser. The president

eventually did release the memo, which helped exacerbate the schism between the White House and career federal law enforcement officials.³³

Within hours of the February 14, 2018, mass shooting at a high school in Parkland, Florida, Russian-linked accounts [spewed](#) venom on both sides of the gun-control debate. Earlier in the day, many of the same accounts were tweeting about the Mueller investigation into Trump and Russia. The furor over the Parkland massacre did not end with the Twitter activity. YouTube videos and thousands of Facebook posts, some suspected of having Russian origins, spread the deliberately dishonest notion that students who survived the bloodshed were paid actors participating in a hoax.³⁴

Violence and racial distrust have served as abiding themes for the Russian-linked social media throng. As a man-hunt unfolded in the wake of an initially mysterious string of bombings in Austin, Texas, in March 2018, the bots pushed [phony narratives](#). According to one, the media were not covering the deadly attacks because the first three victims were not white; another held that law enforcement did not take the situation seriously until there was a white victim.³⁵

U.S. foreign affairs also stimulate Russia's disinformation troops, both human and automated. In April 2018, the Russian-backed Assad regime in Syria used chemical weapons in attacks that killed dozens of Syrian civilians in the city of Douma. In reaction, Russian-linked Twitter accounts strenuously [attempted](#) to seed doubts about Assad's culpability. They portrayed the deadly onslaught as a false-flag operation engineered by the U.S. Twitter trolls went so far as to float the dark fantasy that Syrian children were taught to fake injuries from chemical weapons.³⁶



Immediately after the Parkland, Florida, school shooting in February 2018, Russian-linked trolls and bots turned their attention away from the Mueller investigation of Trump and Russia to spread false stories accusing student survivors of being paid actors participating in a hoax.



4. Russian Exploits in Europe



Coordinated social media posts widely attributed to Russia tried to persuade Swedes that if their country drew closer to NATO, the military alliance would secretly stockpile nuclear weapons in Sweden and even attack Russia from Swedish soil.



While Russian disinformation aimed at the U.S. has become common, Europe has been hit even harder and for much longer. Methods introduced in Estonia, Georgia, and Ukraine have migrated west to France, Germany, Italy, Spain, and the U.K. In each instance, updated active measures have sought to undermine public confidence in national and/or pan-European institutions.³⁷

The “Lisa” case in Germany exemplified Russia’s multifaceted digital-attack strategy. In 2016, the German-language branch of RT and other Russian state-supported media broadcast reports into Germany of a 13-year-old Russian-German girl who purportedly had been sexually assaulted by a group of Middle Eastern immigrants. Facebook and Twitter posts reinforced the anti-immigrant tale even after the German police determined it was false. Nationalist furor ensued, spawning demonstrations against German Chancellor Angela Merkel. The disinformation ultimately was traced back to a Facebook group called Anonymous Kollektiv and an anti-refugee website called Asylterror, which had Russian ties.³⁸

The same year as the Lisa affair, Sweden faced a disinformation blitz widely attributed to Russia. Coordinated social media posts contested a proposed Swedish military partnership with the North Atlantic Treaty Organization. One of the durable motifs of Russia’s European disinformation has been the threat NATO supposedly poses to Russian security and sovereignty. Russian trolls and bots try to open fissures among NATO members and between the organization and friendly non-members. If Sweden moved closer to NATO, the social media campaign falsely claimed,

the military alliance would secretly stockpile nuclear weapons in Sweden and even attack Russia from Swedish soil. The Swedes, like their neighbors in Denmark, Finland, and Norway, generally display a high level of resistance to Russian disinformation. Sweden agreed in May 2016 to allow NATO to operate more easily on Swedish territory.³⁹

Often it is difficult to find Moscow’s fingerprints on disinformation because of the use of “cutouts,” or intermediaries. In the Netherlands in 2016, a group described as consisting of Ukrainian emigres used social media to oppose a proposed European Union trade pact with Ukraine. The opponents portrayed the pro-Western Ukrainian government as murderous, corrupt, and unworthy of Dutch support. It turned out that the most active members of the “Ukrainian” team were actually from Russia or from breakaway regions of Ukraine run by Russian-supported separatists. In a referendum, the Dutch voted down the EU-Ukraine agreement.⁴⁰

Russian involvement in French and Spanish politics illustrates Putin’s goal of promoting nationalist and separatist movements that threaten stability in

Western Europe. In the 2017 French presidential election, Putin publicly backed Marine Le Pen, the far-right National Front candidate whose party has received Russian financing. Secretly, a hacking effort attributed by some cyber-security experts to Russians with ties to the GRU penetrated the campaign computers of political centrist Emmanuel Macron. The intruders [stole](#) thousands of emails and other documents. They interspersed the pilfered material with falsified, seemingly incriminating items and released the mix online. Right-wing activists in the U.S. and France then drew attention to the data dump by means of a vigorous #MacronLeaks campaign on Twitter and Facebook. Nevertheless, Macron handily defeated Le Pen in May 2017.⁴¹

Five months later, Catalan secessionists in Spain received Russian digital support for an independence referendum opposed by the Spanish government, the EU, and the U.S. Russian-linked Twitter bots that normally amplify messages backing the Kremlin or Ukrainian insurgents switched their

“
Moscow went after a pro-Western presidential candidate in the Czech Republic by spreading false online rumors that he belonged to a secret globalist society, advocated mass Muslim immigration, and was a pedophile.
”

focus to [recirculating](#) pro-separatist tweets by Julian Assange. The WikiLeaks founder condemned the Madrid government for “crushing democracy” and acting “like a banana monarchy.” Sputnik’s Spanish-language service augmented the Russian Twitter-based support for secession. The referendum passed overwhelmingly, but Catalonia remains in a political deadlock with Madrid.⁴²

What appeared to be Russian disinformation polluted presidential elections in the Czech Republic in January 2018. The incumbent, Milos Zeman, a defender of Russia’s annexation of Crimea and skeptic of Czech membership in NATO and the EU, faced a pro-Western opponent, Jiri Drahos. A vicious online campaign accused Drahos of belonging to a secret globalist society, advocating mass Muslim immigration, and being a pedophile. Drahos was quoted as saying it was “logical” to assume that the [assault](#) on his record and character emanated from “the Russian secret service and related organizations.” Zeman defeated Drahos in what the editorial board of *The Washington Post* called “one more warning that Moscow can be expected to target the upcoming U.S. midterms” in 2018.⁴³

There is [evidence](#) that Russian social media operatives have meddled in British voting, including the 2016 Brexit referendum.⁴⁴ A dramatic and more recent example from the U.K. involved the misdirection that swirled around the March 2018 poisoning of Sergei Skripal and his daughter. The various alternative realities proposed by the Russian foreign ministry, state media, and online trolls included that it was the British who tried to assassinate the former double agent as a way of fomenting hostility toward Moscow, that Ukraine tried to kill the Skripals to tarnish the Putin regime, or that the daughter’s fiancé and his mother attempted the killing out of jealousy. The contradictory nature of

such disinformation not only hinders comprehension of the incident at hand; it also makes onlookers distrust the very notion of truth.⁴⁵

Fomenting confusion often works. The Digital Forensic Research Lab analyzed the most-shared articles on social media about the Skripal poisoning and found that content from Kremlin-owned and pro-Kremlin media outlets far outranked mainstream and independent media on audience-engagement statistics. “The low-cost, high-impact nature of social media makes it a useful medium for the Kremlin’s war of narratives,” the Lab observed, “and as social media data suggests, Russia is winning.”⁴⁶

The Kremlin enjoyed another success in March 2018 in Italy. In the build-up to national elections, the Italian-language arm of Sputnik provided a steady diet of anti-immigrant stories subsequently [re-gurgitated](#) by thousands of social media accounts. As distilled by the newspaper *El País*, the digital campaign depicted an Italy “invaded by refugees who are to blame for unemployment and inflation, in the midst of a crisis made only worse by the passive attitude of pro-European politicians.”⁴⁷ Russia’s favored parties, the right-wing League and the populist Five Star Movement, prevailed and formed a government with pro-Moscow leanings.

5. Responses by Internet Platforms

“
Taking a deeper look at the Russia problem could reveal disconcerting cracks in the foundation of the platforms’ businesses—namely the heavy reliance on content that appeals to negative emotions such as fear and anger.”

”

In the face of the Russian threat, the major Internet platforms have made certain adjustments. But they have not elevated the problem to an urgent priority; nor have they treated it as a discrete challenge deserving targeted attention. This hesitation seems odd in light of industry leaders’ own [rhetoric](#). “There are people in Russia whose job it is to exploit our systems and other Internet systems,” Facebook Chief Executive Mark Zuckerberg told a Senate committee in April 2018. “So this is an arms race. They are going to keep getting better.”⁴⁸

If that is the case—and we believe it is—Facebook’s incremental and non-specific responses to the Russian threat seem inadequate, as do the responses of the other major platforms. In this section, we describe measures introduced since the 2016 election, as well as their intrinsic limitations.

Making Political Advertising More Transparent

To their credit, Facebook, Google, and Twitter now are making it more difficult for foreign interlopers to use online advertising to interfere with U.S. elections and politics more generally. All three companies have announced recently that they will require disclosure of purchasers of political advertisements. It appears that the platforms are seeking to preempt legislation introduced in both houses of Congress called the [Honest Ads Act](#). The act, which goes beyond policies the companies have voluntarily adopted, would mandate transparency for political ads online in a fashion similar to already-existing requirements for traditional broadcast and print media. Under the legislation, platforms would have to

disclose who bought political ads, how much they cost, and to what audience they were targeted.⁴⁹

Facebook and Twitter have publicly endorsed the act, but they do not seem to be reinforcing that commitment in their private interactions on Capitol Hill. At one point in early 2018, Facebook reportedly dispatched lobbyists to dissuade senators from moving the Honest Ads Act forward.⁵⁰ As we recommend in Section 7, the companies should actively support a modified version of the Honest Ads Act that would assign enforcement authority to a well-resourced regulatory agency like the Federal Communications Commission. The future of political advertising will be online, where candidates can inexpensively micro-target voters. Establishing the strongest possible regulatory framework will be essential.

As part of their voluntary efforts to thwart foreign interference, Facebook, Google, and Twitter will certify political ad buyers’ identity and physical location in the U.S. Facebook and Twitter will also label political ads. And Facebook says it will verify the identity and location of people who

“
As part of their
laudable voluntary
efforts to thwart
foreign interference,
Facebook, Google,
and Twitter will certify
political ad buyers’
identity and physical
location in the U.S.
”

run popular Facebook pages like those Internet Research Agency employees used to pose as Americans clashing over political issues.⁵¹

Twitter has moved more directly against overt Russian propaganda, [banning](#) all ads by RT and Sputnik, although allowing the Kremlin-sponsored services to continue to tweet.⁵² Twitter is also launching an online Transparency Center where a user will be able to see information about not only political ads, but all currently running ads. The information will include which ads target the user and how long ads have been running.⁵³

These examples of greater advertising transparency constitute real progress. But they do not get at the heart of the problem of Russian disinformation.

We suspect that one of the reasons the platforms hesitate to address this problem as pressing and distinct is that they fear that doing so would invite greater scrutiny of the algorithms that support their lucrative business models. To understand this possible concern, one has to step back and consider the basics of digital advertising.

Advertising is the engine of Internet commerce. Users get free access to search and social media sites in exchange for tolerating ads and surrendering personal data. Businesses buying ads seek users’ attention and the ability to micro-target them geographically and demographically, based on their data. Platforms provide the content that commands users’ attention. Platforms also sell ad space next to this content and collect the personal data used in micro-targeting.

As currently structured, the Internet advertising business helps create a strikingly hospitable environment for those generating disinformation.

Dipayan Ghosh, a former public policy strategist at Facebook, and Ben Scott, a former policy advisor at the State Department, have [written](#) about how the “form of the advertising technology market perfectly suits the function of disinformation operations. These campaigns often deploy sensational themes and polarizing politics. This content draws and holds consumer attention, which, in turn, generates revenue for Internet-based content.” A successful disinformation campaign, Ghosh and Scott add, “delivers a highly responsive audience that drives forward engagement on the platform and ultimately delivers more revenue for all parties.”⁵⁴ In other words, the contentious nature of Russian disinformation makes it effective and profitable.

Neither Ghosh and Scott, nor we, are suggesting that Internet companies have consciously cultivated Kremlin-directed deceptions. Instead, the point is that from an ad-revenue perspective, there is not much difference between someone pushing retail products and someone else spreading fake messages meant to inflame the electorate. The current model rewards sensational content that attracts and holds users’ attention—as do the platforms that sell advertising space. Thinking seriously about how to discourage or block politically motivated disinformation could open the door to a broader examination of sensational, polarizing content that increases online advertising generally.

Roger McNamee, a digital financier and early investor in Google and Facebook, has also [noted](#) the parallels between disinformation and conventional Internet fare. In the same way that the Russian IRA deployed discordant political and social content, Facebook’s “algorithms maximize engagement by appealing to emotions such as fear

and anger,” McNamee has written. “Facebook groups intensify preexisting beliefs, increasing polarization,” in just the manner the Russians have sought to achieve.⁵⁵

Given the attributes of Internet advertising that McNamee and Ghosh and Scott describe, top executives of the major platforms may have chosen not to take a deeper look at the Russia problem because it could reveal disconcerting cracks in the foundation of their advertising model. In Section 7 we recommend that the platforms nevertheless rethink their advertising policies.

Hiring More Reviewers

The major platforms are hiring more people to look for suspect ads, phony accounts, and dubious content. YouTube has promised a 25% increase to about 10,000 content reviewers. Facebook says that over the course of 2018, it is doubling the size of the staff it assigns to safety and security, to 20,000 people.⁵⁶ In Germany alone, Facebook reportedly employs 1,200 reviewers to help the company comply with a new law that provides for severe financial penalties if a platform fails to swiftly take down “hate speech” or other offensive material.⁵⁷ Twitter, which is much smaller, plans to expand its workforce by up to 15% in 2018, to reach about 3,800 employees, although only some of the additions will relate to “improving the health of the platform.”⁵⁸

Adding moderators, account monitors, and ad reviewers—a step we recommended in our “Harmful Content” report in November 2017⁵⁹—should have a positive effect. These new employees will focus on a wide range of challenges, including hate speech, terrorist recruitment, and spam. We commend the platforms for recognizing that machines alone cannot adequately tackle all of these problems. But we recommend

the assignment of a dedicated subset of the new employees to tasks addressing Russian political disinformation. Facebook, unfortunately, seems to have rejected an internal push for this kind of focused attention.

According to *The New York Times*, Alex Stamos, Facebook’s outgoing chief information security officer unsuccessfully advocated for more public disclosure of Russian interference, as well as for a corporate restructuring to address the Russia issue in a more intensive way. His recommendations reportedly were overruled by more senior executives. The *Times* said that those within the company who blocked Stamos’s approach feared that it would tarnish Facebook’s image and hurt its business. (Stamos denied the *Times* account, saying, “That’s not what happened.” Top management, he added, “supported the investigation and disclosure of our work, and I’m glad we put out what we found.”) Still, in December 2017, Stamos’ day-to-day responsibilities were reassigned to others, and his team was split between the product and infrastructure groups. He is expected to leave the company in the near future.⁶⁰

We urge Facebook, Google, Twitter, and other Internet platforms to publicly recognize Russian disinformation and give it priority attention. Specifically, we recommend that each company create and staff Russian-focused teams that include specialists with Russian-language skills and area expertise. These teams should work with existing units that are addressing disinformation but be explicitly assigned to grapple with hostile Russian activities in all aspects of these businesses. Once the teams have developed internal methods for combating Russian-generated disinformation, they should share their insights with counterparts at other platforms to help develop common approaches to addressing this critically important problem.

Purging Sham Accounts

The Russian-focused teams created within each company should build on a number of useful steps already undertaken. For example, multiple social media platforms—including Facebook, Twitter, Reddit, and Tumblr—have shut down numerous phony accounts to thwart Russian meddling. Facebook says it has closed more than 740 accounts and pages operated by Russian trolls. For a sense of perspective, Facebook said that all told, it removed 583 million fake accounts in the first quarter of 2018 alone.⁶¹

As noted earlier, Twitter has said it took down 3,800 Russian troll accounts and another 50,300 Kremlin-controlled bots. On a daily basis, Twitter says it blocks 523,000 logins from suspicious bot accounts, although only a tiny fraction of those relate to Russia.⁶²

Purging malicious and sham accounts is an essential part of policing an Internet platform. An advantage of creating Russian-focused teams is that they would provide ongoing oversight to address this problem, which is unlikely to recede in the foreseeable future.

Advancing Artificial Intelligence

An essential complement to human reviewers, artificial intelligence (A.I.) will play an increasingly central role in the identification and removal of fake accounts and problematic content. “We’re going to shift increasingly to a method where more of this content is flagged up front by A.I. tools that we develop,” Mark Zuckerberg told Congress during his April 2018 testimony. His company is opening new A.I. labs in Seattle and Pittsburgh after hiring top academic computer scientists.⁶³ We applaud these efforts.

“
Former Google Executive Chairman Eric Schmidt has said that the search engine should be able to de-rank propaganda from RT and Sputnik, meaning that reports from the Russian outlets would be demoted in search results.
”

Engineers build A.I. screening systems by feeding them examples of good content and bad, until the algorithm “learns” to make that distinction on its own. A.I. algorithms can also pick up how to identify fake social media accounts. Zuckerberg testified that Facebook used A.I. to find and take down 30,000 [sham accounts](#), presumably some of them Russian in origin, in the months leading up to the French presidential election in spring of 2017. A.I. also helped Facebook eliminate an unspecified number of fake accounts emanating from Macedonia that tried to interfere with a closely watched special Senate election in Alabama in December 2017, he said. And as a result of A.I., 99% of the terrorism-related content Facebook takes down is eliminated before any user sees it.⁶⁴

Without having access to the analytical framework for these algorithms, it is difficult for us or others outside of the companies to assess how much A.I. can mitigate damage being done by Russian disinformation. As Zuckerberg emphasized, using A.I. to identify violent words and images employed to recruit extremists has proven easier than distinguishing hate speech or Russian disinformation from ordinary political content. That is because A.I. algorithms are sometimes stumped by subtle matters of context. Zuckerberg estimated that it will take five to 10 years before Facebook develops “A.I. tools that can get into some of the nuances.”⁶⁵ In the meantime, the platforms need to deploy Russian-focused internal teams to address these challenges.

Reordering and Annotating Content

Major platforms are reordering and annotating search results and social media posts to help guide users to genuine content and away from fakery. Google [acknowledged](#) in 2017 that its search algorithms sometimes served up

“blatantly misleading, low quality, offensive, or downright false information.” In response, the company says it has fine-tuned its evaluation methods and algorithms “to surface more authoritative content.” Now, it contends, users are less likely to be misled.⁶⁶

As noted in Section 2, Eric Schmidt, Google’s former executive chairman, said in late 2017 that in his view, search results surfacing propaganda from RT and Sputnik can and should be deprioritized. In fact, he added, Google was in the process of “de-ranking those kinds of sites,” meaning that reports from the Russian outlets would be demoted in search results.⁶⁷

Unfortunately, rather than clarifying and amplifying this statement, Google blurred Schmidt’s meaning only about a week after he spoke. Reacting to Schmidt’s comments, a Russian regulatory agency threatened to take action against Google. In full [retreat](#), the company responded by contradicting its former leader, saying it does not adjust its main search algorithm to de-rank individual websites. “By speaking about ranking web sources, including the websites of Russia Today and Sputnik, Dr. Eric Schmidt was referring to Google’s ongoing efforts to improve search quality,” Google said in a letter to the agency. “We don’t change our algorithm to re-rank.” Recent research confirms that RT and Sputnik continue to surface at the top of Google News searches.⁶⁸

Facebook has announced a number of changes that could bear on the presence of dubious Russian content on its social network. When sending material to users’ News Feeds, Facebook says its algorithms will now prioritize articles that survey respondents have deemed “informative,” as well as articles from publications that respondents have labeled “trustworthy.” Facebook also plays down what it considers “false news,” without necessarily blocking it altogether. “[Demoting false](#)

news (as identified by fact checkers) is one of our best weapons because demoted articles typically lose 80% of their traffic,” Facebook has said on its corporate blog. The fact checkers in question are organizations such as FactCheck.org, PolitiFact, and Snopes, which since shortly after the 2016 presidential election have participated in a partnership with Facebook devoted to identifying false news articles.⁶⁹ Taking a different approach, Google enables publishers to tag news stories that a third-party fact-checking organization has labeled as truthful. We applaud these and other efforts to promote accuracy online, including the [News Integrity Initiative](#), a research consortium run by the City University of New York Graduate School of Journalism and underwritten by Facebook; [Craig Newmark Philanthropies](#); and others.⁷⁰

Several challenges complicate the picture for fact checking and related activity. The first is the need to establish independent and sustainable funding sources so that fact checking can be done on a permanent basis and global scale. The second relates to volume: With more than a billion pieces of content posted every day on Facebook alone, fact checkers cannot possibly review every item one-by-one.⁷¹ Then there is the speed with which disinformation spreads. By the time external reviewers have made their evaluations, some evocative falsehoods have already gone viral. Such was the case in February 2018 when Russian-linked social media accounts helped circulate the myth that survivors of the Parkland, Florida, school shooting were “crisis actors.” FactCheck.org and other groups debunked the fiction, but not before it had proliferated on the web.⁷²

A fourth problem concerns questions raised about the fairness of fact-checking organizations. In today’s toxic political environment, these groups are facing accusations of

partisanship or bias, typically from the political right.⁷³ These attacks underscore the importance of identifying funding sources that are deemed across the political spectrum to be independent—an objective that will not be easy to achieve.

In addition to professional fact-checking organizations, the platforms are relying on users to identify dubious material. “We use signals that people on Facebook produce to deprioritize content that is inauthentic, including hoaxes and misinformation,” a company executive told us. In December 2017, however, Facebook stopped marking suspected false news with a red flag warning. Academic research showed that the flags might actually draw users to the falsehoods—the opposite of what Facebook intended. The site now annotates questionable material by offering users “related articles” providing context and different points of view. According to Facebook, users tend to share false stories less often when they are accompanied by related articles. The company is testing another [context-boosting feature](#) that shows users links to authors’ Wikipedia entries and other recent content they have published. For its part, YouTube began in early 2018 to flag videos uploaded by broadcasters that receive state funding, including both RT and Sputnik and, in the U.S., the Public Broadcasting Service.⁷⁴

Finally, Facebook announced in January 2018 that it would change its [News Feed algorithm](#) to de-emphasize media articles and political news in favor of material shared and commented on by users’ friends and family. It is unclear what effect this change is having vis à vis disinformation. The adjustment might decrease some of the flow of intentionally false political information, but if a user’s friends and family regularly share hoaxes and conspiracy theories, the user’s News Feed presumably will now have more of that kind of material.⁷⁵



In addition to professional fact-checking organizations, the platforms are relying on users to identify dubious material. ‘We use signals that people on Facebook produce to deprioritize content that is inauthentic, including hoaxes and misinformation,’ a company executive told us.



Addressing Concerns About Legal Liability

Another factor may help explain the reluctance of the platform companies to adopt the sort of Russia-specific strategies we are proposing: fear of losing the industry’s liability shield in the United States under [Section 230](#) of the Communications Decency Act of 1996.

With certain exceptions, Section 230 protects online intermediaries—Facebook, Google, Twitter, and the like—from being sued for what others say and do on their sites. This provision has fostered free speech online. It also has allowed Facebook and Google to become giant profit machines, free of most liability worries related to the content they carry. By distinguishing Internet companies from traditional publishers and broadcasters, which do risk being sued over their content, Section 230 has provided legal fortification that allowed the largest social media and search businesses to thrive. (The European Union has adopted a provision similar to Section 230.)

Understandably, Internet platforms do not want to risk losing their liability protection. Former executives of these businesses tell us that, in general, top management at the companies worry about Congress one day restricting or even rescinding Section 230. The notion of broadly combating Russian disinformation by demoting or combing out false and divisive content may exacerbate these anxieties. Company leaders apparently fear that if Congress perceived their sites as anything other than neutral public forums—as opposed, say, to newspaper editors, who pick and choose what to publish—lawmakers might curb Section 230. “The platforms fear that could be the next big debate: whether Congress strips them of their immunity and treats them more like editors or publishers who can be sued,” says one former industry executive. Recent unsuccessful attempts to kindle this debate have been made by politically conservative politicians and right-leaning media outlets accusing Facebook of liberal bias.⁷⁶

The reality of the Internet is more complex than the binary distinction between neutral public forums and active editors. The major platforms fall somewhere in between. They generally do not select or create

individual pieces of content, as an editor would. But their algorithms do continually rank and arrange material, and thereby determine what users see. Facebook and Google speak openly about demoting false news. All of the social media platforms kill accounts they consider inauthentic. When assessing the self-governance of platforms, we argued in “Harmful Content” that the companies ought to follow a third way that acknowledges they are not traditional editors but also recognizes they have a responsibility to downplay or remove certain categories of pernicious content. That responsibility includes diminishing or eliminating political disinformation generated by Russia.⁷⁷



The reality of the Internet is more complex than the binary distinction between neutral public forums and active editors. The major platforms fall somewhere in between.



The Section 230 liability shield deserves to be preserved because it has helped promote the many advantages of a free and open Internet as a medium for information, innovation, education, and commerce. If hostile members of Congress attempt to curtail the protection, these advantages—rather than a dubious claim of absolute neutrality—comprise the best counter-argument. It is worth noting that nothing in the text of Section 230 bars websites from simultaneously policing disinformation and enjoying liability protection.⁷⁸

6. Responses by Governments

“
One U.S. government official says he often hears the question: ‘Why are the Russians eating our lunch in terms of information warfare?’
”

Governments can respond to Russian disinformation in several ways. They can enact laws, for example, that require Internet platforms to block or take down misleading or offensive material, with the threat of pecuniary punishment for failure to comply. In our view, such restrictions on content pose an immediate threat to the basic human right of free speech—and we therefore oppose this approach. One need only look at Internet censorship in China, Iran, or Russia to see extreme examples of the dangers. We seek to avoid having other governments dictate rules for acceptable content within their borders.

But governments can play legitimate roles in response to disinformation. These include enacting regulation that steers clear of content constraints, gathering intelligence and conducting analysis to undergird executive-branch actions, and educating the public to encourage critical thinking by Internet users.

Given these options, the U.S. government has responded haltingly to Russian disinformation, while European governments are moving more aggressively, in some ways that are promising and others that are troubling.

United States

In response to the 2016 presidential election interference, the Obama and Trump administrations each imposed sanctions penalizing a range of Putin cronies and Russian officials and organizations. Separately, Robert Mueller, the special prosecutor, brought his criminal charges against the Internet Research Agency and 13 of its employees. The February 2018 indictments are largely symbolic, as Moscow will not extradite Russian nationals who have faithfully carried out Putin’s disinformation policies.

The sanctions could inflict some economic costs, but they are a partial remedy at best. President Obama’s penalties, imposed in December 2016, did not stop disinformation flows in 2017 and 2018.

The U.S. executive branch also sponsors activities designed to counter foreign disinformation, but generally they have not been ambitious or effective. Voice of America and Radio Liberty, government-funded broadcasters that countered communist propaganda during the Cold War, now have a joint venture called [Polygraph.info](#). Focusing on a narrow audience—English speakers in countries bordering Russia—the American website highlights Russian misdeeds and disinformation. Polygraph has a staff of only five, however, and its traffic registers in the low thousands, meaning that in Internet terms it barely exists.⁷⁹

A sister taxpayer-underwritten operation, [Current Time](#), has a larger 24-hour Russian-language broadcasting and web platform with a more robust online presence. But its annual budget of \$20 million is only about one-tenth the size of RT’s English-language broadcast and

web operation, according to John Lansing, the government official overseeing Polygraph and Current Time. A question Lansing says he often hears in Washington, D.C., is: “Why are the Russians eating our lunch in terms of information warfare?”⁸⁰

Lack of American resolve is a big part of the answer. His sanctions notwithstanding, President Trump has said nothing critical about Russian disinformation. This [conspicuous silence](#) likely reflects his resentment of any hint that his campaign may have received a boost from Russian interference.⁸¹ But the weak executive branch response to Kremlin interference predates the Trump presidency and indicates a deep bureaucratic failing. The short history of the [Global Engagement Center](#) (GEC) at the Department of State illustrates this absence of determination.

The Obama administration established the GEC in 2016 to counter online incitement and recruitment by Al Qaeda and then ISIS. In 2017, Congress expanded its mission to include fighting foreign propaganda and disinformation. On paper, the GEC has responsibility for coordinating counter-disinformation

“
To unify the existing patchwork of U.S. agencies addressing foreign disinformation, we recommend creation of a new coordinating office within the National Security Council and an analysis unit at the Office of the Director of National Intelligence.
”

efforts across the U.S. government and includes personnel from the Departments of Defense and Treasury, the Central Intelligence Agency, and the National Security Agency. But under former Secretary of State Rex Tillerson, the center neglected its disinformation mission, leaving unspent tens of millions of dollars—\$120 million, by [one count](#)—allocated to it by Congress. *Politico* reported that one of Tillerson’s top aides suggested the money was unwelcome because any extra funding for programs to counter Russian media influence would anger Moscow.⁸² As of March 2018, according to *The New York Times*, not one of the center’s 23 analysts was a Russian speaker. Shortly before his ouster that same month, Tillerson gave voice to a remarkable defeatism: “If it’s [the Russians’] intention to interfere, they are going to find ways to do that,” he told Fox News. “And we can take steps we can take, but this is something that once they decide they are going to do it, it’s very difficult to preempt it.”⁸³

The Departments of State and Defense have launched a separate joint initiative called the Russia Information Group (RIG), designed to support “a credible counter-Russian voice” in Eastern Europe. But congressional testimony has indicated that the group lacks sufficient backing from either department to have much impact. The RIG “has to be reinforced, it has to be financed, they have to have the authorities that they need to lead that forward,” [General Curtis Scaparrotti](#), commander of the U.S. European Command, told the Senate Armed Services Committee in March 2017.⁸⁴ Richard Stengel, who served as Undersecretary of State for Public Diplomacy and Public Affairs during the final three years of the Obama presidency, has written that the RIG was [overwhelmed](#) by its task. “We pretty much stopped creating content ourselves,” Stengel conceded in an article in *Politico* in November 2017. “After all, the State Department isn’t exactly a media company, and the Russians were crushing us on volume.”⁸⁵

Overall, U.S. anti-disinformation efforts “have lacked sustained focus and have been hampered by the lack of properly trained professionals,” according to the most recent [National Security Strategy](#), issued by the White House in December 2017. “Efforts to counter the exploitation of information by rivals have been tepid and fragmented.”⁸⁶ The Democratic staff of the Senate Committee on Foreign Relations concurred in a [report](#) published in January 2018: “In contrast to many European countries, especially the Baltic and Nordic states, the U.S. government still lacks a coherent, public strategy to counter the Kremlin’s disinformation operations abroad and at home. Instead, it has a patchwork of offices and programs tasked with mitigating the effects of the Kremlin disinformation operations.”

To unify the existing patchwork, we embrace a recommendation made by the Alliance for Securing Democracy to form a pair of new executive branch entities to coordinate responses to disinformation. As we describe below in Section 7, we urge the creation of a new office within the [National Security Council](#) to oversee the activities of the many individual agencies that are—or ought to be—involved in countering disinformation. The [Office of the Director of National Intelligence](#), meanwhile, should house a unit staffed by experts from across the intelligence community who would track disinformation and feed their analysis to the new NSC branch.⁸⁷

On the legislative front, the U.S. Congress has held two rounds of relevant hearings in 2017 and 2018, but with little practical effect. In November 2017, Senator Dianne Feinstein said to a panel of lawyers representing Facebook, Google, and Twitter: “You’ve created these platforms, and now they’re being misused. And you have to be the ones to do something about it. Or we will.”⁸⁸

But in fact, there is no indication that a politically polarized Congress will act against Russian disinformation anytime soon. As noted earlier, the introduction

of the Honest Ads Act in October 2017 helped spur the platforms to require greater disclosure for online political advertising. Framed around the issue of transparency, the measure would not raise content-regulation or free-speech concerns. We favor adoption of legislation like the Honest Ads Act, which would make disclosure requirements enforceable by the federal government, as compared to the voluntary, and revocable, steps the companies have taken on their own.

But while the legislation seems unobjectionable, it currently lacks the backing needed to make headway in a Republican-controlled Congress. Introduced as a “bipartisan bill,” because one of its three initial Senate sponsors was the independent-minded Arizona Republican John McCain, the act has amassed 26 Senate co-sponsors, but the ailing McCain remains the sole GOP member onboard. Although multiple Republicans have endorsed a House version, the legislation shows no sign of life in either chamber.

Europe

In general, European nations have responded more vigorously to Russian disinformation, both as individual countries and by means of collective action. The neighboring countries of Denmark, Finland, Norway, and Sweden have had the most success achieving what the Democratic staff of the U.S. Senate Foreign Relations Committee has called “strong immunity against Russian malign information operations.” This resistance begins with extraordinary educational systems that emphasize critical thinking, the committee staff observed. In addition, because of their location, the four countries have experienced Moscow’s bellicosity up-close for decades, leaving their populations skeptical of the Kremlin’s disinformation campaigns. Their governments build on this popular disinclination to believe online falsehoods with a variety of preparedness programs.

The Swedish [Civil Contingencies Agency](#), for example, actively warns citizens against Russian-generated false information and offers counter-narratives promoting democracy and free expression. At least in part because of its difficulty gaining traction, Sputnik closed its Danish, Finnish, Norwegian, and Swedish language services in 2016.⁸⁹

European countries collaborate on disinformation via several joint organizations, such as the [Strategic Communications Center of Excellence](#) established by seven NATO member states in 2014 and headquartered in Riga, Latvia. It provides analysis and early warnings about hybrid warfare threats, including Russian disinformation. The European Union’s separate [East StratCom Task Force](#) relies on a network of 400 experts in more than 30 countries to collect examples of pro-Kremlin deceptions and analyze and publicize them in a searchable database. To combine NATO and EU efforts, Finland launched the [European Center of Excellence for Countering Hybrid Threats](#) in Helsinki in mid-2017. The U.S. participates in some of these multilateral enterprises, but according to the Democratic staff of the Foreign Relations Committee, Washington’s contribution “lags far behind what is necessary to defend against and deter the [Russian] threat.”⁹⁰

These NATO and EU organizations were started in an ad-hoc manner and are not all adequately funded. Their activities overlap but aren’t as coordinated as they ought to be. As we explain in Section 7, consolidating the various NATO and EU entities into a joint task force would enhance cooperation and improve effectiveness.⁹¹

Some European governments also have been more active legislatively than their American counterpart. In January 2018, Germany put into effect the most aggressive law enacted by a Western democracy to control what appears on social media. Known as *Netzwerkdurchsetzungsgesetz*, or [NetzDG](#), it seeks to reinforce Germany’s

“

Denmark, Finland, Norway, and Sweden display what has been called a ‘strong immunity’ against Russian disinformation. On top of extraordinary educational systems that emphasize critical thinking, these countries have a variety of preparedness programs that warn citizens against Russian-generated falsehoods and offer positive counter-narratives.

”

already-extensive bans on “hate speech” and other offensive content by requiring online platforms to remove forbidden material quickly. The underlying prohibitions grow out of the country’s Holocaust legacy and aim to block a revival of Nazi ideology or other forms of ethnic intolerance. NetzDG extends the well-established German restrictions from traditional media to social media. The law has a notably potent enforcement mechanism: It gives the platforms only 24 hours to block or remove “manifestly unlawful” content, or up to a week for more complicated cases, with some violators potentially facing a fine of up to 50 million euros.

Critics say NetzDG has two main flaws. The first, according to Bernhard Rohleder, the chief executive of Bitkom, Germany’s federal association for information technology, is that “the state has privatized one of its key duties: enforcing the law.”⁹² Second, skeptics warn that as a practical matter, NetzDG will result in unjustified



A bill pending in the French National Assembly would empower judges to stop the dissemination of ‘manipulated information’ via social media by blocking or closing down offending websites. The law also would authorize the French media council to take foreign state-controlled broadcasters off the air if they attempt to ‘destabilize’ France.



ensorship by platforms seeking to avoid large penalties. The detractors point to a series of high-profile cases, including one involving a satiric magazine that had its Twitter account blocked after it parodied anti-Muslim commentary. According to Reuters, some German lawmakers are discussing amendments to the law, one of which would make it easier for web users to have incorrectly deleted online material restored. Facebook, which, as mentioned earlier, has 1,200 employees reviewing posts in Germany, says it is “not pursuing a strategy to delete more than necessary.”⁹³

Beyond Germany, NetzDG has served as a model—and provided cover—for other countries seeking to clamp down on Internet content. Governments or lawmakers have cited the German statute when discussing or approving censorship laws in Russia, Singapore, and the Philippines.⁹⁴ Russia’s new law so closely resembles its German

antecedent that it has been called a “copy-and-paste” imitation.⁹⁵ Venezuela’s pro-government Constituent Assembly targeted social media with a hate-speech measure in November 2017. And Malaysia has punished its first defendant under a law passed in April 2018 that criminalizes “fake news.” In the Malaysian case, a man reportedly was sentenced to a month in jail for having posted a YouTube video critical of the police. The maximum penalty is six years behind bars and a fine equivalent to \$123,000.⁹⁶

In France, President Emmanuel Macron reportedly has cited NetzDG while urging approval of legislation intended to stop the spread of disinformation, especially during election campaigns. The bill, pending before the National Assembly, would empower judges to stop the dissemination of “manipulated information” via social media by blocking or closing down offending websites. The measure also would authorize the French media council to take foreign state-controlled broadcasters off the air if they attempt to “destabilize” France. These provisions are widely seen as designed to counter future Russian interference.⁹⁷ “Thousands of propaganda accounts on social networks are spreading all over the world, in all languages—lies invented to tarnish public officials, personalities, public figures, journalists,” Macron has said. “We are going to develop our legal means of protecting democracy against fake news.”⁹⁸ France and several other countries—Canada, Israel, and Italy among them—reportedly have contacted the German government to learn more about the impact of NetzDG.⁹⁹

In the U.K., Prime Minister Theresa May has publicly accused Russia of meddling in elections and planting fake stories in the media to sow discord in the West. These actions are “threatening the international order on which we all depend,” she has said.¹⁰⁰ Her government has established a special [anti-fake](#)

[news unit](#) “tasked with combating disinformation by state actors and others,” according to May’s spokesman. The new office, the aide added, “will respond with more and better use of national security communications.”¹⁰¹

Broader legislation may be coming. The European Commission in April 2018 [urged](#) Internet platforms to do more to halt the spread of disinformation, or face potential Europe-wide regulation. “These platforms have so far failed to act proportionately, falling short of the challenge posed by disinformation and the manipulative use of platforms’ infrastructure,” the Commission said in a strategy document. The EU executive body exhorted the companies to agree to a voluntary “Code of Practice on Disinformation,” warning that if self-regulation proves inadequate, the Commission may pursue other options, “including regulatory ones targeted at a few platforms.”

The Commission linked disinformation to political advertising much in the same fashion as the sponsors of the Honest Ads Act in the U.S. and instructed the Internet companies to “ensure transparency about sponsored content, in particular political and issue-based advertising.” It added that “this should be complemented by repositories where comprehensive information about sponsored content is provided, such as the actual sponsor identity, amounts spent, and targeting criteria used.” Setting tough deadlines, the Commission ordered the platforms to draft their code by July 2018, “with a view to producing measurable results” by October. Separately, the Commission said it would support the creation of an independent European network of fact-checkers to improve access to trustworthy content.¹⁰²

7. Recommendations

Some years ago, the Iranian government advanced the notion that its regulators would create a “halal Internet,” ensuring that only content the government deemed appropriate would circulate within Iran.¹⁰³ The Iranian experience reminds us of the need to prevent the fragmentation of the Internet, with each government labeling what is halal, or permissible, for its country. From a human rights perspective, sweeping government regulation invites politicians—and platforms—to overreach, resulting in excessive suppression of speech.

That said, both government and the technology industry have greater roles to play in addressing disinformation. When malign actors such as the Russian government or its proxies manipulate Internet platforms in an attempt to undermine democracy, government and the tech industry must develop appropriate responses.

Given the risks associated with government content regulation, it is incumbent on the major Internet platforms to exercise a more vigorous form of self-governance. For some solutions, the companies can rely on their prodigious technological capacity to identify and marginalize Russian disinformation. Other improvements require bureaucratic adjustments or a willingness to reach beyond company walls to cooperate with rivals and the government. For its part, governments can take up such vital tasks as collecting and disseminating intelligence on disinformation and assuring disclosure of who is purchasing political advertising.

Russia is not the only actor generating politically motivated disinformation, and in the future, other governments may follow its lead. But to date, Russian efforts in this regard are more advanced and prolific than those of any other country. Investigating Moscow’s actions can help us respond to similar attacks by others in the future. Thus, while our recommendations respond to the current Russian onslaught, they also suggest a model for use against other potential antagonists.

Recommendations to the Internet Platforms

1 Create Internal Teams that Enhance Capacity to Focus on Russian Disinformation

The Internet platforms all have acknowledged concern about Russian disinformation. Facebook's Mark Zuckerberg has described a digital "arms race" against Moscow. We urge the companies to act more aggressively on these concerns by creating dedicated internal teams whose primary function would be to address political disinformation generated and amplified by Russian government agents and their proxies. These teams should be integrated into units already addressing disinformation generally. They should include Russian-language and cultural experts, engineers, product managers, and security specialists. They should be charged with exploring the Kremlin's activities in every aspect of each company's business. As other bad actors emerge, these teams would have developed tools to deal with political disinformation, regardless of its origin. The platforms should make these efforts a high priority—and a public one. They need to signal externally and internally that Russian disinformation, because it is part of a broader Kremlin agenda to destabilize democracy, is more pernicious than other forms of "fake news." In addition to establishing specialized teams to address Russia and possibly other hostile states in the future, the companies need to continue to hire more people to monitor and evaluate content, as algorithms and machines alone will never be able to identify accurately all harmful material.

2 Realign Overall Corporate Structure

The primary Internet companies have built their successful businesses in an environment where engineering innovation has had wide latitude to thrive. The main constraint on this structure has been the obligation the companies recognize to abide by the law. In areas where laws are clear—prohibitions on child pornography, for example—the companies have rigorously developed and abided by restrictions on their operations. Political disinformation challenges this relatively simple structure of legal versus illegal. To judges and lawyers, Russian disinformation may be legal, even though it is wrong and potentially destructive. Beyond creating dedicated Russia teams, the companies need to adjust their overall internal structure to develop expertise and a decision-making capacity that prioritizes addressing thorny policy questions. One such question is how to respond to the proliferation of political disinformation that is legal but harmful to democratic discourse. A potential step in this direction would be to put a very senior executive in charge of public policy and have this person report directly to the chief executive officer, rather than to the general counsel.

3 Fund and Conduct Research on Next-Generation Artificial Intelligence

New threats are coming, and the industry must keep up with the next generation of disinformation methods. One menace on the horizon is known as "deep fake." The term describes "digital manipulation of sound, images, or video to impersonate someone or make it appear that a person did something" with a degree of realism so convincing that an unaided observer cannot detect the fake.¹⁰⁴ Deep fakes could facilitate disinformation on steroids. Politicians could be shown giving speeches they had not delivered or fraternizing with shady characters they had never met. Made-up battlefield atrocities could be depicted in minute, if phony, detail. Deep fakes have the potential to erode what remains of public trust in democratic institutions. In light of this threat, the platform companies will have to counter deep fake technology and other innovations by developing new A.I. tools designed to sort the real from the unreal, allowing the latter to be demoted or blocked. Based on their performance to date, the Russians are likely to be the first to experiment with new online weapons. Because A.I. is not a panacea, however, it will require rigorous human oversight and testing as new versions are rolled out.

4 Expand Third-Party Fact-Checking Initiatives

Since the 2016 election debacle, fact-checking organizations such as PolitiFact and Snopes have begun to curb spurious online dispatches linked to Russia and other questionable sources. Facebook should expand its partnership with such groups to strengthen fact-checking efforts, and other platforms ought to follow suit. In an encouraging development, new competitors are entering the fact-checking arena. [NewsGuard Technologies](#), a for-profit startup, plans to license its “nutrition labels” of thousands of websites so that social media users know whether a site “is trying to get it right or instead has a hidden agenda or knowingly publishes falsehoods or propaganda.”¹⁰⁵ Without endorsing any particular fact checker, we urge the platforms to engage more energetically with the ones that prove reliable. None of these initiatives alone can solve the problem—the volume of digital material is just too great—but they can help the platforms provide users with valuable reference points, including the track records and sources of funding for various outlets claiming to disseminate news. More fact checking also will illuminate the vital role legitimate journalists play in providing the factual foundation on which free elections and wise self-governance rest.

5 Increase Industry-Wide Cooperation

Clint Watts, the disinformation expert affiliated with the Center for Cyber and Homeland Security, has noted that “each social media company will see but a part of the Kremlin’s social media influence campaign, but no one company alone can fully comprehend the extent of Kremlin operations.”¹⁰⁶ With this insight in mind, the platforms need to do more to cooperate and share information about Russian threats. The companies have shown they can collaborate: They do so through the Global Network Initiative, which focuses on freedom of expression and privacy; the [Global Internet Forum to Counter Terrorism](#), a collaboration involving technology companies, civil society groups, and government organizations; and the PhotoDNA initiative, which deals with child pornography. Separately, YouTube, Facebook, Twitter, and Microsoft cooperate in maintaining a database of “digital fingerprints” which allow them to take down violent extremist video more efficiently. The platforms should apply this spirit of teamwork to form a new industry organization devoted to the problem of Russian disinformation.

6 Highlight, De-Rank, and Block Russian Disinformation

Companies need to adjust their interfaces to include more warnings, notifications, and other forms of “friction” to lessen the impact of Russian disinformation. As noted, Facebook annotates questionable material with links to more reliable related articles on the same topic. Google’s former executive chairman, Eric Schmidt, has suggested another, more direct method of reducing the prominence of purposely false material: de-ranking it. As noted above, under pressure from the Russian government, Google backed away from Schmidt’s idea—a mistake the company should reverse. Clint Watts has made other sensible proposals meant to dampen the incessant drumbeat of bot-driven untruths. He recommends that social media companies reduce automated disinformation by use of human-verification systems, such as the CAPTCHA technology many websites already use to block computers. CAPTCHA requires a would-be user to reproduce twisted letters and digits, which a bot cannot recognize. And Watts urges constraining rapid-fire trolls by imposing “reasonable limits” on the number of posts non-automated accounts are permitted during an hour, day, or week.¹⁰⁷

7 Support Legislation Requiring Full Disclosure of Sources of Political Advertising

In recent months, Google, Facebook, and Twitter have announced various commitments to disclose the sources of political advertising online. We welcome this development but urge them to go further. The companies ought to support the institutionalization of these commitments by actively backing legislation such as the proposed Honest Ads Act. If the affected companies conspicuously lobbied for passage of the bill, it would put pressure on the Republican leadership to at least allow it to proceed to hearings and a vote. Otherwise, the legislation is likely to continue to languish. In Europe, the platforms are under strict instructions from the European Commission to include advertising-transparency provisions in a forthcoming Code of Practice on Disinformation. While they must comply with the Commission's mandate to self-regulate, the companies, again, should go further, in parallel with what we recommend for the U.S.: They should support a Europe-wide set of rules that ensure that social media users—and the wider electorate—know who is paying for political ads.

8 Rethink the Online Advertising Business Model

As noted in Section 5, the online advertising business inadvertently provides a receptive environment for purveyors of disinformation in that it rewards content that provokes negative emotional reactions. This has prompted a number of serious analysts to propose rethinking the online ad system with an eye toward making major changes. Digital financier Roger McNamee argues for a switch away from advertising in favor of a user-subscription model that would resemble the way cable television bills customers.¹⁰⁸ The Alliance for Securing Democracy recommends consideration of disentangling online advertising from data collection and micro-targeting. The goal of disentanglement would be to move back to the less individualized ads familiar on television or in print.¹⁰⁹ These suggestions may lead to useful reassessments of current practices, but in the end, it does not seem reasonable to expect the platforms to abandon their highly profitable core practices of collecting user data and selling micro-targeting tools to advertisers. A more realistic, if limited, alternative would be for the Internet companies to work with advertisers and intermediary firms to construct so-called white lists of websites preapproved for advertising. Already in use by some mostly large advertisers, whitelisting brings an element of human judgment into the otherwise-automated ad-buying process. The practice presumably would marginalize sites that traffic in disinformation or other unsavory commodities. In one example, [JPMorgan Chase](#) used whitelisting in 2017 to slim drastically the number of websites on which its ads were appearing—from 400,000 to 5,000 it had pre-approved. The financial services giant acted after it became aware that one of its ads appeared on a site called “Hillary 4 Prison,” a meme that Russian bots helped spread in the run-up to the 2016 presidential election.¹¹⁰

Recommendations to Governments

1 Make Bold Public Statements About the Threat Posed by Russian Disinformation

In the U.S., senior administration officials should articulate clearly and repeatedly the country's determination to deter foreign interference in elections and attempts to disrupt our democracy. The main message should be that meddling from abroad will have consequences (see recommendation no. 5, below, on sanctions). Such communication could also encourage media literacy: educating the public about the dangers of disinformation and how it threatens democratic values. British Prime Minister Theresa May provided an admirably blunt [template](#) during a speech she delivered in November 2017, condemning Russian information operations in Europe: "I have a very simple message for Russia," she said. "We know what you are doing, and you will not succeed. Because you underestimate the resilience of our democracies, the enduring attraction of free and open societies, and the commitment of Western nations to the alliances that bind us. The U.K. will do what is necessary to protect ourselves, and work with our allies to do likewise."¹¹¹

2 Form Governmental Bodies to Oversee Counter-Disinformation Efforts

As the Atlantic Council and Alliance for Securing Democracy separately observe,¹¹² the U.S. government needs better coordination of its currently weak and disparate attempts to fight disinformation. At the National Security Council, a new office should be established to oversee activities at the Departments of Defense, Homeland Security, and State and the Federal Bureau of Investigation, among other agencies. The NSC already coordinates myriad aspects of national security policy in this fashion. The new office would become responsible for distilling strategies to combat disinformation and presenting them to the National Security Adviser and the President. A second new body would find a home within the Office of the Director of National Intelligence. It would harness expertise from across the intelligence community—Central Intelligence Agency, National Security Agency, FBI, and others—to monitor sources of disinformation and trends in its dissemination. The new intelligence team would produce research that fuels the policy analysis of the new NSC branch. Both units would provide contact points for greater cooperation with disinformation specialists in Europe.

European governments should unify their various efforts to counteract disinformation. As noted earlier, a number of centers affiliated with NATO, the EU, and individual countries already pursue overlapping missions, mostly focused on Eastern and Central Europe. These organizations should be joined under the aegis of an adequately funded, integrated task force that also trains its attention on Western Europe. A task force could fulfill a function similar to those of the two new bodies we are recommending for the U.S. government: gathering intelligence on disinformation, coordinating responses, and augmenting public outreach and education about how to identify online falsehoods. Communication and mutual assistance between the U.S. and Europe would naturally increase if each side had a consolidated bureaucracy focusing exclusively on disinformation.

Recommendations to Governments (continued)

3 Strengthen Other Governmental Efforts to Respond to Russian Disinformation

During its short existence, the Global Engagement Center has typified the ineffectual U.S. government response to disinformation from Russia or other hostile states. The State Department sub-agency requires more generous funding and should spend judiciously the money it is allocated. As the Atlantic Council urges, it ought to focus primarily on public diplomacy in Europe: the funding of independent research, investigative journalism, and civil society efforts to counter disinformation aimed at allied nations. The Global Engagement Center should also regularly convene civil-society and academic endeavors directed against Russian interference in democratic states.¹¹³ It should, in other words, follow through on its own promise to cultivate “a global network of partners whose voices resonate with individuals most vulnerable to harmful propaganda.”¹¹⁴ In Europe, the functions that ought to be fulfilled by the Global Engagement Center would complement those of the various national and regional organizations previously mentioned. One of the key responsibilities of the EU-NATO task force discussed in the previous recommendation would be to ensure that the national and regional centers have the resources and leadership they require to be effective.

4 Improve Government Information Sharing and Cooperation with Industry

Greater cross-pollination between the public and private sectors would improve the odds that both the industry and democratic governments will stay a step ahead of the Kremlin and other suppliers of disinformation. A revived Global Engagement Center would provide the logical nexus between the U.S. government and the industry-based counter-disinformation organization we have urged the platform companies to form. In Europe, we recommend analogous cooperation between the newly formed EU-NATO task force and industry. Academics and civil society organizations with an interest in disinformation should also take part in regular exchanges with government institutions on both sides of the Atlantic Ocean.

5 Increase Sanctions Against Those Responsible for Disinformation Operations

The U.S. executive branch has authority to ratchet up financial penalties against a wider circle of individuals and organizations linked to Russian interference online. The Countering America’s Adversaries Through Sanctions Act, approved by Congress in July 2017, provides that authority, but the Trump administration has failed to use it fully. Sanctions will not end malign information operations. But they do raise the cost of those operations for the wealthy Russian individuals and relevant industries that back the Putin regime. Tougher sanctions would show there are real consequences for attempting to harm democracies. In anticipation of potential future interference, Congress should pass legislation along the lines of the bipartisan [DETER](#) Act (Defending Elections from Threats by Establishing Redlines Act), which would authorize a fresh round of sanctions on Russia if the Kremlin meddles again in U.S. elections.¹¹⁵

In Europe, EU sanctions against Russia—instituted in 2014 in reaction to Moscow’s annexation of Crimea and other violations of human rights—face opposition from populist politicians, such as those in Italy’s newly elected pro-Russian government. Certain European corporate interests that do business in Russia are also pushing to ease sanctions. Leaders from political, corporate, and civil society circles who understand the Russian threat need to step forward to see that European sanctions, recently extended, are toughened, not weakened.

6 Enact Disclosure Requirements for Political Advertising in the U.S. and Europe

As noted earlier, we urge the platform companies to lobby actively for legislation like the Honest Ads Act. With that industry support, politicians from both sides of the aisle who are concerned about the integrity of campaigns and elections should approve a bill resembling the pending legislation. We advocate an amendment that would vest oversight authority for online advertising disclosure with the Federal Communications Commission or Federal Trade Commission, rather than the Federal Election Commission. The FCC and the FTC have greater staff capacity and more vigorous enforcement cultures than the FEC, which has become mired in partisan standoffs. Once amended and approved, the bill should promptly be signed into law.

The EU should take comparable steps. Political advertising currently is regulated at the national level in Europe, not on an EU-wide basis. European countries generally prohibit or limit paid campaign advertising on traditional broadcast stations, but those rules do not extend to the Internet. As a result, paid political ads online constitute a loophole in most European countries, as they do in the U.S.¹¹⁶ The European Commission is addressing the loophole as part of its mandate that the platform companies develop a self-regulatory Code of Practice on Disinformation. Under the code, companies are supposed to disclose who pays for political ads. If the platforms fail to comply, the Commission has threatened to achieve its goal by means of government regulation. Even if the companies do cobble together a voluntary code that includes transparency provisions similar to those they have adopted in the U.S., we urge the EU to adopt standardized rules that will compel openness in online political advertising all across Europe.

7 Refrain from Adopting Overbroad Legislation Regulating Content

The rise of new challenges creates temptations to act boldly, and we have recommended strong action. But when it comes to government regulation of online content, the best course is to refrain. The extreme cases of crude censorship—China, Russia, Iran—require little elaboration. As we have seen, Germany’s NetzDG, requiring the swift removal of “hate speech” and other offensive expression, could result in platforms overreacting to avoid the law’s draconian penalties. The proposed French law banning “manipulated information” raises even more serious concerns because of the absence of a clear legal definition of what expression would be prohibited. When fighting Russian disinformation—or disinformation from anywhere—lawmakers should remember that they are defending democracy. Imperiling free speech is not the way to accomplish this worthy goal.

Endnotes

- 1 Elisa Shearer and Jeffrey Gottfried, "New Use Across Social Media Platforms 2017," Pew Research Center, September 7, 2017 (<http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/>).
- 2 David Ignatius, "Russia's Radical New Strategy for Information Warfare," *The Washington Post*, January 18, 2017 (https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.8e16e3b3cf49).
- 3 "Assessing Russian Activities and Intentions in Recent U.S. Elections," U.S. Office of the Director of National Intelligence, January 6, 2017 (https://www.dni.gov/files/documents/ICA_2017_01.pdf).
- 4 United States of America v. Internet Research Agency LLC et al., filed February 16, 2018 (<https://www.justice.gov/file/1035477/download>).
- 5 "Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation," NYU Stern Center for Business and Human Rights, November 2017. (https://issuu.com/nyusterncenterforbusinessandhumanri/docs/final.harmful_content_the_role_of_e=31640827/54951655).
- 6 Cecilia Kang and Sheera Frenkel, "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users," *The New York Times*, April 4, 2018 (<https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html>).
- 7 Nicholas Confessore, Cecilia Kang, and Sheera Frenkel, "Facebook Back on the Defensive, Now Over Data Deals with Device Makers," *The New York Times*, June 4, 2018 (<https://www.nytimes.com/2018/06/04/technology/facebook-device-partnerships-criticized.html>); Michael LaForgia and Gabriel J.X. Dance, "Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence," *The New York Times*, June 5, 2018 (<https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html>).
- 8 Paul Stronski and Richard Sokolsky, "The Return of Global Russia: An Analytical Framework," Carnegie Endowment for International Peace, December 14, 2017 (<https://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003>).
- 9 Molly K. McKew, "The Gerasimov Doctrine," *Politico Magazine*, September/October 2017 (<https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538>).
- 10 Todd C. Helmus et al., "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe," Rand Corporation, 2018 (https://www.rand.org/pubs/research_reports/RR2237.html).
- 11 Ellen Nakashima, "Inside a Russian Disinformation Campaign in Ukraine in 2014," *The Washington Post*, December 25, 2017 (https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html?utm_term=.4da2b11086ea); Mark Clayton, "Ukrainian Election Narrowly Avoided 'Wanton Destruction' From Hackers," *The Christian Science Monitor*, June 17, 2014 (<https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers>).
- 12 Nicole Perloth and David E. Sanger, "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says," *The New York Times*, March 15, 2018 (<https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html>).
- 13 Clint Watts, "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions," The German Marshall Fund of the United States, October 31, 2017 (<http://securingdemocracy.gmfus.org/publications/extremist-content-and-russian-disinformation-online-working-tech-find-solutions>).
- 14 Raphael Satter, "Inside Story: How Russians Hacked the Democrats' Emails," *Associated Press*, November 4, 2017 (<https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a>).
- 15 United States of America v. Internet Research Agency LLC et al., (supra note 4), p. 6; Alina Polyakova, "Putin's Re-election Was Decades in the Making," The Brookings Institution (blog), March 19, 2018 (<https://www.brookings.edu/blog/order-from-chaos/2018/03/19/putins-re-election-was-decades-in-the-making/>).
- 16 Philip Bump, "What Obama Did, Didn't Do and Couldn't Do in Response to Russian Interference," *The Washington Post*, February 21, 2018 (https://www.washingtonpost.com/news/politics/wp/2018/02/21/what-obama-did-didnt-do-and-couldnt-do-in-response-to-russian-interference/?noredirect=on&utm_term=.9d3f7802eec7).
- 17 Sam Levin, "Mark Zuckerberg: I Regret Ridiculing Fears Over Facebook's Effect on Election," *The Guardian*, September 27, 2017 (<https://www.theguardian.com/technology/2017/sep/27/mark-zuckerberg-facebook-2016-election-fake-news>).
- 18 Craig Timberg, "Russian Propaganda May Have Been Shared Hundreds of Millions of Times, New Research Says," *The Washington Post*, October 5, 2017 (https://www.washingtonpost.com/news/the-switch/wp/2017/10/05/russian-propaganda-may-have-been-shared-hundreds-of-millions-of-times-new-research-says/?utm_term=.c2178360a04c).
- 19 United States of America v. Internet Research Agency LLC et al., (supra note 4), p. 18.
- 20 Sheera Frenkel, "For Russian 'Trolls,' Instagram's Pictures Can Spread Wider than Words," *The New York Times*, December 17, 2017 (<https://www.nytimes.com/2017/12/17/technology/instagram-russian-trolls.html>).
- 21 "Hamilton 68: How to Read This Dashboard," Alliance for Securing Democracy.org (<https://dashboard.securingdemocracy.org>). For a skeptical perspective on the Hamilton 68 dashboard, see Miriam Elder and Charlie Warzel, "Stop Blaming Russian Bots for Everything," *BuzzFeed News*, February 28, 2018 (https://www.buzzfeed.com/miriamelder/stop-blaming-russian-bots-for-everything?utm_term=.nblxRbx8g#.ourGLwxW1).
- 22 Josephine Lukito and Chris Wells, "Most Major Outlets Have Used Russian Tweets as Sources for Partisan Opinion: Study," *Columbia Journalism Review*, March 8, 2018 (<https://www.cjr.org/analysis/tweets-russia-news.php>).
- 23 Bradley Hanlon, "It's Not Just Facebook: Countering Russia's Social Media Offensive," Alliance for Securing Democracy, April 2018 (<http://securingdemocracy.gmfus.org/publications/its-not-just-facebook-countering-russias-social-media-offensive>).
- 24 Daisuke Wakabayashi and Nicholas Confessore, "Russia's Favored Outlet Is an Online News Giant. YouTube Helped," *The New York Times*, October 23, 2017 (<https://www.nytimes.com/2017/10/23/technology/youtube-russia-rt.html>).
- 25 John Russell and Ben Collins, "Russians Used Reddit and Tumblr to Troll the 2016 Election," *The Daily Beast*, March 1, 2018 (<https://www.thedailybeast.com/russians-used-reddit-and-tumblr-to-troll-the-2016-election>).
- 26 Ben Nimmo, "#TrollTracker: Russian Trolls on Reddit," Digital Forensic Research Lab, Atlantic Council, April 12, 2018 (<https://medium.com/dfribl/trolltracker-russian-trolls-on-reddit-251075642811>).
- 27 Alex Hern, "Google Plans to 'De-rank' Russia Today and Sputnik to Combat Misinformation," *The Guardian*, November 21, 2017 (<https://www.theguardian.com/technology/2017/nov/21/google-de-rank-russia-today-sputnik-combat-misinformation-alphabet-chief-executive-eric-schmidt>).
- 28 Hanlon, "It's Not Just Facebook: Countering Russia's Social Media Offensive," (supra note 23), p. 7.
- 29 Helmus et al., "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe," (supra note 10), p. 19.

- 30 Issie Lapowsky, "Facebook May Have More Russian Troll Farms to Worry About," *WIRED*, September 8, 2017 (<https://www.wired.com/story/facebook-may-have-more-russian-troll-farms-to-worry-about/>); Diana Piliipenko, "Facebook Must 'Follow the Money' to Uncover Extent of Russian Meddling," *The Guardian*, October 9, 2017 (<https://www.theguardian.com/commentisfree/2017/oct/09/facebook-russian-meddling-investigation>).
- 31 Rob Barry and Shelby Holliday, "Russian Trolls Tried to Torpedo Mitt Romney's Shot at Secretary of State," *The Wall Street Journal*, March 8, 2018 (<https://www.wsj.com/articles/russian-trolls-tried-to-torpedo-mitt-romneys-shot-at-secretary-of-state-1520505000>).
- 32 Daisuke Wakabayashi and Scott Shane, "Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election," *The New York Times*, September 27, 2017 (<https://www.nytimes.com/2017/09/27/technology/twitter-russia-election.html?action=Click&contentCollection=BreakingNews&contentID=65882172&pgtype=article&r=0>). This New York Times article and several other sources in this section of the report rely on analysis by the Alliance for Securing Democracy displayed on its Hamilton 68 dashboard (supra note 21).
- 33 Molly K. McKew, "How Twitter Bots and Trump Fans Made #ReleaseTheMemo Go Viral," *Politico*, February 4, 2018 (<https://www.politico.com/magazine/story/2018/02/04/trump-twitter-russians-release-the-memo-216935>).
- 34 Sheera Frenkel and Daisuke Wakabayashi, "After Florida School Shooting, Russian 'Bot' Army Pounced," *The New York Times*, February 19, 2018 (<https://www.nytimes.com/2018/02/19/technology/russian-bots-school-shooting.html>); Jack Nicas and Sheera Frenkel, "Facebook and Google Struggle to Squelch 'Crisis Actor' Posts," *The New York Times*, February 23, 2018 (<https://www.nytimes.com/2018/02/23/technology/trolls-step-ahead-facebook-youtube-florida-shooting.html>).
- 35 Sebastian Herrera, "Russian Bots and the Austin Bombings: Can Fact-Checking Offset Division, Misinformation?" *Austin American-Statesman*, March 28, 2018 (<https://www.512tech.com/technology/russian-bots-and-the-austin-bombings-can-fact-checking-offset-division-misinformation/OEQhfzgtw2GPVfQqxKHNEO/>).
- 36 Adam Rawnsley, "Russian Trolls Denied Syrian Gas Attack—Before It Happened," *Daily Beast*, April 12, 2018 (<https://www.thedailybeast.com/russian-trolls-denied-syrian-gas-attack-before-it-happened>).
- 37 Stronski and Sokolsky, "The Return of Global Russia: An Analytical Framework," (supra note 8), p. 2.
- 38 Alina Polyakova and Spencer P. Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition," Brookings Institution, March 2018 (<https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf>).
- 39 Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *The New York Times*, August 28, 2016 (<https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html>); Charles Duxbury, "Sweden Ratifies NATO Cooperation Agreement," *The Wall Street Journal*, May 25, 2016 (<https://www.wsj.com/articles/sweden-ratifies-nato-cooperation-agreement-1464195502?ns=prod/accounts-wsj>).
- 40 Andrew Higgins, "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote," *The New York Times*, February 16, 2017 (<https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html>).
- 41 Eric Auchard, "French Candidate Macron Claims Massive Hack as Emails Leaked," *Reuters*, May 5, 2017 (<https://www.reuters.com/article/us-france-election-macron-leaks/french-candidate-macron-claims-massive-hack-as-emails-leaked-idUSKBN1812AZ>).
- 42 "#ElectionWatch: Russia and Referendums in Catalonia?" DFRLab, Atlantic Council, September 28, 2017 (<https://medium.com/dfrlab/electionwatch-russia-and-referendums-in-catalonia-192743efcd76>).
- 43 Editorial Board, "From the Czech Republic, a Warning for Our Midterms: The Russians Are Still Meddling," *The Washington Post*, January 29, 2018 (https://www.washingtonpost.com/opinions/global-opinions/from-the-czech-republic-a-warning-for-our-midterms-the-russians-are-still-meddling/2018/01/29/4498a748-0517-11e8-b48c-b07fea957bd5_story.html?utm_term=.afe3e6eb44bd).
- 44 Patrick Wintour, "Russian Bid to Influence Brexit Vote Detailed in New U.S. Senate Report," *The Guardian*, January 10, 2018 (<https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report>).
- 45 "Kremlin-backed Fake News Targets Britain," *The Economist*, April 19, 2018, (<https://www.economist.com/news/britain/21740776-mischievous-englishwomen-are-blamed-everything-skripal-poisoning-17th-century>).
- 46 Donara Barojan, "#PutinAtWar: Social Media Surge on Skripal," Digital Forensic Research Lab, Atlantic Council, April 5, 2018 (<https://medium.com/dfirlab/putinatwar-social-media-surge-on-skripal-b5132db6f439>).
- 47 David Alandete and Daniel Verdú, "How Russian Networks Worked to Boost the Far Right in Italy," *El País*, March 1, 2018 (https://elpais.com/elpais/2018/03/01/inenglish/1519922107_909331.html).
- 48 Elias Groll, "Zuckerberg: We're in an 'Arms Race' With Russia, but AI Will Save Us," *Foreign Policy*, April 10, 2018 (<http://foreignpolicy.com/2018/04/10/zuckerberg-facebook-were-in-an-arms-race-with-russia-but-ai-artificial-intelligence-will-save-us/>).
- 49 Honest Ads Act of 2017, S. 1989, 115th Congress (<https://www.congress.gov/bills/115/congress/senate/bills/1989/text>); Ian Vandewalker and Lawrence Norden, "Getting Foreign Funds Out of America's Elections," Brennan Center for Justice, New York University School of Law, April 2018 (https://www.brennancenter.org/sites/default/files/publications/Getting%20Foreign%20Funds%20Out%20of%20America%27s%20Elections.%20Final_April9.pdf).
- 50 Heather Timmons and Hanna Kozłowska, "Facebook's Quiet Battle to Kill the First Transparency Law for Online Political Ads," *Quartz*, March 22, 2018 (<https://qz.com/1235363/mark-zuckerberg-and-facebooks-battle-to-kill-the-honest-ads-act/>).
- 51 Jack Nicas, "Facebook to Require Verified Identities for Future Political Ads," *The New York Times*, April 6, 2018 (<https://www.nytimes.com/2018/04/06/business/facebook-verification-ads.html>); Daisuke Wakabayashi, "Google Will Ask Buyers of U.S. Elections Ads to Prove Identities," *The New York Times*, May 4, 2018 (<https://www.nytimes.com/2018/05/04/technology/google-election-ad-rules.html>); Nellie Bowles and Sheera Frenkel, "Facebook and Twitter Plan New Ways to Regulate Political Ads," *The New York Times*, May 24, 2018 (<https://www.nytimes.com/2018/05/24/technology/twitter-political-ad-restrictions.html>).
- 52 "Announcement: RT and Sputnik Advertising," Twitter blog, October 26, 2017 (https://blog.twitter.com/official/en_us/topics/company/2017/Announcement-RT-and-Sputnik-Advertising.html).
- 53 Bruce Falck, "New Transparency for Ads on Twitter," Twitter blog, October 24, 2017 (https://blog.twitter.com/official/en_us/topics/product/2017/New-Transparency-For-Ads-on-Twitter.html).
- 54 Dipayan Ghosh and Ben Scott, "#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet," Shorenstein Center on Media, Politics, and Public Policy, January 2018 (<https://shorensteincenter.org/digital-deceit-precision-propaganda/>).
- 55 Roger McNamee, "How to Fix Facebook: Make Users Pay for It," *The Washington Post*, February 21, 2018 (https://www.washingtonpost.com/opinions/how-to-fix-facebook-make-users-pay-for-it/2018/02/20/a22d04d6-165f-11e8-b681-2d4d462a1921_story.html?utm_term=.93b7857eae79).

Endnotes (continued)

- 56 John Naughton, "Who's Doing Google and Facebook's Dirty Work?" *The Guardian*, December 24, 2017 (<https://www.theguardian.com/commentisfree/2017/dec/24/facebook-google-youtube-dirty-work-social-media-inappropriate-content>).
- 57 Katrin Bennhold, "Germany Acts to Tame Facebook, Learning From Its Own History of Hate," *The New York Times*, May 19, 2018 (<https://www.nytimes.com/2018/05/19/technology/facebook-deletion-center-germany.html>).
- 58 Kurt Wagner and Rani Molla, "Twitter is Making Money Now, So It's Going to Start Hiring More People," *Recode*, April 25, 2018 (<https://www.recode.net/2018/4/25/17279308/twitter-twtr-hiring-headcount-earnings-profit>).
- 59 "Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation" (supra note 5), p. 26.
- 60 Nicole Perloth, Sheera Frenkel, and Scott Shane, "Facebook Exit Hints at Dissent on Handling of Russian Trolls," *The New York Times*, March 19, 2018 (<https://www.nytimes.com/2018/03/19/technology/facebook-alex-stamos.html>).
- 61 Sheera Frenkel, "Facebook Says It Deleted 865 Million Posts, Mostly Spam," *The New York Times*, May 15, 2018 (<https://www.nytimes.com/2018/05/15/technology/facebook-removal-posts-fake-accounts.html>).
- 62 "Update on Twitter's Review of the 2016 U.S. Election," Twitter Public Policy blog, January 31, 2018 (https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html).
- 63 Cade Metz, "Facebook's A.I. Growth Squeezes Universities," *The New York Times*, May 5, 2018 (<https://www.nytimes.com/2018/05/04/technology/facebook-artificial-intelligence-researchers.html>).
- 64 Groll, "Zuckerberg: We're in an 'Arms Race' With Russia, but AI Will Save Us," (supra note 48).
- 65 Ibid.
- 66 Ben Gomes, "Our Latest Quality Improvements for Search," Google blog, April 25, 2017 (<https://blog.google/products/search/our-latest-quality-improvements-search/>).
- 67 Hern, "Google Plans to 'De-Rank' Russia Today and Sputnik to Combat Misinformation," (supra note 27).
- 68 "Google Seeks to Defuse Row with Russia Over Website Rankings," *Reuters*, November 27, 2017 (<https://www.reuters.com/article/us-alphabet-russia-media/google-seeks-to-defuse-row-with-russia-over-website-rankings-idUSKBN1DR0T5>); Bradley Hanlon, "From Nord Stream to Novichok: Kremlin Propaganda on Google's Front Page," Alliance for Securing Democracy, June 14, 2018 (<https://securingdemocracy.gmfus.org/from-nord-stream-to-novichok-kremlin-propaganda-on-googles-front-page/>).
- 69 Tessa Lyons, "Replacing Disputed Flags with Related Articles," Facebook Newsroom, December 20, 2017 (<https://newsroom.fb.com/news/2017/12/news-feed-fyi-updates-in-our-fight-against-misinformation/>); Mike Ananny, "Checking in With the Facebook Fact-Checking Partnership," *Columbia Journalism Review*, April 4, 2018 (https://www.cjr.org/tow_center/facebook-fact-checking-partnerships.php).
- 70 Justin Kosslyn and Cong Yu, "Fact Check Now Available in Google Search and News Around the World," Google Blog, April 7, 2017 (<https://www.blog.google/products/search/fact-check-now-available-google-search-and-news-around-world/>); "Announcing the News Integrity Initiative to Increase Trust in Journalism," City University of New York Graduate School of Journalism, April 3, 2017 (<https://www.journalism.cuny.edu/2017/04/announcing-the-new-integrity-initiative/>).
- 71 Tessa Lyons, "Increasing Our Efforts to Fight False News," Facebook Newsroom, June 21, 2018 (<https://newsroom.fb.com/news/2018/06/increasing-our-efforts-to-fight-false-news/>).
- 72 Saranac Hale Spencer, "No 'Crisis Actors' in Parkland, Florida," FactCheck.org, February 22, 2018 (<https://www.factcheck.org/2018/02/no-crisis-actors-parkland-florida/>).
- 73 Matt Shapiro, "Running the Data on PolitiFact Shows Bias Against Conservatives," *The Federalist*, December 16, 2016 (<http://thefederalist.com/2016/12/16/running-data-politifact-shows-bias-conservatives/>).
- 74 Taylor Hughes, Jeff Smith, and Alex Leavitt, "Helping People Better Assess the Stories They See in Their News Feed," Facebook Newsroom, April 3, 2018 (<https://newsroom.fb.com/news/2018/04/news-feed-fyi-more-context/>); "Greater Transparency for Users Around News Broadcasters," YouTube Official Blog, February 2, 2018 (<https://youtube.googleblog.com/2018/02/greater-transparency-for-users-around.html>).
- 75 Mike Isaac, "Facebook Overhauls News Feed to Focus on What Friends and Family Share," *The New York Times*, January 11, 2018 (<https://www.nytimes.com/2018/01/11/technology/facebook-news-feed.html>).
- 76 Senator Ted Cruz, "Facebook Has Been Censoring or Suppressing Conservative Speech for Years," Fox News, April 11, 2018 (<http://www.foxnews.com/opinion/2018/04/11/sen-ted-cruz-facebook-has-been-censoring-or-suppressing-conservative-speech-for-years.html>).
- 77 "Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation," (supra note 5), p. 9.
- 78 Elliot Harmon, "No, Section 230 Does Not Require Platforms to Be 'Neutral,'" Electronic Frontier Foundation, April 12, 2018 (<https://www.eff.org/deeplinks/2018/04/no-section-230-does-not-require-platforms-be-neutral>).
- 79 Ken Dilanian and Rich Gardella, "One Tiny Corner of the U.S. Government Pushes Back Against Russian Disinformation," NBC News, April 15, 2018 (<https://www.nbcnews.com/politics/donald-trump/one-tiny-corner-u-s-government-pushes-back-against-russian-n866021>).
- 80 Ibid.
- 81 Peter Baker, "Trump's Conspicuous Silence Leaves a Struggle Against Russia Without a Leader," *The New York Times*, February 17, 2018 (<https://www.nytimes.com/2018/02/17/us/politics/trump-russia.html>).
- 82 Nahal Toosi, "Tillerson Spurns \$80 Million to Counter ISIS, Russian Propaganda," *Politico*, August 2, 2017 (<https://www.politico.com/story/2017/08/02/tillerson-isis-russia-propaganda-241218>).
- 83 Gardiner Harris, "State Dept. Was Granted \$120 Million to Fight Russian Meddling. It Has Spent \$0," *The New York Times*, March 4, 2018 (<https://www.nytimes.com/2018/03/04/world/europe/state-department-russia-global-engagement-center.html>).
- 84 United States Senate Committee on Foreign Relations, Democratic Staff, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," p. 151, January 10, 2018 (<https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf>).
- 85 Rick Stengel, "What Hillary Knew About Putin's Propaganda Machine," *Politico*, November 15, 2017 (<https://www.politico.com/magazine/story/2017/11/15/hillary-clinton-putin-russia-propaganda-election-215826>).
- 86 "National Security Strategy of the United States of America," The White House, p. 35, December 2017 (<https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>).
- 87 Jamie Fly, Laura Rosenberger, and David Salvo, "Policy Blueprint for Countering Authoritarian Interference in Democracies," Alliance for Securing Democracy, p. 25, July 25, 2018 (<https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Policy-Blueprint.pdf>).
- 88 Craig Timberg, Hamza Shaban, and Elizabeth Dwoskin, "Fiery Exchanges on Capitol Hill as Lawmakers Scold Facebook, Google, and Twitter," *The Washington Post*, November 1, 2017 (https://www.washingtonpost.com/news/the-switch/wp/2017/11/01/fiery-exchanges-on-capitol-hill-as-lawmakers-scold-facebook-google-and-twitter/?utm_term=.e701b3b4c82b).

- 89 United States Senate Committee on Foreign Relations, Democratic Staff, "Putin's Asymmetric Assault on Democracy in Russia and Europe," (supra note 84), pp. 109-111.
- 90 Ibid., p. 141.
- 91 Fly, Rosenberger, and Salvo, "Policy Blueprint for Countering Authoritarian Interference in Democracies," (supra note 87), p. 29.
- 92 Bernhard Rohleder, Germany Set Out to Delete Hate Speech Online. Instead It Made Things Worse," *The Washington Post*, February 20, 2018 (https://www.washingtonpost.com/news/worldpost/wp/2018/02/20/netzdg/?utm_term=.a9f48ad2bb89).
- 93 Emma Thomasson, "Germany Looks to Revise Social Media Law as Europe Watches," *Reuters*, March 8, 2018 (<https://www.reuters.com/article/us-germany-hatespeech/germany-looks-to-revise-social-media-law-as-europe-watches-idUSKCN1GK1BN>).
- 94 "Germany: Flawed Social Media Law," Human Rights Watch, February 14, 2018 (<https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law>).
- 95 "Russian Bill is Copy-and-Paste of Germany's Hate Speech Law," Reporters Without Borders, July 19, 2017 (<https://rsf.org/en/news/russian-bill-copy-and-paste-germanys-hate-speech-law>).
- 96 Melanie Ehrenkranz, "First Person Charged Under Malaysia's 'Anti-Fake News' Law Gets Month in Prison for YouTube Video," *Gizmodo*, April 30, 2018 (<https://gizmodo.com/first-person-charged-under-malaysia-s-anti-fake-news-1825650301>).
- 97 Rohleder, "Germany Set Out to Delete Hate Speech Online. Instead, It Made Things Worse" (supra note 92).
- 98 Laura Smith-Spark and Saskya Vandoorne, "As France Debates Fake News Bill, Critics See Threat to Free Speech," *CNN*, June 7, 2018 (<https://www.cnn.com/2018/06/07/europe/france-fake-news-law-intl/index.html>).
- 99 Bennhold, "Germany Acts to Tame Facebook, Learning From Its Own History of Hate," *The New York Times* (supra note 57).
- 100 Rowena Mason, "Theresa May Accuses Russia of Interfering in Elections and Fake News," *The Guardian*, November 14, 2017 (<https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news>).
- 101 "Britain to Set Up Unit to Tackle 'Fake News': May's Spokesman," *Reuters*, January 23, 2018 (<https://www.reuters.com/article/us-britain-politics-fakenews/britain-to-set-up-unit-to-tackle-fake-news-mays-spokesman-idUSKBN1FC2AL>).
- 102 "Tackling Online Disinformation: a European Approach," European Commission, April 26, 2018 (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN>); Natalia Drozdiak, "EU Presses Tech Firms on Search Results, Fake News," *The Wall Street Journal*, April 26, 2018 (<https://www.wsj.com/articles/eu-urges-web-platforms-to-do-more-to-stop-spread-of-fake-news-1524734404>).
- 103 John Gambrell, "'Halal' Internet Means More Control in Iran After Unrest," *Associated Press*, January 29, 2018 (<https://www.apnews.com/c02a320725fc4afda305a0f3a660d8be6>).
- 104 Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Crisis for National Security, Democracy, and Privacy?" *Lawfare*, February 21, 2018 (<https://www.lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy>).
- 105 "Introducing: NewsGuard," NewsGuard website, undated (<https://newsguardtechnologies.com/>).
- 106 Clint Watts, "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions," Statement Prepared for the U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, October 31, 2017 (<https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Watts%20Testimony.pdf>).
- 107 Clint Watts, "Terrorism and Social Media: Is Tech Doing Enough?" Statement Prepared for the U.S. Senate Committee on Commerce, Science, and Transportation, January 17, 2018 (<https://www.fpri.org/wp-content/uploads/2018/01/Testimony-Clint-Watts-Senate-Commerce-17-Jan-2018.pdf>).
- 108 McNamee, "How to Fix Facebook: Make Users Pay for It," (supra note 55).
- 109 Fly, Rosenberger, and Salvo, "Policy Blueprint for Countering Authoritarian Interference," (supra note 87) p. 33.
- 110 Sapna Maheshwari, "Chase Had Ads on 400,000 Sites. Then, on Just 5,000. Same Results," *The New York Times*, March 29, 2017 (<https://www.nytimes.com/2017/03/29/business/chase-ads-youtube-fake-news-offensive-videos.html>).
- 111 Mason, "Theresa May Accuses Russia of Interfering in Elections and Fake News," (supra note 100).
- 112 Daniel Fried and Alina Polyakova, "Democratic Defense Against Disinformation," Atlantic Council, February 2018 (http://www.atlanticcouncil.org/images/publications/Democratic_Defense_Against_Disinformation_FINAL.pdf); Fly, Rosenberger, and Salvo, "Policy Blueprint for Countering Authoritarian Interference," (supra note 87), p. 25.
- 113 Fried and Polyakova, "Democratic Defense Against Disinformation," (supra note 112), p. 5.
- 114 "Global Engagement Center," U.S. Department of State, undated website (<https://www.state.gov/r/gec/>).
- 115 Fly, Rosenberger, and Salvo, "Policy Blueprint for Countering Authoritarian Interference," (supra note 87), p. 22-23.
- 116 Karen Kornbluh, "How Europe and Canada Are Fighting Foreign Political Ads on Social Media," Council on Foreign Relations, May 17, 2018 (<https://www.cfr.org/blog/how-europe-and-canada-are-fighting-foreign-political-ads-social-media>).

NYU Stern Center for Business and Human Rights
Leonard N. Stern School of Business
44 West 4th Street, Suite 800
New York, NY 10012
+1 212-998-0261
bhr@stern.nyu.edu
bhr.stern.nyu.edu



Center for Business
and Human Rights