Flooding the Gap

How Big Tech's Failures Empowered Foreign Adversaries and Undermined the 2024 U.S. Election

December 2024

Flooding the Gap

How Big Tech's Failures Empowered Foreign Adversaries and Undermined the 2024 U.S. Election

By Jamie Neikrie and Liana Keesing

Introduction and Overview

On many levels, elections across the United States this year were a success. Election officials across the country, who had been preparing for this moment for years, stretched limited resources to deliver timely, accurate results to the nation. Systems like early voting, mail-in and overseas voting, and ballot drop boxes worked as designed, helping meet the moment. Threats of mass violence failed to materialize, and claims of widespread cheating died down as election night progressed. Republican presidential nominee Donald Trump was elected according to the rule of law and the will of the voters.

While the election process unfolded with relatively few disruptions — underscoring the resilience of our systems and the heroic efforts of election officials — the road to election night told a different story. Despite widespread attention on online foreign influence operations since the 2016 Cambridge Analytica scandal and Russian interference in the 2016 election, foreign adversaries continue to successfully exploit the failures of Big Tech and a broken information ecosystem to divide Americans and undermine our democracy and national security.

Ahead of the 2024 election, fear about the rise of generative artificial intelligence (AI) and the proliferation of deepfakes caused pundits to dub this year's contests the first "post-truth election." In many ways, these fears came to fruition. Adversaries like Russia, China, and Iran seized on divisions within the United States, amplifying false narratives about noncitizen voting, partisan manipulation of ballot drop boxes, absentee ballots, and overseas voting, and other conspiracy theories to destabilize trust in the electoral process.

On Election Day, these tactics escalated. Viral false claims about voters being bused into swing states and noncitizens voting in Philadelphia, paired with unfounded theories about open panels on tabulating machines in Milwaukee, demonstrate the precision with which foreign actors weaponized misinformation in real time to manipulate the U.S. electorate. These campaigns mirrored strategies seen in previous elections, but with increasingly sophisticated tools and narratives designed to sow confusion and discord during a critical period.

The ability of foreign adversaries to wage these influence campaigns was enabled by significant failures in the design, operations, and oversight of social media platforms. In the wake of both the 2016 and 2020 elections, and particularly after the insurrection at the U.S. Capitol on January 6, 2021, Big Tech companies promised policymakers, regulators, and the press that they would take steps to address their role in amplifying false information and fostering real-world violence. However, in the lead up to the 2024 election, that brief moment of encouragement was undermined by internal policy rollbacks, industry-wide layoffs, and intensified partisan pressure that stifled efforts to combat false information online.

Elon Musk's acquisition of Twitter (now X) marked a turning point in the tech industry's retreat from election integrity efforts, sparking a wave of industry layoffs and policy rollbacks. At the same time, partisan intimidation campaigns targeted platforms' internal teams and their external collaborators, further weakening the infrastructure needed to counter false narratives.

Seeing Big Tech's backslide, Congress could have stepped up its oversight of the sector, capitalizing on the bipartisan scrutiny that materialized in the wake of January 6. Instead, in the face of historic lobbying efforts by the tech platforms, policymakers allowed crucial reforms like comprehensive data privacy, platform transparency, and responsible safeguards for children to languish.

The result was a fractured information ecosystem that foreign adversaries leveraged to divide voters, erode trust in democratic institutions, and influence public opinion.

This report analyzes how these vulnerabilities emerged, the strategies foreign adversaries employed, and what Congress must do to ensure that the same mistakes are not repeated in future elections.

"The result was a fractured information ecosystem that foreign adversaries leveraged to divide voters, erode trust in democratic institutions, and influence public opinion."

Recommendations

Improve the design of technology platforms to create an information ecosystem that nurtures, rather than undermines, American democracy.

1. Enact design-focused legislation to slow the spread of false information online, such as virality circuit breakers, rate limits on new accounts, and alternatives to attention-based algorithms.
2. Pass the Online Consumer Protection Act, or similar legislation, to require social media platforms to establish, disclose, and maintain written terms of service (including a consumer protection program) and hold these platforms accountable for failures to uphold these terms.

Hold platforms accountable for disseminating foreign propaganda.

1. Reform clause (c)(1) of Sec. 230 of the Communications Decency Act to clarify that legal immunity does not apply to internet service providers who fail to take reasonable steps to prevent foreseeable harm to our national security or who engage in deliberate attempts to avoid learning about such harm.
2. Preserve immunity for platforms that remove access to potentially unlawful or harmful content.
3. Enact legislation that creates annual, mandatory reporting requirements for major tech platforms, with independent third-party audits.
4. Consider criminal liability for extreme cases of negligence by executives.

Increase public reporting, education, and research on the threat of foreign malign influence operations.

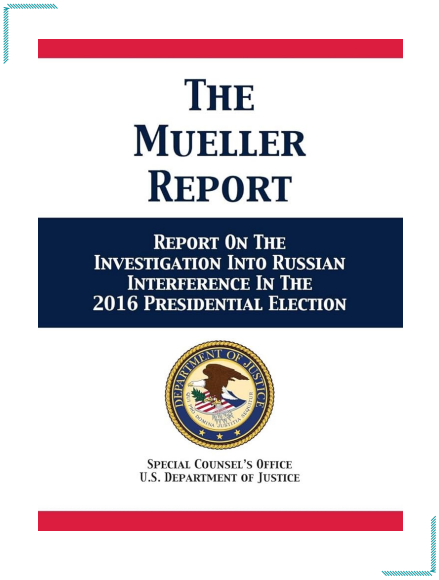
1. Pass the Platform Accountability and Transparency Act, or similar legislation, to give independent, vetted academic and nonprofit institutions the ability to conduct public data-driven research on tech platforms.
2. Establish safe harbor protections for researchers to collect public information (with privacy enhancing guidelines) from online platforms without fear of intimidation.

Restrict our adversaries' influence on social media and in the political process.

1. Require tech platforms to label state-backed accounts and advertisements (as Meta, X, TikTok, and YouTube have pledged, but often fail to do) and prohibit any advertisements from foreign-backed groups regarding the election within six months of an election.
2. Pass the Honest Ads Act, or similar federal legislation, that improves the transparency of online political advertisements to stop foreign influence in U.S. elections.
3. Strengthen the Foreign Agents Registration Act (FARA) by increasing penalties and enhancing enforcement mechanisms. Expand it to specifically cover digital influence activities, potentially by establishing a FARA compliance office within the DOJ focused specifically on online influence.

The Backdrop:

The Brief Rise and Rapid Fall of the Responsible Tech Platform



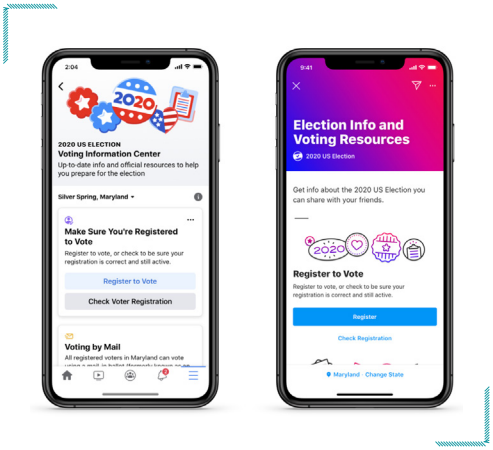
Taking place in an historic year, where 64 countries representing a combined 49% of the world's population will hold elections, the challenges facing the U.S. electoral system during the 2024 election were eminently foreseeable. Despite lessons learned from prior foreign malign interference efforts stretching back to 2014, a combination of economic and political pressures dismantled many of the safeguards established after the 2016 election to protect the U.S. information ecosystem. This left the American electoral system increasingly vulnerable to both domestic and foreign interference, with adversaries like Russia, China, and Iran exploiting these weaknesses to manipulate public opinion and sow distrust in democratic institutions.

The threat of foreign interference is not new. In 2016, Russia launched a sophisticated and aggressive campaign to influence the U.S. election, as detailed in an extensive report by the Senate Intelligence Committee. Those efforts, which the committee deemed "one of the single most grave counterintelligence threats in modern American history," included hacking and leaking sensitive political documents, targeting election systems in all 50 states, and carrying out large-scale influence operations on social media. Russian operatives successfully infiltrated election infrastructure in Illinois and Arizona, and targeted an election technology company in Florida.

Many of these operations were laundered through the Kremlin-backed Internet Research Agency, though the report produced by Justice Department special counsel Robert Mueller also found that Russian spy agency GRU used Facebook, Twitter, and email to communicate with U.S. reporters and others, often giving them access to leaked files. Russia also built out its network of proxy websites, individuals, and organizations to boost discord around conspiracies in Ukraine, California secession, and the Colin Kaepernick controversy, among other hot-button issues.

In response to these threats, Congress passed the bipartisan Countering Foreign Propaganda and Disinformation Act, creating the Global Engagement Center (GEC) within the State Department to coordinate efforts to counter foreign propaganda from adversaries like Russia and China. The Trump administration expanded these effortsby allocating additional resources for the GEC and creating an Information Access Fund to coordinate civil society groups, media outlets, federally funded research and development centers, private companies, and academic institutions to counter propaganda.

American technology companies, in turn, also launched their own initiatives to combat the foreign influence operations that had exploited their platforms. Ahead of the 2018 midterms, Facebook (now Meta) convened representatives from the biggest players in the tech industry along with



Meta's Voting Information center launched ahead of the 2020 U.S. presidential election

officials from the FBI and Department of Homeland Security (DHS). The purpose of the meeting was to strengthen ties between social media platforms and law enforcement to mitigate abuse by malicious actors. These efforts expanded in subsequent elections; ahead of the 2020 and 2022 elections, Meta launched its Voting Information Center. As part of this nonpartisan effort, Meta worked with state election officials and nonpartisan civic organizations to direct users to and ensure its center was updated with the latest, accurate election information in each state.

These public-private partnerships proved critical. During the 2020 presidential election, for example, a story went viral on Twitter with photographs alleging to show thousands of mail-in ballots being disposed of in Sonoma County, California. Researchers at the Election Integrity Partnership sprang into action, working with Sonoma County election officials to clarify that the pictures showed old, empty envelopes from the November 2018 election that were disposed of in a manner directed by law. Their reporting helped alert Twitter, which took action on many of these tweets, in line with their civic integrity policy. Later investigation into this story uncovered that Russian state-backed actors had helped amplify this false narrative. Other public-private partnerships helped uncover influence operations by the Chinese Communist Party-backed influence network Spamouflage Dragon (or Dragonbridge), which began posting in English and Spanish in the leadup to the 2020 election with attempts to discourage Americans from voting and discredit the American political system.


The New York Times

California County Enlists Social Media to Thwart a Misleading Election Photo

Officials moved swiftly when old images of discarded mail-in ballots were circulated and portrayed as new pictures.

Share full article

By Nick Corasaniti

Sept. 25, 2020

On September 25, 2020, several news outlets, including The New York Times, reported on disinformation circulating on social media. Users were sharing photographs that allegedly showed thousands of mail-in ballots being disposed of in Sonoma County, CA.

Response to January 6 and Growing Tech Oversight

While these policies and partnerships represented a significant step forward for the tech industry, they fell short of creating an ecosystem that could withstand manipulation by foreign and domestic bad actors. The events of January 6, 2021, emphasized these remaining gaps, and brought renewed scrutiny to the role that American social media platforms played in amplifying false narratives about the 2020 elections. **The bipartisan House Select Committee to Investigate the January 6th Attack identified social media's "attention-seeking, algorithmically-driven business model" and "shoddy**

content moderation and opaque, inconsistent policies," as significant drivers of the lie that Trump had won the 2020 election and the mobilization of extremist groups behind the insurrection. Although these findings were conspicuously excluded from the committee's final report, staffers and witnesses spoke publicly about their frustrations (and eventually leaked the findings), saying the committee failed to adequately hold major social media companies to account for the role they played in the worst attack on the Capitol in 200 years.

The fundamental design flaws identified by the January 6 Committee were compounded by poor judgment and slow decision making at the platforms. For example, an internal Facebook investigation from 2019 found that an experimental account purporting to represent a conservative mother in North Carolina was directed, without any prompting, QAnon content within just five days of the account's creation. Despite this realization, the company would not take significant steps to remove QAnon content for another 15 months. Other choices that Meta made — such as exempting high-reach users from key policies, disbanding its Civic Integrity team shortly after the election, and rolling back policies around election denialism during the critical certification period — added fuel to the fire.

In the aftermath of January 6, tech companies publicly acknowledged the role their platforms played in undermining trust in democracy and spurring violence. "After the violence at the Capitol erupted and as we saw continued attempts to organize events to dispute the outcome of the presidential election, we removed content with the phrase 'stop the steal' under our Coordinating Harm policy and suspended [former President] Trump from our platforms," said Facebook spokeswoman Dani Lever. However, the company later rejected a recommendation from its own Oversight Board calling for the company to "review its potential role in the election fraud narrative that sparked violence in the United States on January 6, 2021, and report on its findings." Instead, they put the onus for these reflections on "independent researchers and our democratically elected officials."

Across the board, most companies removed users who spread anti-democratic conspiracies or used their online platforms to incite violence. For example, in 2020, following petitions by civil society organizations like Free Press and the Stop Hate for Profit coalition, Meta classified QAnon as a dangerous organization and began enforcing policies that would remove the group's violent and extremist content. YouTube committed to ending the algorithmic amplification of neo-Nazi content and removed a number of known, virulent conspiracists.

Rollback of Critical Policies

In October 2022, Elon Musk completed his acquisition of Twitter (later rebranded as X). Within months, Musk slashed 50% of the company's workforce, eliminated X's Trust & Safety Council, removed the company's ban on COVID-19 disinformation, and reinstated the accounts of key election deniers, white supremacists, and extremists. These sweeping changes marked a sharp departure from the platform's previous commitments to combating disinformation and protecting democratic processes.

Musk's brazen rebuke of commitments that the tech industry had touted for years to policymakers, regulators, press, and users empowered other Big Tech companies to follow suit. Meta (the parent company of Facebook and Instagram) and Alphabet (the parent company of Google and YouTube) initiated a series of their own layoffs, including gutting key teams dedicated to platform integrity and combating the spread of false information. YouTube began allowing election denialism content to appear on the platform again, and Meta stopped enforcing its transparency rules around political advertisements. These cuts took place as at the same time that platforms began touting record revenue reports (and spending record quantities on lobbying).

The rollback of these critical policies marked a stark departure from the promises Big Tech companies had made following the 2020 election, the COVID-19 pandemic, and the January 6 insurrection. **These examples, alongside more than 130 other similar entries, are captured in Issue One's comprehensive database, Big Tech's Broken Promises.** The tracker includes new updates as of November 2024, and some of the most egregious, election-related failures are detailed in a post on Issue One's Substack.

Case Study: Meta's Closure of CrowdTangle

Social media platforms wield immense power as social, economic, and political tools, yet they remain opaque black boxes, shielded from meaningful scrutiny. We have little insight into how content is spread, amplified, or suppressed on these platforms, beyond what the tech companies choose to disclose. This lack of transparency heightens the importance of the limited tools available to policymakers, regulators, the press, and users to ensure accountability and safeguard the public interest.

In August, just weeks before voting began in the 2024 election, Meta quietly dismantled one of its most important tools for public interest monitoring and oversight. CrowdTangle, a data tracking tool Facebook purchased in 2016, made it possible for approved academics, journalists, election observers, and researchers to study activity on Meta's social media platforms. Since its launch, this tool has allowed researchers to track ISIS propaganda content; aided journalists in

identifying local voices for key stories like the COVID-19 epidemic; and helped researchers analyze Russian-backed influence operations in Africa. In 2020, The New York Times deemed it "perhaps the most effective transparency tool in the history of social media."

Meta's decision to sunset CrowdTangle in the middle of a global election year was met with confusion and concern. In a survey of tech researchers across the world, 88% expressed concern that the shutdown will impede their work or cause them to abandon key research projects altogether. Despite letters from members of Congress on both sides of the aisle, along with 181 civil society groups (including Issue One), Meta moved forward with its plan to end CrowdTangle in August, replacing it with a less powerful tool called the Meta Content Library that fewer outsiders have been allowed to access.

Despite Meta's claims, this new tool is far from an adequate replacement. It lacks much of the functionality that made CrowdTangle effective: It offers no historical data for posts, no way to track reach and engagement over time, and no ability to track posts and engagement from public figures. Access to the Content Library excludes all for-profit newsrooms, and according to survey results, only a small percentage of researchers who qualify for access have been granted it. **Put plainly, this change leaves most of the journalists, researchers, and advocates who had access to CrowdTangle without the ability to glean the same insights from Meta platforms.**

Meta isn't the only tech giant that's been limiting access to critical data tools. In February 2023, Google laid off at least a third of the team behind Jigsaw, a tool that helped track misinformation and radicalization on Google and YouTube. A few months later, X changed its policies and skyrocketed the fee for its previously-free research API to more than $42,000 a month — a prohibitive cost for most researchers and academic institutions. This decision jeopardized more than 250 projects, including other tools that relied on API access. Former Twitter CEO Jack Dorsey referred to the decision as the "worst thing we did."

Without key accountability and transparency tools like CrowdTangle, it's virtually impossible to ensure compliance with other tech legislation or measure its efficacy. In the recommendation portion of this report, we highlight other methods, such as annual independent audits and safe harbor protections for researchers that would make oversight of the tech industry clear and effective. Many of these policies have already been enacted in Europe through Article 40 of the Digital Services Act. We deserve the same transparency here in the U.S, especially from our own companies.

Attacks on Independent Researchers and Academic Institutions

After Musk's takeover of X and the wave of rollbacks and layoffs that followed, a new assault began on the independent researchers, academics, and federal agencies that helped combat disinformation and foreign propaganda in the previous elections. Musk launched lawsuits against the Center for Countering Digital Hate (CCDH) — a group that had uncovered repeated failures by X to remove antisemitism, anti-Black racism, neo-Nazism, white supremacy ideology, and other hate speech — and the state of California over a new law mandating regular transparency reporting by the major social-media platforms on their content moderation practices. He also threatened a lawsuit against the Anti-Defamation League.

Musk was not alone in these attacks, however. In *Murthy v. Missouri*, a case that reached the U.S. Supreme Court, the states of Missouri and Louisiana accused the federal government of colluding with tech companies, civil society groups, and academic institutions to censor conservative speech around previous election and the pandemic. At the same time, House Judiciary Committee Chairman Jim Jordan (R-OH) led a series of hearings and issued subpoenas that targeted these institutions, demanding internal records, including emails from students.

Despite these pressures, legal victories affirmed the importance of these partnerships and protections. Musk's case against CCDH was thrown out summarily by a federal judge, who ruled that "this case is about punishing the Defendants for their speech." And in the *Murthy* case, the Supreme Court vacated a lower court ruling that had sided with the states, with the justices deciding that the state plaintiffs lacked standing to sue — indicating that private-public partnerships to combat disinformation were consistent with the First Amendment and crucial for maintaining public health, safe elections, and combating foreign interference.

After Musk's takeover of X and the wave of rollbacks and layoffs that followed, a new assault began on the independent researchers, academics, and federal agencies that helped combat disinformation and foreign propaganda in the previous elections.

These wins did little to blunt the impact of the chilling campaign launched against independent research and tech accountability efforts. Under political pressure, Stanford University shuttered its critical Internet Observatory and laid off critical staff, including Renee DiResta, a member of Issue One's Council for Responsible Social Media. The Election Integrity Partnership, which played a key role in uncovering election interference — such as the Russian-backed story of ballot destruction in Sonoma County — announced it would not operate during the 2024 election. The backlash also came for the previously bipartisan GEC, which will shut down on December 23, 2024, due to partisan pressure. And until August 2024, federal agencies like the Department of Justice (DOJ), DHS, FBI, and the Cybersecurity and Infrastructure Security Agency (CISA) had largely stopped communicating with tech companies about global influence operations or providing them with resources to help election administrators respond to false information.

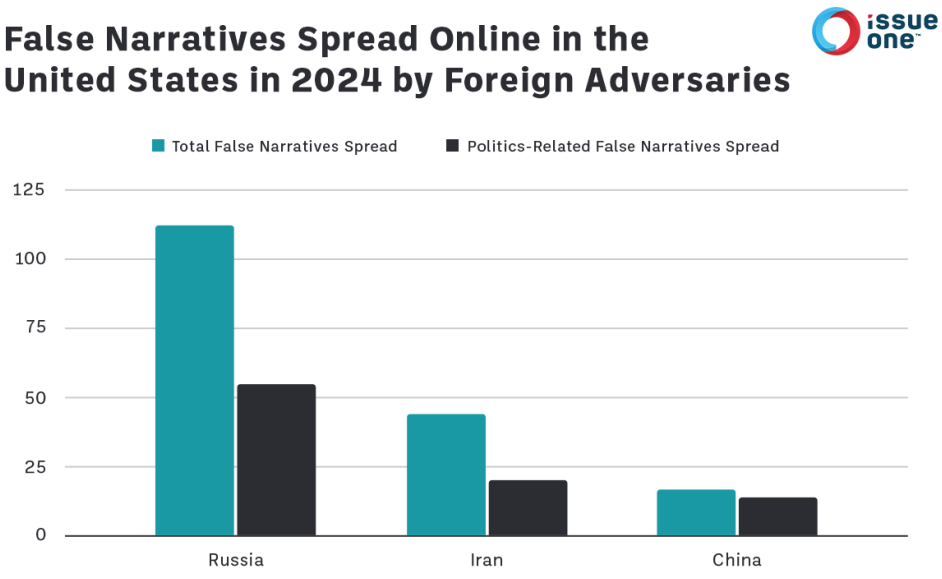
The Consequences:
Foreign Influence Operations Strike Home

The rollback of critical tech company policies, the gutting of trust and safety teams, and the erosion of public-private partnerships created a dangerously fragile information ecosystem around the 2024 election. Into this void stepped foreign adversaries intent on undermining American democracy and the rule of law.

These were familiar adversaries: Russia, China, Iran, and other authoritarian regimes. While some had a clear preference for particular candidates — with Russia reportedly favoring Trump and Iran reportedly favoring Democratic presidential nominee Kamala Harris — their primary aim was not merely to sway votes. Directly altering the outcome of an election, even with sophisticated disinformation campaigns, remains exceedingly difficult. Instead, their goals were broader and more insidious: to deepen polarization, erode trust in democratic institutions, and degrade social cohesion. By targeting vulnerable populations and exploiting existing societal fractures, these foreign actors advanced their destabilizing agenda.

On October 22, the National Intelligence Council released a declassified report warning against foreign intervention in the 2024 elections, particularly from China, Iran, and Russia. This followed a separate public service announcement from the FBI and CISA that identified hundreds of foreign-run websites and accounts intent on spreading election-related false narratives. Similar warnings were issued by the Department of State, the White House, and Microsoft.

For this report, we provide a brief overview of the specific narratives that spread by these actors and the mechanisms they used. **Just this year, at least 160 false narratives were spread in the United States by foreign governments, according to an Issue One analysis of data from the media rating**



Source: Issue One analysis of NewsGuard data.

Note: About a dozen false narratives were amplified by multiple foreign adversaries and are counted in each country's respective total.

system NewsGuard.[1] Roughly half of these narratives appear designed to fan domestic divisions about foreign affairs (such as the wars in Ukraine and Gaza), with the other half explicitly related to politics in the United States.

Russia spread the vast majority of these false narratives, accounting for at least 110 of the total narratives and 55 of the politics-focused narratives. Meanwhile, Iran amplified roughly 40 narratives (about half of which were politics-focused), and networks associated with China amplified about 20 false narratives (most of which were politics-focused). At least a dozen narratives were spread by multiple foreign adversaries.

Many of the politics-focused false narratives involved Trump and Harris, who were, respectively, the subject of 26 and 15 false narratives. Other prominent politicians — including President Joe Biden, Democratic vice presidential nominee Tim Walz, and Ukrainian President Volodymyr Zelensky — were also the subjects of false narratives.

Source: Issue One analysis of NewsGuard data

The frequency of the false narratives about the 2024 election rose during the final two months before Election Day, with a major focus on discrediting Harris' candidacy. Other recurring topics included the presidential debate, Harris' eligibility and competency as a candidate, and the actors behind the assassination attempt on Trump — all part of a broader effort to cast doubt over the legitimacy of the election.

The Influence Toolbox Grew, but Still Relied on Old Tricks

In order to spread these narratives and manipulate the 2024 information ecosystem, foreign adversaries deployed a sophisticated and multifaceted array of tools, exploiting vulnerabilities created by weakened tech platform safeguards. Below is an overview of the primary tools employed:

1. **Ad Buys and Targeted Propaganda:** Foreign actors leveraged lax ad policies on platforms to purchase political and issue-based ads, often disguising their origin through shell organizations or proxies. In September, the DOJ seized 32 internet domains that a Russian operation, known as "Doppelganger," used to buy ads on social media platforms despite supposed restrictions against this by major social media companies. As documented by various investigations from Global Witness, the Institute for Strategic Dialogue, and NYU's Cybersecurity for Democracy project, there are clear failures in the verification process that social media companies use to verify the origin and authenticity of election-related ads.

[1] These numbers take into account both false narratives and reports as filed by NewsGuard. Entries that include both a false narrative and an associated report are treated as just one entity.

2. **Bot Networks and Troll Farms:** Automated bot networks and troll farms remain cornerstone tools of foreign influence operations, playing a central role in amplifying disinformation and manipulating online discourse. These networks flooded hashtags, hijacked trending topics, and artificially inflated the visibility of fringe narratives to create the illusion of widespread support. Social media platforms' design decisions, which reward virality and attention, facilitate these efforts, creating an ecosystem where foreign actors can exploit algorithmic preferences for sensational and divisive content. While the phenomenon has been well-documented since 2016, the 2024 election saw these tactics evolve with the integration of generative AI-powered bots, which dramatically increased the sophistication and scale of these campaigns. Unlike earlier iterations that relied on repetitive, easily identifiable messaging, these bots generated contextually relevant and personalized content, making them harder to detect and counter. Troll farms also employed generative AI to create highly convincing fake profiles, complete with unique writing styles and even AI-generated profile pictures, further blurring the lines between authentic and fabricated online personas. These operations include the Chinese government's Spamouflage (also known as Taizi Flood), which parroted antisemitic messages, amplified accusations of corruption, and promoted more pro-China candidates in down-ballot races.

3. **Deepfakes and Synthetic Media:** The 2024 election also saw a sharp rise in the use of deepfake technology. Adversaries created convincing synthetic videos and audio clips of candidates making inflammatory statements or engaging in unethical behavior. Although these clips were frequently debunked, their release achieved the intended effect of spreading doubt and division. Deepfakes spread by Russia, China, and Iran elevated conspiracy theories that Trump's bodyguards had orchestrated the assassination attempt against Trump as either an attack by the deep state or, conversely, as a fake ruse to garner support for him. During the election, generative AI was used more heavily to create short-form, emotionally charged content such as memes, GIFs, and videos. These low-effort, high-impact formats spread quickly across platforms, reaching millions with little opportunity for moderation. Cartoonish AI-generated images portrayed Trump in Nazi garb and Harris in sexually suggestive and racially offensive ways.

4. **Staged Content:** In addition to the AI-enabled tools that foreign actors used to generate synthetic content, adversaries like Russia used production teams and actors to create fabricated videos of "fraud" in the U.S. election. For example, a viral video created by the Russian disinformation team known as Storm-1516 depicted an election worker in Bucks County, Pennsylvania purportedly ripping up ballots to boost the candidacy of Kamala Harris. The video was seen by hundreds of thousands of users on X and shared widely before officials were able to investigate and react. "This Russian activity is part of Moscow's broader effort to raise unfounded questions about the integrity of the U.S. election and stoke divisions among Americans," said the FBI, CISA, and the Office of the Director of National Intelligence in a joint statement. Another video depicted two Haitian migrants who claimed to have acquired U.S. citizenship and multiple Georgia IDs just six months after coming to the country; the actors claimed to be voting for Harris in multiple counties. The video, which was viewed millions of times on X, played on conspiracies that were prevalent in the 2024 election cycle, including myths of noncitizen voting and

citizens voting numerous times during early voting periods. CISA Director Jen Easterly said that the video was "Russian-produced and specifically designed to go viral and undermine American confidence in the security and the integrity of our election."

5. **Pink Slime News Networks:** Adversaries expanded the use of "pink slime" sites — low-quality pseudo-news outlets that mimic legitimate journalism — to spread disinformation. These sites produced articles laden with foreign propaganda, often disguised as opinion pieces or "exclusive" investigations, which were amplified through social media and bot networks. These websites have been deployed to target swing state populations (such as one pushed by Iranian operatives that purported to be reporting from Savannah, Georgia) to push false narratives about the election and conflict in the Middle East.

6. **Alternative Platforms and Influencer Networks:** While larger platforms like Facebook and YouTube remained venues for disinformation and influence, foreign actors also turned to smaller, less-regulated platforms such as Telegram, Gab, and Rumble. These platforms became hubs for disseminating content to extremist creators and influencers, who then re-shared it across broader networks. This strategy effectively laundered foreign narratives through domestic voices, lending them legitimacy. NBC News documented how this pipeline was used to elevate a fake video, created by the Kremlin, in which a man falsely confesses to being bribed by the Ukranians to assassinate Tucker Carlson. While first posted to YouTube, the video was immediately laundered through Kremlin-preferred platforms and websites, including Telegram and Gab. After being posted by a popular QAnon supporter on X, the video was shared by Turning Point USA President Charlie Kirk, podcaster Tim Pool, conservative commentator Benny Johnson, and comedian Jimmy Dore to their millions of U.S. followers.

7. **American Proxies and Organizations:** Foreign governments covertly paid American organizations, advocacy groups, and influencers to promote their narratives. The most notable example came from a federal indictment against two Russian nationals, who worked for a news network controlled by Russian President Vladimir Putin's government that funneled millions of dollars to an American media company in Tennessee. U.S. prosecutors alleged that the media company paid right-wing influencers for videos pushing narratives favorable to the Kremlin. The Chinese government has also used this technique by financing American advocacy organizations with pro-China messages.

Timing is also key to understanding how foreign adversaries deployed these tools. In many cases, foreign malign influence operations capitalized on natural disasters and other national crises, framing these events as evidence of government incompetence or corruption. Breaking news moments, such as the Trump assassination attempt or speculation about Biden stepping down, became prime opportunities for foreign actors to dominate the narrative. By the time legitimate information surfaced, the false narratives had already gained traction across social media platforms. The following case studies offer examples of how these tools were deployed to spread specific false narratives.

Case Study:
Trump Assassination Attempts

In the wake of the July 13, 2024, attempted assassination of Trump, many Americans took to social media to find breaking information and commentary about the shocking event. As traditional news outlets waited to communicate official and confirmed information, social media platforms were overwhelmed with a deluge of conspiracy theories, rumors, and half-truths, many driven by foreign adversaries seeking to confuse and divide the American people.

Shortly after the assassination attempt, pro-Kremlin and Russian government-backed influence networks spun into gear, promoting narratives about Secret Service failures or complicity, warning of a looming American civil war, and attempting to pin the attack on Ukranian actors. A number of Russian-backed actors, including the Russian Ministry of Foreign Affairs and Kremlin spokesperson Dmitry Peskov (with more than 500,000 followers between them) pinned the blame on the rhetoric of Biden and Democrats, who created the atmosphere in which violence against Trump was not only allowed, but encouraged.

A similar narrative was encouraged by Chinese state media, which shared English-language cartoons labeling America a "violence exporter" and implying that the shooting was emblematic of broader trends of political violence within the country that would lead to a shattering of American democracy. Many of these posts came from verified accounts and received several thousand views on platforms like X, Facebook, and Instagram. According to researchers at the Institute for Strategic Dialogue, the Chinese government also used social media to amplify allegations that Secret Service failures led to the violence. Other themes from the post-attack Chinese influence campaign in English and Spanish include criticism of U.S. media coverage of the incident and predictions that the event would help Trump win in November. Major Iranian outlets questioned whether Trump staged the incident to boost his electoral prospects (leaning into a left-wing narrative), but also promoted far-right narratives that suggested deep state involvement and insinuated that Biden was responsible for the attack.

When Ryan Wesley Routh attempted to assassinate Trump on Sept. 15, 2024, Russian actors once again looked to capitalize on the event, linking Routh to the Ukrainian government due to his rejected attempt at joining Ukraine's International Legion, a military unit composed of foreign volunteers. Using data collected by Alethea, a technology company with a focus on disinformation detection and mitigation, Issue One identified the X account "@Roosevelt177" as the user who originated this narrative on Sept. 15, 2024. But the next day, Dmitry Medvedev —

former president and prime minister of Russia and current deputy chairman of the Russian Security Council — picked up the exact same rhetoric, claiming that Routh was actively recruiting for the International Legion and potentially acted as an agent of the Ukrainian government. Medvedev has about 1.3 million followers on X and his post amassed nearly 1 million views, 18,000 likes, 5,000 reposts, and 2,000 comments.

Real-World Consequences

While foreign influence operations thrived online in the 2024 election cycle, their efforts also extended to the real world, posing real threats to frontline election workers. On Election Day, hoax bomb threats originating from Russian email domains were targeted to polling locations in five battleground states, temporarily disrupting the voting process and requiring court-ordered extended voting hours. Georgia Secretary of State Brad Raffensperger, a Republican, also identified Russian actors as the source of the threats: "They don't want us to have a smooth, fair and accurate election. If they can get us to fight among ourselves, they can count that as a victory." The bomb threats continued in the days following the election, disrupting post-election processes and instilling fear in election workers and administrators. Beyond responding to bomb threats, countering disinformation about the election — particularly false narratives spread by foreign adversaries — requires substantial extra work for election administrators that are already overburdened and underresourced, as documented throughout Issue One's Faces of Democracy campaign.

"They don't want us to have a smooth, fair and accurate election. If they can get us to fight among ourselves, they can count that as a victory."

— GA Sec. of State Brad Raffensperger

Case Study:
Foreign Adversaries Take Advantage of Hurricanes

In the immediate aftermath of Hurricanes Helene and Milton, foreign influence operations helped spark physical threats against first responders. The natural disasters, which ravaged American towns and cities from coastal and central Florida to the Appalachian regions of North Carolina and Tennessee, provided another period of confusion and uncertainty that foreign adversaries leveraged to sow discord. Shortly after Helene made landfall, false narratives emerged online taking aim at the Federal Emergency Management Agency (FEMA) and the Biden administration's response efforts. In the weeks following the disasters, experts found Russia, China, and Cuba all played a role in amplifying these narratives.

Russian state-affiliated social media accounts pushed false claims that portrayed the Biden administration as incompetent and furthered the country's geopolitical interests. Russian state media sites Sputnik and RT alleged widespread institutional failure during the response and falsely claimed that the Biden administration diverted funds for disaster relief to programs for migrants and the Ukraine war. Dmitry Medvedev — former president and prime minister of Russia and current deputy chairman of the Russian Security Council — contributed to the spread of this narrative, alleging that the domestic needs of U.S. citizens following Hurricane Milton are in competition for aid that is being used in Ukraine. Medvedev's Oct. 13 post on X garnered nearly 700,000 views, 17,000 likes, 5,000 reposts, and 2,000 comments.

This narrative was eventually spread by U.S. politicians as well. President-elect Trump repeated false claims, debunked by FEMA, that hurricane victims would only receive $750 in relief. In an X post to her four million followers, Congresswoman Marjorie Taylor Greene (R-GA) shared the same sentiment and suggested that FEMA funds were diverted to house migrants. And in a post on X that has amassed more than three million views, user "@ImMeme0," compared the debunked claim about hurricane aid to the amount the United States has provided in aid to Ukraine, Israel, and Taiwan. That post, which is still up on X, has nearly 30,000 likes, 20,000 reposts, and 3,000 comments.

China and Cuba also engaged in influence operations around the hurricanes, taking advantage of the moment to advance their geopolitical interests. Chinese-linked accounts spread AI-generated content and imagery promoting the narrative that the government spent disaster relief funds on foreign aid for Ukraine, Israel, and Taiwan. Similarly, Cuban influence operatives advanced narratives of misguided spending along with messaging that the government had abandoned its citizens.

At a moment of vulnerability and uncertainty just before the election, these coordinated attacks helped manipulate public perception, subvert public confidence in U.S. institutions and authorities, and deepened fissures.

Conclusion

During the 2024 election, our electoral system held firm — a testament to its resilience and the hard work of election officials. But that resilience shouldn't obscure a stark reality: Tech platforms, driven by a reckless "move fast and break things" ethos and exploitative business models, continue to undermine our democracy. Their profit-driven algorithms fuel division. Opaque content policies deflect accountability. And a relentless pursuit of engagement amplifies misinformation and extremism, vulnerabilities that our adversaries eagerly exploit. These practices are corroding our democratic systems, straining the functioning of our electoral process, and fracturing the cohesion of our country.

Tech companies had an opportunity, following the 2016 and 2020 elections, to establish the policies and partnerships that would ensure that our information ecosystem could no longer be weaponized against American voters by our adversaries. Instead, they went the opposite direction. Musk's takeover of X, the subsequent gutting of key policies and integrity teams by numerous platforms, and the sharp rise in political power have shown other tech executives that they don't have to live up their commitments. At the moment, they are beyond accountability.

Congress also had a chance to usher through meaningful reforms that would finally bring oversight and responsible safeguards to the tech sector. Instead, they have allowed policies with widespread bipartisan support — including comprehensive privacy protections, guardrails to protect minors, and fundamental transparency mechanisms — to languish in the face of overwhelming tech lobbying. At the same time, partisan actors in key positions of power have weaponized their authority in Congress to wage a partisan chilling campaign against the researchers and public servants who were helping to stem the tide of foreign influence attacks. In many cases, this effort has already been successful in shuttering key operations and discouraging others.

Tech platforms, driven by a reckless "move fast and break things" ethos and exploitative business models, continue to undermine our democracy.

In short, the rollback of critical tech company policies, the gutting of trust and safety teams, and an assault on public-private partnerships made the information ecosystem surrounding the 2024 election the most vulnerable the country had seen in a decade. Into this void stepped foreign adversaries looking to undermine American democracy and the rule of law.

For the continued viability of American democracy, we must reaffirm that elevating truthful, authoritative information and limiting the spread of false, conspiratorial information — especially originating from foreign adversaries — is both necessary and nonpartisan. While false information and conspiracy theories have always existed, they now thrive on platforms designed to amplify sensational and divisive content. By addressing the structural incentives and systems that allow

misinformation to dominate, we can strengthen public trust, protect democratic processes, and ensure that reliable information can effectively inform voters and civic discourse. We must also reconstitute the platforms' civil society teams, federal departments, and public-private partnerships that led this work in previous elections.

This responsibility falls on Congress and our political leaders, who must recognize that Big Tech companies cannot be blindly trusted to act in our best interests. It falls on civil society and academic institutions, who must band together to withstand political pressure and continue to fight for their constitutionally-protected right to research the spread of false information online. And it falls on platforms users and voters across party lines, 71% of whom favor platforms prioritizing the prevention of false claims over unrestricted expression.

Reclaiming this once-prized ideal will not be easy. But it is the only way.

About Issue One and Our Tech Reform Work

Issue One is a leading crosspartisan political reform group based in Washington, D.C. We unite Republicans, Democrats, and independents in the movement to fix our broken political system and build an inclusive democracy that works for everyone.

The challenges facing American democracy, including elections, are increasingly driven by the information ecosystem that dictates where Americans get their information, how they connect with each other, and who they trust. That is why Issue One, in the wake of the January 6 insurrection, launched its Technology Reform work in an effort to help build an information environment that enhances, rather than undermines, American democracy.

Much of this work is aimed at social media platforms, which promised to build a more interconnected, informed world. Instead, these platforms have become engines of division, disinformation, and extremism, fueling a wide range of challenges for our democracy: growing political polarization, conspiracy theories going mainstream, increased distrust of foundational institutions, and growing violence aimed at public servants. These harms all stem from the same core social media business model, which promotes the most inflammatory, engaging content to users in order to keep them on the platform longer and sell advertisements for more money.

Without any serious accountability or oversight, Big Tech companies have decided to put profits above the societal harms to our kids, for our communities, and to U.S. national security. In order to push for accountability and drive bipartisan reforms on Capitol Hill, Issue One formed the Council for Responsible Social Media in October 2022. Today, the council brings together Republicans and Democrats, policymakers and members of the media, impacted communities and key stakeholders to elevate a bipartisan conversation and advance impactful, achievable solutions.

The council has been instrumental in driving bipartisan reforms that would protect minors online, safeguard Americans' private and sensitive data, and create meaningful transparency standards for Big Tech platforms.

Acknowledgments

This report was written by Jamie Neikrie and Liana Keesing. Michael Beckel, Angelina Clapp, Alix Fraser, Abigail Gaetz, Oliver Ni, and Claire Woodall contributed to this report.

Design by Sydney Richards.

About Issue One

Issue One is the leading crosspartisan political reform group in Washington, D.C. We unite Republicans, Democrats, and independents in the movement to fix our broken political system and build a democracy that works for everyone. We educate the public and work to pass legislation on Capitol Hill to bolster U.S. elections, build a healthier digital information environment for our democracy, improve the ability of Congress to solve problems, strengthen ethics and accountability, and limit the influence of big money over politics.

issueone.org | | | |

Media Contact

Cory Combs
ccombs@issueone.org | (202) 204-8553


issue
one™