alliance for securing democracy
G|M|F

PolicyBrief

2018 | No. 041

A Long Way To Go: Analyzing Facebook, Twitter, and Google's Efforts to Combat Foreign Interference

By Bradley Hanlon

Executive Summary

Two years after the Russian government manipulated social media to interfere in the 2016 U.S. presidential election, online information platforms continue to serve as mediums for such operations, including the 2018 midterm elections. Under intense public criticism and congressional scrutiny, the three most prominent online information platforms – Facebook, Twitter, and Google – have taken steps to address vulnerabilities and to protect their users against information operations by actors linked to authoritarian regimes. However, given the ongoing nature of online authoritarian interference, the steps taken by these companies continue to fall short.

This report reviews and analyzes the steps taken by online information platforms to better defend against foreign interference since 2016, adopting the framing of the Senate Intelligence Committee by focusing on the largest and most influential online information platforms of Facebook, Twitter, and Google.

The platforms' efforts to combat foreign interference have focused primarily on three key lines of effort: preventing or suppressing inauthentic behavior, improving political advertising transparency, and investing in forward-looking partnerships. Measures to limit user interaction with inauthentic behavior include content removal, labeling, and algorithmic changes. The platforms have also taken steps to improve advertising through policies to publicize advertiser information and improve verification standards for those hoping to publish political advertisements. Investments in forward-looking measures have included internal initiatives to critically assess vulnerabilities and external partnerships with civil society, academia, and fact-checking organizations. They have also led to increased transparency about the behavior and content of accounts linked to the Russian operation against the 2016 and 2018 elections, as well as other nation-state operations targeting Americans.

Though all of these steps are important, ongoing vulnerabilities demand more urgent action by the platforms to secure the online information space against foreign manipulation, while ensuring American's ability to engage freely in robust speech and debate. Six areas where Facebook, Twitter, and Google must take further steps include:

- **Focusing on behavior:** Online information platforms have unique insight into the computational tools used by bad actors on their respective platforms, allowing them to identify and eradicate coordinated inauthentic behavior, even when attribution is impossible. Although they have made recent progress in targeting behavior rather than content, a more aggressive focus on detecting and tackling networks will be key to counter evolving influence operations.

- **Increasing transparency and information sharing:** Recent efforts to expose foreign interference operations have demonstrated

greater transparency and information sharing by online information platforms. But these efforts remain largely ad hoc, and robust sharing that includes privacy protections requires the development of standing information sharing mechanisms with industry peers, government agencies, and the greater public.

- **Establishing standardization and effective coordination:** Despite numerous actions to counter disinformation and inauthentic behavior, platforms still lack a unified understanding of the threats they face. Standardizing terminology and constructing institutionalized communication mechanisms will foster better cross-platform cooperation to tackle interference operations.

- **Improving policies and enforcing rules clearly and consistently:** Platforms need to ensure that current policies go past window-dressing to achieve stated goals. And companies should work to more clearly articulate their terms of service, and should consistently and transparently apply those rules.

- **Thinking critically about future technologies:** As the threat of foreign interference continues to evolve and change, tech companies will need to think proactively about how to protect users against manipulation, and about how future technologies may be exploited by hostile foreign actors.

- **Making user protection the bottom line:** Platforms need to improve efforts to inform users about the threats that target them and to empower them with tools they can use to protect themselves. Further, platforms will need to change the ways that they design new features to emphasize user protection over ad revenue or convenience.

Online Information Platforms and Foreign Interference

Following a series of revelations throughout 2017 that Russia had exploited social media platforms to influence the 2016 presidential election, executives from Facebook, Twitter, and Google testified before the Senate Judiciary Committee on October 31, 2017 to discuss foreign interference on their platforms.[1] Lawmakers chastised the platforms for failing to report disinformation campaigns waged by the Russian government and its proxies for almost a year. As described by the New York Times, the executives expressed remorse and regret for their companies' failures during the 2016 election and promised to prevent future information operations from manipulating their users.[2]

Over ten months later, on September 5, 2018, representatives from tech giants were again called to Capitol Hill to update lawmakers on their efforts in the lead-up to the midterm elections.[3] In their written testimonies, all three companies reported numerous changes and policies to help improve transparency and protect users from foreign interference. However, questions from lawmakers elicited more apologies and promises than concrete solutions. And, in contrast to seemingly improved dialogue between policymakers and the witnesses from Facebook and Twitter, Google's chair sat empty for the duration of the hearing, a symbolic reminder that cooperation between the public and private sector on technological threats to democracy remains insufficient.

This report reviews and analyzes the steps taken by online information platforms to better defend against foreign interference since 2016, specifically focusing on three lines of effort: policies to address inauthentic behavior, measures to improve advertising transparency, and forward-looking investments and external partnerships.

The analysis of this report adopts the framing of the

1 Cecilia Kang, Nicholas Fandos, and Mike Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill," *The New York Times*, December 27, 2017, sec. U.S., https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html.

2 Cecilia Kang, Nicholas Fandos, and Mike Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill," *The New York Times*, December 27, 2017, sec. U.S., https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html.

3 Tony Romm and Craig Timberg, "Facebook and Twitter Testified before Congress. Conservative Conspiracy Theorists Lurked behind Them.," *Washington Post*, September 5, 2018, https://www.washingtonpost.com/technology/2018/09/05/facebook-twitter-sandberg-dorsey-congress-tech-hearings/.

Senate Intelligence Committee by focusing specifically on the online information platforms of Facebook, Twitter, and Google. Though interference operations are not limited to these platforms,[4] these companies serve as leaders and trendsetters in the wider tech community, operate the largest and most influential social networks in the U.S., and function as important mediums for the spread and consumption of information. The report concludes with six broad recommendations for online information platforms to better protect the American people from foreign interference.

Reviewing Online Information Platforms' Efforts to Counter Foreign Interference

Inauthentic Behavior and Inaccurate Information

In the years leading up to the 2016 election, the Russian Internet Research Agency employed inauthentic and automated accounts, often posing as American citizens, to spread false or divisive content, organize demonstrations and protests, and manipulate algorithms. Russian intelligence services similarly utilized inauthentic personas to help dispense and spread stolen information. Alongside these efforts, Russian government-linked media outlets and proxies spread disinformation across information platforms to disrupt and distract discussions surrounding key geopolitical events. Facebook, Twitter, and Google have sought to address inauthentic behavior and the spread of inaccurate information by targeting and removing inauthentic accounts, fact-checking and providing contextual information to users, and adjusting algorithms to reduce user interaction with misleading or harmful content.

Targeting Inauthentic Behavior

In the wake of revelations regarding foreign interference, online information platforms scrambled to improve their ability to target and remove malign content. In recent months, the platforms have begun to focus on tracking networks of inauthentic behavior in identifying and dismantling influence operations. In 2018, Facebook has identified and removed five major nation-state information operations targeting American audiences, including efforts originating in Iran and Russia.[5] The company has also worked with governments around the world to take down inauthentic accounts seeking to manipulate information on elections.[6] Twitter has similarly attempted to crack down on inauthentic accounts, particularly bot networks and accounts attempting to manipulate trending lists. In recent months, Twitter has suspended tens of millions of accounts (often unattributed bot networks),[7] and has also joined Facebook in tackling nation-state information operations.[8] For its part, Google has removed inauthentic accounts from its video-sharing platform YouTube,[9] though on a smaller scale. Google's platforms are more often targeted by overt propaganda

4 Bradley Hanlon, "It's Not Just Facebook: Countering Russia's Social Media Offensive," Alliance for Securing Democracy, April 11, 2018, https://securingdemocracy.gmfus.org/its-not-just-facebook-countering-russias-social-media-offensive/.

5 "Taking Down More Coordinated Inauthentic Behavior," Facebook Newsroom, August 21, 2018, https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/; Ben Nimmo and Graham Brookie, "#TrollTracker: Facebook Uncovers Active Influence Operation," Medium, July 31, 2018, https://medium.com/dfrlab/trolltracker-facebook-uncovers-active-influence-operation-74bddfb8dc06; "More Information About Last Week's Takedowns," Facebook Newsroom, November 13, 2018, https://newsroom.fb.com/news/2018/11/last-weeks-takedowns/; DFRLab, "#TrollTracker: Facebook Uncovers Iranian Influence Operation," Medium, October 26, 2018, https://medium.com/dfrlab/trolltracker-facebook-uncovers-iranian-influence-operation-d21c73cd71be.

6 Eric Auchard and Joseph Menn, "Facebook Cracks down on 30,000 Fake Accounts in France," Reuters, April 13, 2017, https://www.reuters.com/article/us-france-security-facebook/facebook-cracks-down-on-30000-fake-accounts-in-france-idUSKBN17F25G; Selena Larson, "Facebook Says It Took down 'tens of Thousands' of Fake Accounts before German Election," CNNMoney, September 27, 2017, https://money.cnn.com/2017/09/27/technology/business/facebook-german-elections-fake-accounts/index.html; Julia Love, Joseph Menn, and David Ingram, "In Mexico, Fake News Creators up Their Game Ahead of Election," Reuters, June 29, 2018, https://www.reuters.com/article/us-mexico-facebook/in-mexico-fake-news-creators-up-their-game-ahead-of-election-idUSKBN1JO2VG.

7 Mallory Locklear, "Twitter Says Most Recent Follower Purge Is about Bots, Not Politics," Engadget, February 21, 2018, https://www.engadget.com/2018/02/21/twitter-follower-purge-bots-not-politics/.

8 Hamza Shaban, "Twitter Suspends Guccifer and DCLeaks after Mueller Links Them to Russian Hacking Operation," *The Washington Post*, July 16, 2018, https://www.washingtonpost.com/technology/2018/07/16/twitter-suspends-guccifer-dcleaks-after-mueller-links-them-russian-hacking-operation/?noredirect=on&utm_term=.45e8e54200f4; Dave Paresh and Christopher Bing, "Facebook, Twitter Dismantle Disinformation Campaigns Tied to Iran and Russia," *Reuters*, August 21, 2018, https://www.reuters.com/article/us-facebook-russia-usa/facebook-twitter-dismantle-disinformation-campaigns-tied-to-iran-and-russia-idUSKCN1L62FD.

9 Kent Walker, "An Update on State-Sponsored Activity," Google Blog, August 23, 2018, https://www.blog.google/technology/safety-security/update-state-sponsored-activity/.

efforts via Russian government-controlled media outlets, which operate with a large presence on YouTube and effectively dominate search results on issues key to Russia's geopolitical interests.[10]

While the three companies have shown better coordination and capacity in tackling inauthentic behavior in recent months, they need to demonstrate greater transparency and commitment to consistently enforcing their policies. For example, while Facebook released a detailed report on its August takedown of foreign interference campaigns, the company still has not revealed the names of all of the accounts involved, and only released select information and content samples, preventing researchers from learning more about the operation.[11] Additionally, Twitter and Google – both of which participated in the coordinated takedown – failed to release any specifics on the operations removed from their platforms, leaving users unaware if they interacted with inauthentic content.[12] More recently, Twitter set a good example by releasing a trove of data from accounts linked to the Russian Internet Research Agency and issuing a commitment to expose future information operations. This should become a new standard for disclosures of information operations, as greater transparency will prove key in inoculating users against the tactics of foreign interference campaigns and empowering researchers to find solutions to future threats.[13]

Looking to the future, it is unclear whether the platforms have the capacity to keep up with the rapid speed and evolving threat of information manipulation. A recent report by the Knight Foundation revealed that despite Twitter's large-scale purges of inauthentic accounts, over 80 percent of accounts linked to disinformation campaigns during the 2016 elections are still active.[14] Additionally, Jonathan Albright's research has revealed the way that coordinated influence operations on Facebook have adapted to use the platform's "groups" to more covertly organize and execute information operations.[15] While Facebook and Twitter have committed to hiring more personnel to help moderate content on their sites, the companies remain confident that artificial intelligence will solve their problems.[16] However, researchers and experts remain skeptical of AI as a blanket solution to online information platform's challenges, and many have criticized social media companies for overstating its effectiveness and capabilities.[17] Even if AI does become an effective tool for combating inauthentic behavior, malign actors will also be able to make use of developing technologies to adapt and improve their efforts. In order to meaningfully reduce foreign interference on their sites, online information platforms will need to outsmart malign actors in a constant digital arms race.

"Looking to the future, it is unclear whether the platforms have the capacity to keep up with the rapid speed and evolving threat of information manipulation."

Revelations since 2016 have also indicated a startling lack of coordination between the platforms in tackling

10 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/; Donara Barojan, "YouTube's Kremlin Disinformation Problem," Medium, May 3, 2018, https://medium.com/dfrlab/youtubes-kremlin-disinformation-problem-d78472c1b72b .

11 "Taking Down More Coordinated Inauthentic Behavior," Facebook Newsroom, August 21, 2018, https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/.

12 @TwitterSafety, Twitter, (August 21, 2018), https://twitter.com/TwitterSafety/status/1032055161978585088; Kent Walker, "An Update on State-Sponsored Activity," Google Blog, August 23, 2018, https://www.blog.google/technology/safety-security/update-state-sponsored-activity/.

13 "Elections Integrity Hub," Twitter, accessed October 18, 2018, https://about.twitter.com/en_us/values/elections-integrity.html.

14 Tim Mak, "Most Twitter Accounts Linked To 2016 Disinformation Are Still Active, Report Finds," NPR, October 4, 2018, https://www.npr.org/2018/10/04/653454568/most-twitter-accounts-linked-to-2016-disinformation-are-still-active-report-find.

15 Jonathan Albright, "The Shadow Organizing of Facebook Groups," Medium, November 4, 2018, https://medium.com/s/the-micro-propaganda-machine/the-2018-facebook-midterms-part-iii-granular-enforcement-10f8f2d97501.

16 Michal Lev-Ram, "Why Thousands of Human Moderators Won't Fix Toxic Content on Social Media," *Fortune*, March 22, 2018, http://fortune.com/2018/03/22/human-moderators-facebook-youtube-twitter/.

17 Drew Harwell, "AI Will Solve Facebook's Most Vexing Problems, Mark Zuckerberg Says. Just Don't Ask When or How.," *Washington Post*, April 11, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/ai-will-solve-facebooks-most-vexing-problems-mark-zuckerberg-says-just-dont-ask-when-or-how/; Will Knight, "Three Problems with Facebook's Plan to Kill Hate Speech Using AI," *MIT Technology Review*, April 12, 2018, https://www.technologyreview.com/s/610860/three-problems-with-facebooks-plan-to-kill-hate-speech-using-ai/.

information operations that exploit all of their platforms concurrently. For example, an inauthentic persona managed by Russian intelligence officers, Alice Donovan, was removed from Facebook in September 2017 following revelations of Russian interference. However, despite Facebook's takedown, Alice Donovan's twitter account remained active until June 2018 after the persona was exposed by an indictment on the Russian officers by Special Counsel Mueller.[18] A New York Times investigation into Facebook's management of its recent scandals also reveals that the company has actively attempted to deflect criticism toward its competitors rather than working with them to tackle issues.[19] If online platforms hope to effectively combat malign actors – who operate with ease across various platforms – more open and institutionalized coordination will be key.

Finally, online information platforms have struggled to clearly state and consistently enforce their terms of service, leaving significant room for manipulation. According to data journalist Jonathan Albright, though Facebook has shown recent success in tackling inauthentic behavior, "a longstanding pattern of ineffective rules paired with inconsistent enforcement" undermine the company's efforts and open up "many loopholes and workarounds" for malign actors.[20] Twitter has received similar criticism for the way it "haphazardly" enforces of its terms of service (often in response to public criticism).[21] For example, despite touting improved abilities to remove content that violates its rules, investigations have revealed that pages and accounts banned on Facebook have been easily reestablished under new names and with little loss to engagement metrics.[22] Research indicates that Twitter has similarly struggled to uphold its standards, often failing to adequately respond or act on user reports for rules' violations for hate speech, abuse, and impersonation.[23] If online platforms hope to successfully counter information manipulation, they will need to more clearly define and consistently uphold their own rules.

Fact-checking and Labeling

Online platforms have also sought to combat the spread of inauthentic behavior by instituting various fact-checking features, and by labeling content and search results to provide important contextual information to users. Facebook has launched fact-checking partnerships with organizations in 16 countries,[24] including an agreement to partner with the Associated Press in the leadup to the 2018 midterm elections.[25] In 2017, Google instituted a label to help readers identify fact-checking articles in search results.[26] Additionally, Google temporarily introduced a feature to highlight fact-checked content when users searched for publishers, though the company quickly removed the feature following backlash alleging that it was biased against conservative sources.[27]

Online platforms have implemented various labeling features to provide contextual information for content and search results. Since the 2016 election, Facebook has introduced several new labels to provide users with

18 Laura Rosenberger, "Foreign Influence Operations and Their Use of Social Media Platforms," Alliance For Securing Democracy, July 31, 2018, https://securingdemocracy.gmfus.org/foreign-influence-operations-and-their-use-of-social-media-platforms/.

19 Sheera Frenkel et al., "Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis," *The New York Times*, November 15, 2018, sec. Technology, https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html.

20 Jonathan Albright, "Facebook's Failure to Enforce Its Own Rules – Member Feature Stories," Medium, November 6, 2018, https://medium.com/s/story/the-2018-facebook-midterms-part-iii-granular-enforcement-10f8f2d97501.

21 Sara Boboltz, "Twitter Haphazardly Enforces Its Rules. That's Great For Alex Jones and Infowars.," Huffington Post, August 15, 2018, sec. Media, https://www.huffingtonpost.com/entry/alex-jones-twitter-suspension_us_5b6cb23de4b0530743c85d03; Oliver Darcy, "Twitter Says InfoWars Hasn't 'violated Our Rules.' It Looks like That's Not the Case," CNNMoney, August 9, 2018, https://money.cnn.com/2018/08/09/media/twitter-infowars-alex-jones/index.html.

22 Jonathan Albright, "Facebook's Failure to Enforce Its Own Rules – Member Feature Stories," Medium, November 6, 2018, https://medium.com/s/story/the-2018-facebook-midterms-part-iii-granular-enforcement-10f8f2d97501.

23 "Toxic Twitter - The Reporting Process," Amnesty International, March 2018, https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-4/; Tim Samples, "My Short Life as (the Face of) a Russian Disinformation Troll," *Columbia Journalism Review*, July 30, 2018, https://www.cjr.org/first_person/russian-troll-twitter.php.

24 "Third-Party Fact-Checking on Facebook," Facebook Business, accessed August 27, 2018, https://www.facebook.com/help/publisher/182222309230722.

25 Natasha Bach, "Facebook Has Enlisted the Help of This News Agency to Debunk Fake News During Midterm Elections," *Fortune*, March 8, 2018, http://fortune.com/2018/03/08/ap-associated-press-fact-checkers-facebook-fake-news-midterm-elections/.

26 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/.

27 Daniel Funke, "Google Suspends Fact-Checking Feature over Quality Concerns," Poynter, January 19, 2018, https://www.poynter.org/news/google-suspends-fact-checking-feature-over-quality-concerns.

important background information on publishers and articles shared on its site.[28] In May 2018, Twitter similarly instituted labels for election candidates in the 2018 U.S. midterms to help users identify authentic accounts for candidates.[29] Google has also implemented labeling features through YouTube. In July 2018, YouTube launched a new tool to provide users with context surrounding certain issues prone to misinformation. The tool displays "fact-confirming text" below videos and at the top of search results to help users separate fact from fiction on key subjects that attract conspiracy theories such as the moon landing, the JFK assassination, and the downing of flight MH17.[30] YouTube also took steps to limit the impact of state-backed propaganda on its platform by labeling all content from state-sponsored news outlets, such as RT and Sputnik.[31]

While fact-checking efforts have increased substantially in recent years, efforts remain incomplete and likely ineffective. Though Facebook has claimed that its fact-checking efforts have produced positive results, partners of the program have argued that it is far too limited to effectively keep pace with the spread of false information on the platform.[32] Partners have also alleged that the program is more about window-dressing than about fixing the problem, with one former partner explaining, "They've essentially used us for crisis PR … They clearly don't care."[33] Google's fact-checking label may be similarly ineffective, as it appears infrequently in search results. Unfortunately, even more robust programs may prove equally as flawed, as researchers have questioned whether fact-checking is even an effective way to change readers' opinions.[34] Additionally, fact-checking often misses the point of information operations, which is not to establish a specific falsehood as the truth, but rather to flood the information space with so many competing narratives that there seems to be no truth at all.[35]

Labeling efforts, although promising, are plagued by similar challenges. Twitter's labeling of election candidates represents a small step forward, but much more must be done to empower users with more contextual information about content, such as why that content is being presented to them and whether it is being shared via an automated account.[36] Additionally, while the recent inclusion of "fact-confirming" labels on YouTube presents a positive model for future efforts, the program needs to be significantly expanded to include additional searches. Further, YouTube's current program does not include fact-confirming labels on state-sponsored videos, such as those from RT and Sputnik, even when those videos present misleading or inaccurate information.[37] Finally, YouTube's disclaimers for state-sponsored videos remain misleading, as videos produced by BBC, NPR, and RFE/RL include the same disclaimers as those accompanying RT and Sputnik videos. While it is true that all of these outlets are state-supported, only RT and Sputnik are used by their host government to publish false or deliberately misleading information. Conflating RT and Sputnik with institutions that have full, independent editorial control and high journalistic standards undermines legitimate news organizations and may mislead users into trusting inaccurate content.

28 "New Test to Provide Context About Articles | Facebook Newsroom," Facebook Newsroom, October 5, 2017, https://newsroom.fb.com/news/2017/10/news-feed-fyi-new-test-to-provide-context-about-articles/.

29 Bridget Coyne, "Introducing U.S. Election Labels for Midterm Candidates," Twitter Blog, May 23, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/introducing-us-election-labels-for-midterm-candidates.html.

30 Brandon A. Weber, "YouTube Now Displays Facts below Conspiracy Theory Videos," Big Think, August 8, 2018, https://bigthink.com/brandon-weber/new-to-youtube-a-fact-checking-collaboration-with-wikipedia-encyclopedia-brittanica.

31 Geoff Samek, "Greater Transparency for Users around News Broadcasters," Official YouTube Blog, February 2, 2018, https://youtube.googleblog.com/2018/02/greater-transparency-for-users-around.html.

32 Aaron Sharockman, "We Started Fact-Checking in Partnership with Facebook a Year Ago Today. Here's What We've Learned," *PolitiFact*, December 15, 2017, https://www.politifact.com/truth-o-meter/article/2017/dec/15/we-started-fact-checking-partnership-facebook-year/; 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.

33 Sam Levin, "'They Don't Care': Facebook Factchecking in Disarray as Journalists Push to Cut Ties," *The Guardian*, December 13, 2018, sec. Technology, https://www.theguardian.com/technology/2018/dec/13/they-dont-care-facebook-fact-checking-in-disarray-as-journalists-push-to-cut-ties.

34 Michelle Amazeen, "Sometimes Political Fact-Checking Works. Sometimes It Doesn't. Here's What Can Make the Difference.," *Washington Post*, June 3, 2015, https://www.washingtonpost.com/news/monkey-cage/wp/2015/06/03/sometimes-political-fact-checking-works-sometimes-it-doesnt-heres-what-can-make-the-difference/.

35 Joby Warrick and Anton Troianovski, "How a Powerful Russian Propaganda Machine Chips Away at Western Notions of Truth," *Washington Post*, December 10, 2018, https://www.washingtonpost.com/graphics/2018/world/national-security/russian-propaganda-skripal-salisbury/.

36 Laura Rosenberger, "Foreign Influence Operations and Their Use of Social Media Platforms," Alliance For Securing Democracy, July 31, 2018, https://securingdemocracy.gmfus.org/foreign-influence-operations-and-their-use-of-social-media-platforms/.

37 Zahra Hirji, "YouTube Is Fighting Back Against Climate Misinformation," *BuzzFeed News*, August 7, 2018, https://www.buzzfeednews.com/article/zahrahirji/youtube-climate-change-denial.

Adjusting Algorithms

Another significant line of effort for online platforms has been the adjustment and improvement of algorithms to reduce the spread of spam, inaccurate, or unverified content. Facebook announced several changes to reduce the spread of inaccurate content, most notably making significant adjustments to reduce the prevalence of news and advertising content in Newsfeeds in January 2018 (and promising to promote content from sources deemed "trustworthy" by users).[38] Twitter has similarly reported that it is improving algorithms to reduce the visibility of suspicious accounts.[39] In the leadup to the 2018 midterms, Twitter also launched a temporary feature that algorithmically generated a tweet feed to help users follow commentary on the upcoming elections. However, almost immediately after the feature launched, it surfaced tweets from accounts that are known promoters of conspiracy theories and disinformation campaigns.[40]

Due to constant attempts by various actors to manipulate Google search results, Google is continuously working to refine and improve its algorithms. Malign actors, including the Russian Internet Research Agency, have been known to employ Search Engine Optimization teams to improve their visibility in search results.[41] And in response to criticism that its algorithms inadvertently promote misleading information and state-sponsored propaganda, Google has announced on several occasions that it is working to specifically surface "more authoritative content"[42] and to "improve search quality."[43]

Google's efforts to promote authoritative content are important, but, so far, inadequate. Despite claims that the company is reducing the prominence of misleading content in search results, specifically citing RT and Sputnik,[44] Russian state-sponsored propaganda continues to dominate Google's search results on issues key to the Kremlin.[45] By constantly reporting on these subjects, it appears that RT and Sputnik are able to game Google's algorithm and dominate the search results for these events due to Google's focus on surfacing recent reporting. Google's News function is more successful at weeding out state-sponsored propaganda, but even News often promotes unlabeled Russian state-sponsored media in its results for certain geopolitical topics. To better protect and inform its users, Google should adjust its algorithms to value authoritative and trustworthy articles over "fresh" content in search results.[46]

Additionally, recent revelations regarding the targeting of Google's search results present a substantial vulnerability for foreign interference. Results of a new research study indicate that Google actively tailors its search results to specific users based on data collected from them, even when users are logged out or in private browsing mode.[47] If accurate, this is extremely problematic, as this means Google's search algorithm filters information to users that reinforces their preconceived notions, potentially promoting misinformation and propaganda over the truth.

38 Jonathan Vanian, "Everything to Know About Facebook's Big News Feed Change," Fortune, January 12, 2018, http://fortune.com/2018/01/12/facebook-news-feed-change/.

39 Yoel Roth and Del Harvey, "How Twitter Is Fighting Spam and Malicious Automation," *Twitter Blog*, June 26, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html.

40 Charlie Warzel and Ryan Mac, "Twitter Just Launched A Midterm Elections Page And It's Already Full Of Garbage," BuzzFeed News, October 30, 2018, https://www.buzzfeednews.com/article/charliewarzel/twitter-just-launched-a-midterms-page-and-its-already.

41 Bradley Hanlon, "Target USA: Key Takeaways from the Kremlin's 'Project Lakhta,'" Alliance For Securing Democracy, accessed December 11, 2018, https://securingdemocracy.gmfus.org/target-usa-key-takeaways-from-the-kremlins-project-lakhta/.

42 Ben Gomes, "Our Latest Quality Improvements for Search," *Google Blog*, April 25, 2017, https://www.blog.google/products/search/our-latest-quality-improvements-search/.

43 "Google Vice President: 'We Don't Change Our Algorithm to Re-Rank Websites,'" *Sputnik*, November 27, 2017, https://sputniknews.com/world/201711271059465018-google-re-rank-websites/.

44 Alex Hern, "Google Plans to 'de-Rank' Russia Today and Sputnik to Combat Misinformation," *The Guardian*, November 21, 2017, sec. Technology, https://www.theguardian.com/technology/2017/nov/21/google-de-rank-russia-today-sputnik-combat-misinformation-alphabet-chief-executive-eric-schmidt.

45 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/.

46 "News, Disinformation, and Free Expression," The Open Mind, September 22, 2018, https://www.thirteen.org/openmind/media/news-disinformation-and-free-expression/6027/.

47 Natasha Lomas, "Google 'Incognito' Search Results Still Vary from Person to Person, DDG Study Finds," TechCrunch, December 4, 2018, http://social.techcrunch.com/2018/12/04/google-incognito-search-results-still-vary-from-person-to-person-ddg-study-finds/.

Facebook's algorithm changes have also drawn criticism, as the reduction of news in users' newsfeeds significantly constricted online traffic to legitimate outlets.[48] A more productive policy would be to promote the prevalence of verified content and sources, rather than to shun all news. Twitter should similarly promote the prevalence of verified accounts or content, and both platforms should ensure that their verification processes are stringent enough to weed out inauthentic actors.

Advertising

On September 6, 2017, Facebook announced that the Russian government-linked Internet Research Agency (IRA) had spent $100,000 on advertising to influence the 2016 U.S. election.[49] The ads, which were later released to the public, targeted specific U.S. demographics, seizing on and inflaming discussions of hot-button issues to amplify divisions between Americans and influence public opinion.[50] In the months following, Facebook, Twitter, and Google, facing increased pressure from policymakers and the public, implemented numerous changes to increase transparency and security for political advertisements on their platforms.

One of the main policy changes introduced by the platforms is the institution of labeling for political advertisements to help users identify political ads and understand who is funding them. On Facebook, new features include "paid for by" tags for political and issue ads (defined as ads on "national issues of public importance") and a tool allowing users to see all of the different active ads run by a Page.[51] Twitter has similarly implemented labels for election-related and issue ads, and now requires disclaimers for promoted content to help users identify political campaigns.[52] Finally, Google has also launched a new measure requiring election advertisers to include information on ads' funding sources within the ads themselves.[53]

The platforms also took measures to try to weed out foreign ads before they could go live. In May 2018, Facebook announced a new policy requiring political advertisers in the U.S. to verify their identity and location.[54] Twitter instituted a similar verification standard for political and issue advertisers in the U.S.,[55] while Google now requires a government-issued ID or proof of lawful permanent residence to run election ads in the country.[56]

A final component of advertising transparency reform has been the establishment of publicly-accessible archives for advertisements. In recent months, Facebook, Twitter, and Google have all launched online archives for ads, which include information about political advertisers in the U.S.[57] Both Facebook and Twitter's archives feature both political and issue ads, while Google's archive is

48 Kathleen Chaykowski, "Facebook's Latest Algorithm Change: Here Are The News Sites That Stand To Lose The Most," Forbes, March 6, 2018, https://www.forbes.com/sites/kathleenchaykowski/2018/03/06/facebooks-latest-algorithm-change-here-are-the-news-sites-that-stand-to-lose-the-most/.

49 Alex Stamos, "An Update On Information Operations On Facebook", Facebook Newsroom, September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update/.

50 Scott Shane, "These Are the Ads Russia Bought on Facebook in 2016," *The New York Times*, November 1, 2017, sec. U.S., https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html.

51 "National Issue of Public Importance," Facebook Business, accessed August 27, 2018, https://www.facebook.com/business/help/214754279118974; Anthony Ha, "Facebook Will Allow You to See All the Active Ads from Any Page," *TechCrunch*, June 28, 2018, http://social.techcrunch.com/2018/06/28/facebook-ad-transparency/.

52 Bridget Coyne, "Introducing U.S. Election Labels for Midterm Candidates," *Twitter Blog*, May 23, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/introducing-us-election-labels-for-midterm-candidates.html; Bruce Falck, "Providing More Transparency around Advertising on Twitter," *Twitter Blog*, June 28, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/Providing-More-Transparency-Around-Advertising-on-Twitter.html; Del Harvey and Bruce Falck, "Announcing New US Issue Ads Policy," August 30, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/Announcing-new-US-issue-ads-policy.html.

53 Kent Walker, "Supporting Election Integrity through Greater Advertising Transparency," *Google Blog*, May 4, 2018, https://www.blog.google/outreach-initiatives/public-policy/supporting-election-integrity-through-greater-advertising-transparency/.

54 "Shining a Light on Ads With Political Content," *Facebook Newsroom*, May 24, 2018, https://newsroom.fb.com/news/2018/05/ads-with-political-content/.

55 Vijaya Gadde and Bruce Falck, "Increasing Transparency for Political Campaigning Ads on Twitter," *Twitter Blog*, May 24, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/Increasing-Transparency-for-Political-Campaigning-Ads-on-Twitter.html; Del Harvey and Bruce Falck, "Announcing New US Issue Ads Policy," August 30, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/Announcing-new-US-issue-ads-policy.html.

56 Kent Walker, "Supporting Election Integrity through Greater Advertising Transparency," *Google Blog*, May 4, 2018, https://www.blog.google/outreach-initiatives/public-policy/supporting-election-integrity-through-greater-advertising-transparency/.

57 "Shining a Light on Ads With Political Content," *Facebook Newsroom*, May 24, 2018, https://newsroom.fb.com/news/2018/05/ads-with-political-content/; Bruce Falck, "Providing More Transparency around Advertising on Twitter," *Twitter Blog*, June 28, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/Providing-More-Transparency-Around-Advertising-on-Twitter.html; "Political Advertising on Google – Google Transparency Report," *Google*, accessed August 27, 2018, https://transparencyreport.google.com/political-ads/overview?hl=en&spend_by_geo=state:;p:MToxMDo&lu=spend_by_geo.

currently limited to election ads (with stated plans to expand in the future). Facebook's archive also initially included advertisements from news organizations, a policy the company reversed after intense backlash pointed out that the inclusion inaccurately conflated marketing for news organizations with lobbying for a political agenda or candidate.[58]

The most glaring deficiency in the measures adopted by the platforms to eliminate foreign political ads is apparent gaps in their enforcement and implementation. Since their adoption, researchers and media organizations have exposed numerous loopholes in the ad policies. For example, in August 2018, Facebook took down a foreign influence operation that included over $10,000 in ads.[59]The takedown was initiated via a tip from cybersecurity firm FireEye, not from Facebook's internal mechanisms.

Additionally, over the summer of 2018, researchers successfully purchased ads through Google while impersonating the Kremlin-linked Internet Research Agency (IRA).[60] The researchers, who used the name and identifying details of the IRA to purchase ads that included known IRA content, were able to purchase ads on the YouTube channels and websites of CNN, CBS This Morning, HuffPost, and the Daily Beast, despite Google's ad reforms. Google responded to the revelation by stating that it had "taken further appropriate action to upgrade our systems and processes."

A similar experiment conducted by Vice News in the weeks before the midterm elections revealed a glaring vulnerability in Facebook's "paid for by" label. Vice successfully purchased, and Facebook approved, ads that Vice inauthentically claimed were "paid for by" Vice President Mike Pence, the Islamic State, and all 100 sitting U.S. senators.[61] According to Jonathan Albright, Facebook's ad policies are plagued by structural "loopholes" that allow for exploitation, such as Facebook's failure to adequately monitor pages running political ad campaigns after their initial verification.[62]

In their current form, online information platforms' ad policies also lack sufficient scope to prevent potential manipulation. Google's focus on just election ads is inadequate and unrepresentative of the type of advertising used by foreign actors to interfere in elections and political debate in the past few years. Additionally, Twitter's ad archive only includes ads from the past seven days, limiting the information provided to users. Finally, all three companies need to extend these features outside of the United States. Facebook's recent expansion of transparency requirements for political advertisers in the U.K. is a positive step,[63] but further implementation is necessary to protect users around the world.

A final issue with online information platforms' focus on improving advertising policies is that reforming ad transparency constitutes a disproportionately large portion of the platforms' efforts despite its limited role in foreign interference campaigns. In the case of the Russian Internet Research Agency, unpaid-for activity played a much larger part in spreading Russian narratives than advertisements.[64] While Facebook, Twitter, and Google have proudly paraded their ad reforms on Capitol Hill, the companies should also acknowledge the limitations of focusing on content as a solution to foreign interference. Closing off these vulnerabilities remains important, but online information platforms should concentrate their efforts on targeting coordinated inauthentic behavior rather than the results of that behavior.

58 Sara Fischer, "Facebook Drops Controversial Policy on Archiving Promoted News," Axios, November 29, 2018, https://www.axios.com/facebook-drops-controversial-policy-on-archiving-promoted-news-8535f0ba-317d-4755-99c1-25cff5988859.html.

59 "Taking Down More Coordinated Inauthentic Behavior," *Facebook Newsroom*, August 21, 2018, https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/.

60 Charlie Warzel, "This Group Posed As Russian Trolls And Bought Political Ads On Google. It Was Easy.," *BuzzFeed News*, September 4, 2018, https://www.buzzfeednews.com/article/charliewarzel/researchers-posed-as-trolls-bought-google-ads.

61 William Turton, "Facebook's Political Ad Tool Let Us Buy Ads 'Paid for' by Mike Pence and ISIS," Vice News, October 25, 2018, https://news.vice.com/en_us/article/wj9mny/facebooks-political-ad-tool-let-us-buy-ads-paid-for-by-mike-pence-and-isis; William Turton, "We Posed as 100 Senators to Run Ads on Facebook. Facebook Approved All of Them.," Vice News, October 30, 2018, https://news.vice.com/en_us/article/xw9n3q/we-posed-as-100-senators-to-run-ads-on-facebook-facebook-approved-all-of-them.

62 Jonathan Albright, "Facebook and the 2018 Midterms: A Look at the Data – Member Feature Stories," Medium, November 4, 2018, https://medium.com/s/story/the-2018-facebook-midterms-part-i-recursive-ad-ccountability-ac090d276097.

63 "Facebook Requires UK Political Ad Buyers to Reveal Identity," Associated Press, October 16, 2018, https://apnews.com/2dc8b765903745f4a60447c68aad83b4.

64 Nina Jankowicz, "The Top Three Trends We Miss When Discussing Russian Ads," Alliance For Securing Democracy, May 15, 2018, https://securingdemocracy.gmfus.org/the-top-three-trends-we-miss-when-discussing-russian-ads/.

Forward-Looking Investments and External Partnerships

A final key effort that online information platforms have embraced to counter foreign interference is investing in forward-looking internal resources and external partnerships to build capacity. These efforts can be divided into two main categories: partnerships with researchers and experts, and partnerships with media institutions and civil society.

Partnerships with Researchers and Experts

By employing experts and sharing data with external researchers, online information platforms can build greater capacity to identify impending threats and empower analysts to identify potential solutions. Investment in these partnerships varies significantly between platforms, and greater commitment and information sharing will be necessary to secure online platforms from foreign interference.

Partnerships with external researchers allow the academic and policy communities to analyze the tactics and impact of online information operations and offer potential solutions. In April 2018, Facebook launched one such partnership, announcing plans to form a commission of academic experts to develop a research agenda about the impact of social media on elections.[65] According to Facebook, the commission will solicit research and produce reports on the subject, although no such reports appear to have been released to date. Facebook also established a similar partnership with the Atlantic Council's Digital Forensics Research Lab in May to help the company get "real-time insights and updates on emerging threats and disinformation campaigns."[66] Although it lacks formal partnerships with outside organizations, Twitter's recent release of IRA data represents an important step towards greater information sharing with users and external researchers.[67]

Online platforms have also constructed internal mechanisms to increase their capacity to identify and counter potential foreign interference. Facebook recently launched its "Investigative Operations Team," a group of "ex-intelligence officers and media experts" who will help test the company's systems, pages, and apps to identify potential areas of misuse.[68] To complement this effort, the company also built a physical "war-room" to track potential interference surrounding the 2018 midterm elections,[69] and is working towards doubling its 10,000-person security staff.[70] Facebook shuttered its war-room shortly after the elections.[71] Google has invested in internal research on future threats through its think tank "Jigsaw," which is tasked with "invest[ing] in and develop[ing] tech solutions to geopolitical problems and digital attacks," though efforts thus far have focused mostly on cybersecurity.[72]

While external partnerships have enabled researchers and experts to assist online platforms in their battle against foreign interference, they have not gone far enough. For example, in July, Facebook shared only a fraction of the names of the pages and accounts associated with the Iranian and Russian interference operations that the company ultimately removed (and shared them only after they were erased off the site). Even Facebook's partners were not allowed to review much of the content, including one page which had reportedly organized several protests in the United States.[73] Google has similarly failed to publish the names of inauthentic accounts during its takedowns, inhibiting users and

65 Elliot Schrage and David Ginsberg, "Facebook Launches New Initiative to Help Scholars Assess Social Media's Impact on Elections," *Facebook Newsroom*, April 9, 2018, https://newsroom.fb.com/news/2018/04/new-elections-initiative/.

66 Katie Harbath, "Announcing New Election Partnership With the Atlantic Council," *Facebook Newsroom*, May 17, 2018, https://newsroom.fb.com/news/2018/05/announcing-new-election-partnership-with-the-atlantic-council/.

67 "Elections Integrity Hub," Twitter, accessed October 18, 2018, https://about.twitter.com/en_us/values/elections-integrity.html.

68 John Bowden, "Facebook Unveils New Team to Prevent Disinformation, Data Leaks," *The Hill*, June 22, 2018, http://thehill.com/policy/technology/393729-facebook-unveils-new-team-to-prevent-future-crises.

69 Rachel England, "Facebook Is Building a 'war Room' for the Midterm Elections," Engadget, September 4, 2018, https://www.engadget.com/2018/09/04/facebook-war-room-2018-midterm-elections/.

70 Eric Rosenbaum, "Facebook Data Privacy Scandal Has One Silver Lining: Thousands of New Jobs AI Can't Handle," CNBC, March 23, 2018, https://www.cnbc.com/2018/03/23/facebook-privacy-scandal-has-a-plus-thousands-of-new-jobs-ai-cant-do.html.

71 Sara Salinas, "Facebook Shutters Election Interference 'war Room' for Now," CNBC, November 26, 2018, https://www.cnbc.com/2018/11/26/facebook-wont-use-its-war-room-for-future-elections-report-says.html.

72 Catherine Shu, "Google's Think Tank Changes Its Name To Jigsaw And Becomes A Tech Incubator," *TechCrunch*, February 16, 2016, http://social.techcrunch.com/2016/02/16/jigsaw/; Jeff John Roberts, "Google Offers Free Protection to U.S. Political Websites," Fortune, May 16, 2018, http://fortune.com/2018/05/16/google-jigsaw-project-shield-political-websites/.

73 Sheera Frenkel, "How a Fake Group on Facebook Created Real Protests," *The New York Times*, August 14, 2018, sec. Technology, https://www.nytimes.com/2018/08/14/technology/facebook-disinformation-black-elevation.html.

researchers from learning from the campaigns.[74] Twitter's recent mass release of IRA data sets an important precedent for greater information sharing,[75] although even this data dump lacked information on inauthentic accounts that investigations have revealed were created by Russian intelligence officers in the run-up to the 2016 election.[76]

Partnerships with Media and Civil Society

Through partnerships with journalists, publishers, and civil society organizations, online information platforms have sought to build resilience to disinformation and foreign information operations throughout society. Since the 2016 election, Facebook has partnered with outside organizations to support research on news literacy,[77] publishing public service announcements on spotting false information,[78] and investing in and collaborating with newsrooms to support journalists and local news outlets.[79] Facebook also recently announced its "Digital Literacy Library," which offers lesson plans for educators "to help young people think critically and share thoughtfully online."[80] Twitter launched similar initiatives, including investments in media literacy programs,[81] partnerships to support digital literacy amongst educators and civil society,[82] and training programs for journalists.[83]

Even before the 2016 election, Google invested in funding, training, and support for journalists through several programs that now focus on combating misinformation in elections, helping to promote trustworthy content, and supporting newsrooms and journalists.[84] In March 2018, the tech company expanded its efforts by launching the Google News Initiative (GNI).[85] The GNI includes an array of efforts, including: training for journalists; software to recognize breaking news and direct searches to authoritative content; work with research institutions to improve media literacy; a Disinfo Lab aimed at fighting disinformation; open source tools to secure safer internet access for journalists; and initiatives to help media companies improve their revenue. Google has promised to commit $300 million to the GNI over the next three years.

Online information platforms' investments in media organizations and civil society indicate an important recognition of the need to protect the information ecosystem. While these partnerships and initiatives are impressive, platforms must do more to inform and empower their users by highlighting the threats they are working to address and the programs they have created to address them. Even the best tools are useless if no one knows how to access and apply them, and, as of yet, platforms have done a poor job communicating with users about their counter-interference efforts.

> ***"Steps toward transparency are welcome, but without more complete commitment, are little more than window-dressing."***

74 Kent Walker, "An Update on State-Sponsored Activity," Google, August 23, 2018, https://www.blog.google/technology/safety-security/update-state-sponsored-activity/.

75 "Elections Integrity Hub," Twitter, accessed October 18, 2018, https://about.twitter.com/en_us/values/elections-integrity.html.

76 See: https://www.justice.gov/file/1080281/download

77 Adam Mosseri, "Working to Stop Misinformation and False News," *Facebook Newsroom*, April 6, 2017, https://newsroom.fb.com/news/2017/04/working-to-stop-misinformation-and-false-news/.

78 Adam Mosseri, "A New Educational Tool Against Misinformation," *Facebook Newsroom*, April 6, 2017, https://newsroom.fb.com/news/2017/04/a-new-educational-tool-against-misinformation/.

79 "Facebook Journalism Project," *Facebook Media*, accessed August 27, 2018, https://www.facebook.com/facebookmedia/solutions/facebook-journalism-project; Campbell Brown, "The Next Step in Our Journey to Help Local News Publishers," Facebook Media, August 2, 2018, https://www.facebook.com/facebookmedia/blog/the-next-step-in-our-journey-to-help-local-news-publishers.

80 Antigone Davis and Karuna Nain, "A New Resource for Educators: Digital Literacy Library," *Facebook Newsroom*, August 2, 2018, https://newsroom.fb.com/news/2018/08/digitalliteracylibrary/.

81 Twitter Public Policy, "Update: Russian Interference in 2016 US Election, Bots, & Misinformation," *Twitter Blog*, September 28, 2017, https://blog.twitter.com/official/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html.

82 Lucia Gamboa and Patricia Cartes, "Twitter's Contribution to Media Literacy Week," *Twitter Blog*, November 11, 2017, https://blog.twitter.com/official/en_us/topics/events/2017/medialiteracyweek2017.html.

83 Twitter Public Policy, "Update: Russian Interference in 2016 US Election, Bots, & Misinformation," *Twitter Blog*, September 28, 2017, https://blog.twitter.com/official/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html.

84 Ludovic Blecher, "Digital News Initiative: €20 Million of Funding for Innovation in News," Google Blog, December 13, 2017, https://www.blog.google/around-the-globe/google-europe/digital-news-initiative-20-million-funding-innovation-news/; Steve Grove, "Introducing the News Lab," Google Blog, June 22, 2015, https://www.blog.google/outreach-initiatives/google-news-initiative/introducing-news-lab/.

85 Philipp Schindler, "The Google News Initiative: Building a Stronger Future for News," *Google Blog*, March 20, 2018, https://www.blog.google/outreach-initiatives/google-news-initiative/announcing-google-news-initiative/.

Overall, platforms' partnerships with external organizations should be cooperative, rather than competitive. Information operations cut across all online platforms, and establishing coordinated cross-platform partnerships with researchers and experts, along with structured lines of communication with media, users, and government agencies, will allow for more effective identification of and response to foreign interference. Partnerships should also constitute a commitment to information sharing on a holistic level. Steps towards transparency are welcome, but without more complete commitment, are little more than window-dressing.

Recommendations

Efforts to combat foreign interference by Facebook, Twitter, and Google have resulted in new initiatives to improve advertising transparency, address inauthentic behavior, and establish forward-looking investments and partnerships to build resilience to information manipulation. While these steps have yielded progress in understanding and addressing the threat of foreign interference, gaps and vulnerabilities persist. Most notably, Facebook, Twitter, and Google must make significant strides in six main areas:

- **Focusing on behavior:** Online information platforms have unique insight into the computational tools used by bad actors on their respective platforms. By focusing on their structural vulnerabilities, platforms can limit or quarantine malicious activity without regulating content. Identifying and eradicating coordinated inauthentic behavior does not require attribution and can be executed regardless of the motivation(s) of the actors involved. Online platforms are the only ones positioned to police this activity and, though they've made recent progress, more aggressive efforts to reduce the space for inauthentic behavior can minimize the scale and scope of evolving operations.

- **Increasing transparency and information sharing:** Since 2016, online information platforms have proved increasingly more willing to share information on foreign interference with the public and with government agencies. However, these efforts remain largely ad hoc, and the platforms should act to better institutionalize information sharing between their threat analysis teams and the appropriate government authorities, as well as with users and researchers. Public exposure of operations, while protecting user privacy, will be key to inoculating society against the effects of foreign interference.

- **Establishing standardization and effective coordination:** Facebook, Twitter, and Google continue to engage in counter-interference efforts without a unified understanding of the threats that face their community. Platforms should work to establish a more coordinated threat picture to encourage effective cross-platform cooperation. Platforms should also institutionalize community-wide communication mechanisms to encourage consistent information-sharing regarding emerging threats. Efforts to combat interference should be cooperative, not competitive, and this coordination will be key to tackle operations, which are often cross-platform, in a holistic and thorough manner.

- **Improving policies and enforcing rules clearly and consistently:** Though online information platforms are tackling inauthentic behavior and content at an increased rate, current efforts are plagued by vulnerabilities, inconsistencies, and a lack of clarity. Platforms should close the gaps in their current counter-interference efforts to ensure that new policies go past window-dressing to achieve intended outcomes. Additionally, platforms should more clearly articulate their terms of service and their responses to violations, and should consistently and transparently apply those rules. Clear communication and consistent enforcement will build credibility with users and civil society, and will demonstrate a stronger commitment to combating future interference efforts.

- **Thinking critically about future technologies:** Many of the policy updates and initiatives launched by online platforms are intended to correct the failures of the past, namely

addressing interference tactics employed during the 2016 election. However, as the threat of foreign interference continues to evolve and change, tech companies will need to build their capacity to think more proactively about how to protect users against manipulation, and about how future technologies may be exploited by hostile foreign actors. Companies should act to institutionalize this type of thinking, and should prepare to take the initiative in recognizing, countering, and publicizing new forms of interference in the future.

- **Making user protection the bottom line:** Facebook, Twitter, and Google need to improve their efforts to inform and train users in regards to the threats that face them, and the tools and tactics they can employ in response. Further, companies need to provide users with more contextual information to evaluate content and should also explain to users why this context is important. Finally, platforms will need to change the ways that they design features to emphasize user protection over ad revenue or convenience. In the past, companies have created products with the intention of retaining user attention or manipulating human tendencies, providing a significant vulnerability for exploitation. Future technologies and platform features should hold user protection as their bottom line, rather than profit.

The views expressed in GMF publications and commentary are the views of the author alone.

About the Author

Bradley Hanlon is a research assistant at the Alliance for Securing Democracy.

About the Alliance for Securing Democracy

The Alliance for Securing Democracy is a bipartisan, transatlantic initiative housed at The German Marshall Fund of the United States (GMF) that is committed to developing comprehensive strategies to defend against, deter, and raise the costs on Russian and other state actors' efforts to undermine democracy and democratic institutions. The Alliance is informed by an advisory council composed of former senior officials with experience in politics, foreign policy, intelligence, Russia, and Europe - bringing deep expertise across a range of issues and political perspectives.

About the German Marshall Fund (GMF)

About GMF The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, nonprofit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

1700 18th Street NW
Washington, DC 20009
T 1 202 683 2650 | F 1 202 265 1662 | E info@securingdemocracy.org

http://www.securingdemocracy.org/

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington • Ankara • Belgrade • Berlin
Brussels • Bucharest • Paris • Warsaw

www.gmfus.org