IN APRIL 2014 A PECULIAR NEWS STORY APPEARED on social media feeds across the United States. The story: A curious petition on the WhiteHouse.gov website, “Alaska Back to Russia,” had gained over 30,000 online signatures in less than a week.1 The petition advocated for America to return its largest state back to the country from which it was originally purchased. Until March 30, 2017, the story was widely forgotten. On that day, Clint Watts, former FBI agent and senior fellow at the Foreign Policy Research Institute, testified in front of the Senate Intelligence Committee at the first public hearing on Russian interference in the 2016 U.S. presidential election. Russia has weaponized fake news, Watts told Senators, using social media-driven crusades to discredit U.S. institutions and leadership. Thousands of the accounts signing, commenting on, and promoting the “Alaska Back to Russia” petition were automated, pro-Russian bots. Together, these bots were able to create a story so large it made news across America. The bots, however, were not news. The story they manipulated was. Russia, a long-time U.S. adversary in the battle of narratives, has edged an advantage by testing social media’s potential to gain disproportionate influence over citizens beyond its own. The U.S. government must recognize and respond to the bot threat, in coordination with social media companies, in order to protect and preserve American democracy as we know it.

Bots, defined as social media identities that use automated scripts to rapidly or strategically disseminate content, have quickly become a prominent element of online politics.2 Watts and his colleagues identified and named three types of bot accounts—Hecklers, Hacker bots, and Honeypots—that push four categories of Russian propaganda on social media.3 Hecklers are synchronized “trolls” that attack political targets using analogous talking points, promoting Russian foreign-policy positions and targeting key English-speaking audiences. Hacker bots compromise the social media accounts of prominent leaders, such as U.S. government officials, American security experts, and media personalities, to post disinformation or gain access to private communications. Honeypot accounts are used to contrive friendships between real users and bots, building trust through direct messaging or email conversations before pushing a pro-Russia agenda.

The bot accounts generally advance four categories of propaganda: political
messages to undermine democratic institutions, financial propaganda to diminish confidence in global capitalism, social issues to deepen societal cleavages, and large-scope conspiracy theories to build skepticism of leadership. As evident by the propaganda categories, bots aim to weaken several of the essential tenants of democracy: institutions, capitalism, societal cohesion, and trust in leadership. Thus, a successful bot offensive has the potential to deteriorate democracies from the inside-out. So far, these operations have gone largely unhindered.

Today, the U.S. government has no clear strategy to combat information campaigns enabled by the Internet. One reason for this is the limited ability to accurately discern bot activity. Social media platforms are not amenable to sharing data on account activity, making it difficult for researchers to analyze message frequency, networks, or employ other techniques to identify bots online. Even where bot detection methodology is improving, such as with bot detection software, bots have often been able to outpace surveillance with constant, increasingly sophisticated adaptations. Unnatural speech patterns, synchronization and persistent, aggressive language from accounts with unusual biographies provide indication upon examination, but manual heuristics will never be efficient or extensive enough to secure the United States from such a dynamic cyberthreat.

Government response also remains constrained by free speech guarantees in the Constitution. Any U.S. government endeavor to counter the flow of disinformation through explicit deterrence would face major political, legal, and moral obstacles, potentially weakening the same institutions that deterrence would seek to protect. Therefore, third parties must step in to deter bots where democratic governments cannot. Social media companies, which harbor the greatest insight and control over accounts, are the obvious answer here, but may not be particularly willing to get involved. Following the 2016 U.S. election, Facebook CEO Mark Zuckerberg said his company was not responsible for influencing people’s votes: “Personally, I think the idea that fake news on Facebook—of which it’s a small amount of content—influenced the election in any way is a pretty crazy idea.” Yet, a Pew study found that
20 percent of social media users have “modified their stance on a social or political issue because of material they saw on social media.”

Thus, the government must create an incentive to ensure social media companies do their part in taking on this national threat. A related approach has been employed to combat bots of another kind. In December 2016, the Better Online Ticket Sales Act, or BOTS Act, which makes it illegal to use software to purchase tickets to popular events, was passed with bipartisan support in both the House and Senate. The now-law gives enforcement authority to the Federal Trade Commission, punishing with a fine those who do not comply. Following suit, the government can legally require social media companies to monitor and shut down unregulated bot accounts, with a fine for noncompliance.

While social media companies are not legally responsible for the content distributed on their sites in the United States, many platforms, including Facebook and Twitter, note that accounts must reflect real individuals or entities in their terms of service. Thus, while social media companies cannot be required to eliminate accounts for posting disinformation specifically, the government can require that companies live up to their own platform-user agreements. This is not to say that all bot accounts on social media must be shut down: many companies develop and employ branded bots to benefit their clientele. However, bot accounts created with the intention of manipulation, that are not forthrightly tied to a sanctioned origin and purpose, must be considered unregulated and shut down accordingly. The termination of unregulated bot accounts is not financially wise for social media companies, as they generate ad revenue based on user activity. Therefore, the fine must impose a greater burden on companies than the revenue lost from decreased account activity.

In Germany, government incentives seem to be working in the fight against propaganda. In March 2017, Germany began pressuring social networks to take responsibility for the spread of fake news with a bill to fine social media companies as much as 50 million euros if they fail to give users the option to complain about hate speech and fake news, or refuse to remove illegal content. The week after the bill was backed, Facebook Inc. published full-page ads in the country’s most widely circulated newspapers offering readers 10 ways to identify the validity of news. Facebook took out similar ads in newspapers in France. The company also removed over 30,000 bot accounts spreading fake news stories, spam, misinformation, and other deceptive content in the country.

Currently, the grand effects of social media are not fully understood. By experimenting with the budding power of this tool, Russia looks to gain
influence within global democracies amidst the thick of the digital age. If left for too long, manipulated stories end up in a country’s mainstream media where the impact of information cannot be underestimated. In the United States, what started as a news story about a laughable petition has grown into a full-blown threat to national security. As social media companies have laid the foundation for this threat to grow, they must recognize their role in disabling it. With law, the U.S. government must ensure that happens.

*Sofie Kodner is the media relations coordinator with External Relations at CSIS.*


Ibid.


See Facebook’s Rights and Responsibilities, Section 4, and Twitter’s Parody, Commentary, and Fan Account Policy.


Ibid.