Defending 2020

What worked, what didn't, and what's next

By Jessica Brandt and Bradley Hanlon

G|M|F alliance for securing democracy

Please direct inquiries to
The Alliance for Securing Democracy at
The German Marshall Fund of the United States
1700 18th Street, NW Washington, DC 20009
T 1 202 683 2650
E info@securingdemocracy.org

This publication can be downloaded for free at https://securingdemocracy.gmfus.org/defending-2020/.

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

Cover design by Katya Sankow

Alliance for Securing Democracy

The Alliance for Securing Democracy (ASD), a nonpartisan initiative housed at the German Marshall Fund of the United States, develops comprehensive strategies to deter, defend against, and raise the costs on autocratic efforts to undermine and interfere in democratic institutions. ASD has staff in Washington, D.C., and Brussels, bringing together experts on disinformation, malign finance, emerging technologies, elections integrity, economic coercion, and cybersecurity, as well as Russia, China, and the Middle East, to collaborate across traditional stovepipes and develop cross-cutting frameworks.

About the Authors

Jessica Brandt is head of policy and research for the Alliance for Securing Democracy and a fellow at the German Marshall Fund of the United States. She was previously a fellow in the Foreign Policy program at the Brookings Institution, where her research focused on multilateral institutions and geopolitics, and where she led a cross-program initiative on Democracy at Risk. Jessica previously served as special adviser to the president of the Brookings Institution, as an International and Global Affairs fellow at the Belfer Center for Science and International Affairs at Harvard University, and as the director of Foreign Relations for the Geneva Accord. She is a member of the Advisory Council of the American Ditchley Foundation, a term member of the Council on Foreign Relations, and a David Rockefeller Fellow of the Trilateral Commission. Follow her on Twitter @jessbrandt.

Bradley Hanlon is a program manager and analyst with the Alliance for Securing Democracy at GMF. Brad most recently served as a Brimley Congressional Fellow in the Office of Representative Elissa Slotkin working to support the Congresswoman's work on the House Armed Services and Homeland Security Committees. He was previously a research assistant at ASD. Prior to joining GMF, he consulted for the Institute for the Study of War on Russian activity in the Middle East and North Africa. Earlier, he worked as a civilian research assistant at the National War College, and as an intern at the State Department's Bureau of Conflict and Stabilization Operations. He graduated from the University of Pittsburgh in 2016 with a bachelor's degree in history and international and area studies and a minor in Russian and East European studies. Brad studied Russian at the University of Pittsburgh and at the International University in Moscow. He earned his master's degree in security policy studies from the George Washington University's Elliott School of International Affairs.

Table of Contents

Executive Summary 3

Introduction: Setting the Stage for 2020 7

Election 2020: Assessing Efforts to Counter Foreign Interference 9

Finding 1: Platforms Do Not Have Answers to Tough Questions 9

Finding 2: Civil Society Conducts Resilience-Building Activity in the Information Space That Is Essential, But Potentially Unsustainable 12

Finding 3: Communication and Coordination on Cyber and Election Infrastructure Security Increased Substantially, But There Is Still Room for Improvement 13

Finding 4: Politicization Undermines Efforts to Shore Up Vulnerabilities, Provides Fodder for Foreign Influence Campaigns, and Reduces Trust in Democratic Institutions 15

Finding 5: Cross-sector Communication About and Public Exposure of Foreign Interference Has Improved Since 2016 16

Finding 6: Current Mechanisms to Protect Electoral Legitimacy Assume Good Faith Leadership from the Top 18

Recommendations: Building Stronger Resilience 19

Recommendation 1: Address Platform Architecture and Moderation 19

Recommendation 2: Sustain and Build on Civil Society Efforts in the Information Space . 21

Recommendation 3: Build on Improvements in Cyber and Election Security Coordination 21

Recommendation 4: Develop a Safety Net Against Politicization of Election Security . 22

Conclusion 25

Appendix A: Actions to Secure the 2020 Election 26

Public Sector 26

Executive Branch 26

Congress 32

State and Local Officials 34

Private Sector 35

Cybersecurity and Technology Companies 35

Social Media Companies 36

Civil Society and Media 42

Civil Society Organizations 42

News Media 46

Appendix B: Acronyms 50

Acknowledgements 51

Endnotes 52

Executive Summary

The 2016 presidential election served as a wakeup call to the threat of authoritarian interference, and in the years since, many segments of American society—from the federal government to private companies and civil society groups—have taken valuable steps to prepare for and counter it. Congress and the Executive Branch stood up a new government agency and multiple coordinating bodies to protect election infrastructure, while social media platforms have instituted policies to restrict the manipulation of advertisements, label misleading and false content, and slow the spread of disinformation. Working together, civil society instituted new cross-sector coordination mechanisms for election security. Yet longstanding vulnerabilities—including crippling political polarization and underfunded election jurisdictions—persist. A series of high-profile failures to prosecute the solicitation of foreign interference in U.S. elections further threaten to solidify a dangerous new norm.

Meanwhile, the threat landscape is growing more dynamic. New actors, including China and Iran, have taken an interest in adopting elements of Russia's information manipulation playbook. And that playbook is itself evolving. In 2020, Russia and Iran took active steps to influence U.S. voters, engaging in information operations—at times augmented by cyberattacks—to denigrate candidates, sow chaos and division, and reduce trust in democratic institutions.[1] New players, including Cuba, Venezuela, and other, non-state actors also took steps to influence voters and attack election infrastructure.

Most notably, domestic actors embraced disinformation tactics, as President Trump and his allies repeatedly undermined confidence in the legitimacy of the election. These events highlighted the extent to which foreign and domestic threats to democracy are related. Domestic attacks on democratic institutions and principles create opportunities for foreign actors to carry out their activities, while authoritarian efforts to increase polarization and decrease trust in institutions can create an enabling environment that is ripe for democracy-denigrating activity by domestic partisans.

For nearly a year, the Alliance for Securing Democracy has documented steps taken by the government, the private sector, and civil society to secure the 2020 election against foreign interference. Our team has collated more than 200 actions in the cyber, financial, election infrastructure, and information domains beginning in February 2020 with the Iowa Caucus and continuing through the inauguration of President Biden. Using this data, we conducted a cross-sector, multi-domain assessment to identify gaps and failures in election security efforts, as well as successes to be built upon. We identified six findings:

Platforms do not have answers to the tough questions. Ahead of 2020, social media companies implemented numerous, wide-reaching policies to try to prevent a foreign operation on their platforms. But in certain, arguably predictable circumstances, they were again caught flat-footed, suggesting that they still do not have good answers for some of the thorniest problems. In particular, the events of 2020 highlighted that:

- Platforms do not have effective mechanisms for handling a suspected "hack and leak," in part because there are few good options available to them. Platforms need to act quickly to have an impact but will not have definitive attribution in real time.
- Platforms do not have effective policies for handling an information operation run through authentic domestic voices and institutions, which implicates constitutionally protected speech.
- Labeling can inadvertently create the false impression of endorsement for misleading content or inspire confusion about the platforms' intent.
- Platform architecture drives engagement with conspiracy groups, but business incentives cut against changing that architecture.

Civil society conducts resilience-building activity in the information space that is essential, but potentially unsustainable. Civil society organizations stepped in to fill gaps between government and the private sector, monitoring the domestic information space, informing citizens of emerging disinformation tactics and narratives, and facilitating cross-sector information sharing and coordination. These activities were fueled by a high degree of public interest and considerable philanthropic support that may not be sustainable.

Communication and coordination on cyber and election infrastructure security increased substantially, but there is still room for improvement. Ahead of 2020, coordination among federal, state, and local officials, as well as with election stakeholders in other sectors, increased dramatically. Federal agencies and civil society partners also offered a range of services, support, and funding to state and local election jurisdictions. But there is more to do, starting with expanding outreach to the 7,000 jurisdictions who have yet to join the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and including strengthening defenses against cyberattacks and protecting election workers and staff.

Politicization undermines efforts to shore up vulnerabilities, provides fodder for foreign influence campaigns, and reduces trust in democratic institutions. In 2020, senior government officials appeared to politicize the threat of foreign interference with statements that misrepresented threats to the election. Politicization inhibited Congress from closing known vulnerabilities and providing regular, predictable funding to state and local election officials. A domestic disinformation campaign launched by President Trump and his allies—including some members of Congress—undermined confidence in the electoral process and provided fodder for foreign influence operations.[2]

Cross-sector communication about and public exposure of foreign interference has improved since 2016. Ahead of the 2020 election, government officials took regular action to communicate with the public about foreign interference threats and activity, as well as government responses—from proactive warnings to public announcements of retaliatory measures, such as sanctions. Social media companies exposed foreign state-sponsored information operations. Meanwhile, government, private sector, and civil society leaders directed citizens to trusted sources of information and helped prepare citizens for coronavirus-related changes to election processes.

Current mechanisms to protect electoral legitimacy assume good faith leadership from the top. Bad faith efforts from the White House and from some members of Congress undermined public confidence in the election, accomplishing the goals of foreign actors for them and providing fodder for authoritarian actors to denigrate democracy. The U.S. election system proved resilient in spite of these attacks because of the energetic work of leaders from all corners of society.

Recommendations

Closing longstanding vulnerabilities, keeping pace with evolving threats, and building resilience to new challenges is a whole-of-society task. Leaders from across sectors will need to take action to address platform architecture, strengthen civil society efforts in the information space, expand on progress in cyber and election infrastructure coordination, and construct a safety net that can protect against the politicization of election security.

Address Platform Architecture and Moderation

- Platforms should emphasize policies to slow the spread of election-related disinformation before it achieves virality. Platforms should construct mechanisms to identify harmful content before it achieves virality and to slow its spread to give time for other policy responses. Companies should expand human moderation of accounts with high potential for public harm and implement measures to remove false and misleading content from recommendation algorithms. Platforms should consider punishing repeat offenders for sharing false content by attaching labels to accounts.
- Platforms should increase transparency and information-sharing with researchers. Companies should provide more clarity around moderation policies and decisions, including making them accessible to users. Platforms should be more forthcoming about the details and impacts of architecture and algorithm changes.
- Platforms should amplify authoritative voices. Companies should take steps to identify, verify, and amplify the accounts of election officials ahead of future elections, including prioritizing content in newsfeed and recommendation algorithms. They should consider more permanent architecture changes to boost authoritative news sources in algorithms.

- Platforms should empower credibly independent oversight. Platforms should establish oversight bodies to insulate important content moderation decisions from business interests, improve transparency around decisions, and build public confidence. Oversight bodies should be granted broad jurisdiction to be responsive to users and platforms should commit to adhering to and enforcing the precedence of oversight decisions. The bodies should aim to promote healthy online discussion and protect the interests of users and the public.
- Congress should consider establishing an independent federal regulator for social media platforms. Congress should establish a federal regulator to conduct oversight of digital platforms in the public interest, focusing on protecting consumers and promoting a healthy information space. The regulator could conduct audits of platform algorithms and confirm companies are taking sufficient action to mitigate negative externalities. Congress could consider requiring companies to cooperate with the regulator as a condition of maintaining liability protections from content published on their platforms.

Sustain and Build on Civil Society Efforts in the Information Space

- Civil society organizations should consider establishing a permanent coordinating center for cross-sector information sharing. Building on the work of organizations like the Election Integrity Partnership, the center could take an active role in identifying, tracking, and flagging mis- and disinformation narratives and could serve as a clearinghouse for cross-sector information sharing. To maintain independence and credibility, the center should be funded by foundations focused on democracy, elections, and the information space. To increase sustainability, its scope of work should expand beyond elections to cover broader trends in the information space.

Build on Improvements in Cyber and Election Security Coordination

- Congress should provide additional support to authorities responsible for election security. Congress should provide sufficient funding—including in non-election years—to help states and local jurisdictions update election systems and improve their security. Congress should also ensure that Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), and the EI-ISAC receive robust support to expand outreach and deliver support to state and local jurisdictions. Congress should also consider clarifying responsibilities for federal agencies supporting election security.
- Congress should strengthen security standards and incentivize local jurisdictions to innovate. Congress should provide funds for jurisdictions to replace paperless voting machines with paper-based voting systems and should support the implementation of risk-limiting audits. Congress should also resource the EAC to expand its Voluntary Voting System Guidelines to include non-voting election technologies and should equip CISA to investigate threats to the election security supply chain. Congress should consider ways to incentivize innovation in state and local election security efforts.
- Federal and state lawmakers should invest in the protection, recruitment, and training of election workers. Lawmakers should examine ways to improve worker safety for state and local election officials and to deter threats against officials as seen in the 2020 election cycle. Lawmakers should also invest in programs to develop and retain talent in election administration, including cybersecurity trainings and certification or fellowship programs. Lawmakers should also help state and local election officials build out communications plans for public communication in future election cycles.

Develop a Safety Net Against Politicization of Election Security

- Congress should explore methods to depoliticize reporting on foreign interference. Congress should investigate mechanisms to empower non-partisan reporting of election security threats. One model to examine is Canada's Security and Intelligence Threats to Elections Task Force, which empowers senior civil servants to decide on publicly disclosing foreign interference operations.

- Congress should reinforce CISA's independence. Congress should insulate CISA from potential future political pressure by making the CISA Director a 10-year, single-term position. Congress should also require other high-ranking positions within CISA to be held by career officials rather than political appointees and should move responsibility for permanent maintenance of CISA's "Rumor vs. Reality" webpage to the EI-ISAC.
- Americans must renew their democratic culture. The United States must reinvest in democratic values, institutions, and processes. This challenge goes beyond the scope of this paper, but an important first step will almost certainly be to reconstruct civic infrastructure and establish programs that bring citizens together outside of the online environment. That should include embracing civic education and service learning.

Introduction: Setting the Stage for 2020

In the aftermath of the 2016 U.S. presidential election, revelations of Russia's "sweeping and systematic" interference efforts amounted to a wake-up call for democratic policymakers across the transatlantic space to the threat of authoritarian interference.[3] One of the most striking features of Russia's operation was the failure of actors across the spectrum to identify, counter, or respond in an effective or timely manner. Government agencies siloed information and failed to communicate with the public, private sector leaders, and even state and local election officials.[4] Major U.S. media organizations played an active—at times unwitting—role in amplifying disinformation, irresponsibly reporting on stolen and leaked material without properly contextualizing it and embedding the tweets of Russian troll accounts in their stories.[5] Social media companies were similarly caught off-guard. At first, executives shrugged off the idea that their platforms could serve as a megaphone for disinformation, before investigations—prompted by considerable pressure from Congress—revealed the extent of the problem and caused them to reverse course.[6]

In the years since the 2016 election, the U.S. government, private sector, and civil society have taken numerous steps to prepare for and counter interference efforts. Platforms have publicly taken down multiple state-sponsored information operations targeting the United States and implemented new policies to restrict the manipulation of advertisements, label misleading and false content, and slow the spread of disinformation. Civil society researchers have exposed and studied evolving foreign interference threats, identifying new actors, tactics, and vulnerabilities. Ahead of the 2018 midterms, government and civil society partners stood up new bodies for countering interference, including the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), while U.S. Cyber Command reportedly took Russia's infamous troll farm offline for several days around the election.[7] Just two weeks later, the U.S. government officially established the Cybersecurity and Infrastructure Security Agency (CISA) in part to coordinate and assist in future election security efforts.[8]

Despite these actions, vulnerabilities—including malign financial loopholes, varied election security capacities around the country, and crippling political polarization—have persisted.[9] Efforts to close them off have often fallen short or failed to materialize. At the same time, a series of signals from officials at the highest level of government have normalized the damaging notion that soliciting foreign interference will not be prosecuted, with prosecutors declining to pursue charges or investigations and failing to secure convictions on important cases.[10] And meaningful legislation to close off potential avenues for interference, including by restricting the foreign purchase of online political ads, allocating resources for postelection audits and paper ballots, and requiring political campaigns and organizations to report foreign offers of assistance, did not pass the Senate.[11]

Meanwhile, stakeholders aiming to secure the 2020 presidential election faced a threat picture that was dynamic. New actors, including China and Iran, have taken an interest in adapting Russia's playbook. Both have proven willing and capable of executing influence campaigns targeting audiences in the United States.[12] Beijing, which has adopted a more assertive approach to the information space over the course of the coronavirus pandemic, regularly trolls the United States on racial justice issues.[13] Tehran, which has developed a penchant for cyber-enabled information operations, targeted U.S. voters with an e-mail-based intimidation campaign ahead of the election, impersonating the far-right Proud Boys extremist group as part of a multidimensional campaign that aimed to denigrate President Trump, undermine confidence in the election, and exacerbate social divisions.[14] Others too—including Cuba, Venezuela, and a range of non-state actors—attempted to influence voters or impact election infrastructure.

Russia's playbook is not static. The tools, tactics, and techniques that the Kremlin and its proxies use to interfere in democratic processes have evolved, such that we are now witnessing a shift toward harder-to-detect, more carefully targeted information operations that stretch across greater swaths of the information ecosystem, likely carried out by Russian military intelligence.[15] According to U.S. Intelligence Community, Russian intelligence services and proxies—at the behest of the Kremlin—engaged in influence operations to denigrate President Joe Biden, working to funnel information through U.S. media, officials, and prominent individuals, including close associates of President Trump.[16] These domestic actors also embraced disinformation tactics: starting before voting began and lasting well after it finished, President Trump and his allies launched repeated attacks to undermine confidence in the election process.

For nearly a year, the Alliance for Securing Democracy has documented steps taken by government, private sector, and civil society to secure the 2020 election against foreign interference. Our team has collated more than 200 actions in the cyber, financial, election infrastructure, and information domains beginning in February 2020 with the Iowa Caucus and running through the inauguration of President Biden. The aim of this cross-sector, multi-domain assessment is to identify gaps, failures, and shortcomings that must be remedied, as well as to highlight successes that can be replicated and built upon.

The first section of this paper lays out important findings from an analysis of efforts to secure the 2020 election, noting the successes and failures of the government, the private sector, and civil society. The second section identifies a set of concrete, actionable recommendations for consolidating successes and mitigating failures. The paper also includes an appendix that provides a catalogue of the actions and efforts of major actors to secure the election against interference in each domain, providing supporting evidence for the paper's recommendations and a resource for researchers.

Although we aimed to paint a thorough picture of efforts to secure the 2020 election, our analysis was constrained by two inherent limitations. First, our research was restricted to information currently available in the public domain. As more is made public, our understanding and assessments may mature. Second, our analysis is bounded by our selected timeline. We focus on the immediate lead-up to and aftermath of the election, but in doing so exclude inflection points that occurred before the start of our collection, including the first impeachment of President Trump, the formation of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) and Twitter's decision to ban political ads on its platform, among others.[17]

Finally, while the aim of this assessment is to analyze efforts to counter and prevent foreign interference, events in the 2020 election cycle highlighted the extent to which domestic threats to democracy are significant and closely related. Domestic attacks on democratic institutions and principles create opportunities for foreign actors to carry out their activities, while authoritarian efforts to drive polarization up and trust in institutions down can create an enabling environment that is ripe for democracy-denigrating activity by domestic partisans. Many of the measures to prevent or mitigate foreign interference identified in this report proved relevant to addressing the homegrown challenges that were so salient in 2020, while others fell short. The recommendations that emerge from this analysis aim to help guide efforts to secure future elections against potential interference, regardless of its source.

Election 2020: Assessing Efforts to Counter Foreign Interference

The lead-up to, execution of, and aftermath of the 2020 election was characterized by energetic action by state, local, and federal officials, civil society organizations, and private sector companies to secure the democratic process. This section focuses on findings that provide a framework for mitigating future threats of foreign election interference.

Finding 1: Platforms Do Not Have Answers to Tough Questions

Ahead of 2020, social media companies implemented numerous, wide-reaching policies to try to prevent a foreign operation on their platforms—some of them effective at thwarting malign activity, others less so. But in certain, arguably predictable circumstances, they were again caught flat-footed, suggesting that they still do not have good answers for some of the thorniest problems. In particular, the events of 2020 highlighted that:

- Platforms do not have effective mechanisms for handling a suspected "hack and leak," in part because there are few good options available to them. Platforms need to act quickly to have an impact but will not have definitive attribution in real time.
- Platforms do not have effective policies for handling an information operation run through authentic domestic voices and institutions, which implicates constitutionally protected speech.
- Labeling can inadvertently create the false impression of endorsement for misleading content or inspire confusion about the platforms' intent.
- Platform architecture drives engagement with conspiracy groups, but business incentives cut against changing that architecture.

Platform Action: "Prebunking," Labeling, Content Moderation, Coordination, and Algorithm Tweaks

Ahead of the 2020 election, online platforms launched a range of policies and actions—some temporary and some permanent—to close previously identified vectors for interference. These included restricting advertisements, removing inauthentic networks, "prebunking" false narratives, promoting trustworthy election information, and labeling inaccurate content and foreign state-backed accounts.[18] Companies also ramped up engagement and coordination with government, civil society actors, and each other through meetings and other mechanisms to share information and best practices.[19]

The most interesting of these actions included efforts to change algorithms and platform architecture to prevent or slow the spread of unverified information between users. For example, days before the election, Facebook confirmed that it stopped recommending that people join groups dealing with political or social issues, which can push users toward extreme content and facilitate the spread of disinformation.[20] In October, Twitter took steps to provide users greater context and encourage thoughtful sharing, including limiting the number of tweets from non-followed accounts that appeared on users' feeds and adding friction to retweets by prompting users to "quote" tweets and add context.[21] Immediately after election day, alarmed by the proliferation of disinformation about the vote count, Facebook implemented "break glass" measures to demote harmful content and add "friction" on sharing it, thereby limiting its spread.[22]

Predictable But Tough Challenge: A Suspected "Hack and Leak"

Despite these changes, platforms found themselves unprepared for tougher, but predictable challenges, including a suspected "hack and leak" operation. In October 2020, the New York Post published an unsubstantiated article about Hunter Biden, son of the Democratic presidential nominee, which contained a cache of files and emails supposedly taken from Biden's laptop. Facebook reduced its distribution pending review of third-party fact-checkers.[23] Twitter blocked users from sharing the story altogether, and locked the personal account of Kayleigh McEnany, White House press secretary, as well as the official account of the Trump campaign, which linked to it.[24] Facing pressure from prominent conservative lawmakers and media personalities who accused the companies of censorship, both companies scrambled to respond.[25] Within 48 hours of the story's publication, Twitter apologized and changed its policy on sharing hacked materials, saying that it would only remove content shared directly by hackers or those "acting in concert with them."[26] And that instead of blocking tweets that share the underlying material, it would apply contextual labels.[27] Facebook pointed critics to its misinformation policy, which stated that the company would restrict distribution to give time for fact-checking when it has "signals" that content may be false.[28] The company claimed it had taken similar steps in the past, though not always disclosed it. Critics quickly seized on Facebook's lack of transparency about the signals it had seen, the specific actions it took to restrict distribution, how long those restrictions were in place, and the results of the fact-checking review.[29] Meanwhile, YouTube took no initial action to address the spread of related videos on its platform, eventually announcing that it would not be removing or labeling any content about the article.[30]

It remains unclear what role, if any, foreign actors played in the episode, though a recent U.S. Intelligence Community report indicates that Russian proxies and state media amplified narratives related to the story.[31] Still, as ASD Media and Digital Disinformation Fellow Bret Schafer has noted, "One can't help but think that the response of the tech platforms and media to the leak, and the subsequent firestorm those responses created, was, if not the intended outcome, at the very least a desirable one for the leakers." [32] In dealing with potential "hack and leaks" where virality is achieved rapidly but attribution may never occur, it may be the case that platforms face a problem with few good answers.

One thing was clear: the lack of transparent and consistent policy positions from the companies opened them up to additional criticism and undermined their credibility. Yet calls for consistency could prompt platforms to default to a policy that would not require action except in the most egregious cases, where materials are leaked directly onto their platforms. The episode suggests that much more thinking is needed about how to manage these tensions through policies that are transparent and uniform, but also effective and responsive to context.

Predictable But Tough Challenge: Disinformation from Domestic Actors

The events of 2020 also reveal that platforms do not have effective policies for handling another predictable challenge: information operations emanating from authentic domestic voices and institutions, which implicate constitutional protections on expression and fraught political dynamics. When a broad domestic disinformation campaign alleging election fraud erupted across platforms on and immediately after election day, companies were caught flat footed. As election results were tallied, allies and supporters of President Trump began to publicize a range of conspiracy theories across social media alleging voter fraud, suppression, and manipulation.[33] On Twitter, conservative influencers helped hashtags like #stopthesteal and #sharpiegate, which referred to a quickly debunked voter suppression claim, go viral. Videos claiming the election was rigged spread widely on YouTube.[34] On Facebook, groups sharing false information about the election exploded in membership. One such group, "Stop The Steal," amassed over 320,000 followers in less than a day, for a time gaining 100 new members every ten seconds, making it one of the fastest-growing groups in Facebook's history.[35]

Platforms deployed emergency policies and actions to try to stop the spread of false claims. On November 5, Facebook implemented its break-glass measures and made changes to its newsfeed algorithm to boost authoritative content.[36] The change increased the weight that Facebook's news feed algorithm assigned to an internal "news ecosystem quality" score. It resulted in a decrease in traffic to hyper-partisan sites and an increase in traffic to authoritative publishers, including CNN, NPR and New York Times.[37] Twitter attached labels to tweets spreading false information, including 300,000 posts during a two-week period around the election.[38] It was more than a month after election day before YouTube announced that it would crack down on baseless claims that errors or widespread fraud changed the outcome of the vote. Until December 9, it stood by its decision to allow those claims to remain on the platform.[39] YouTube said it was trying to strike a balance between "allowing for a broad range of political speech and making sure our platform isn't abused to incite real-world harm or broadly spread harmful misinformation."[40]

These actions were too limited and too late. Election fraud claims spread rapidly and haphazardly across platforms. On Facebook, numerous other groups emerged in place of “Stop The Steal,” seizing on the popularity of the narrative. These included “Stop The Steal 2.0,” which gained more than 70,000 followers in less than 24 hours, and generated some of the site’s most popular posts in the days after the election.[41] Previously unrelated groups were also rebranded to focus on the “Stop The Steal” movement. As the Atlantic Council’s DFRLab reports, groups focused on coronavirus lockdown protests and other issues, such as “Boot Pelosi,” were “retrofitted to deliver misinformation about the election and to organize rallies.”[42] On Twitter, allies and influential supporters of President Trump, including several members of Congress, quickly adopted the narrative, helping it go viral.[43] Despite Twitter’s efforts to label misleading tweets, election fraud narratives spread rapidly, with #stopthesteal tripling in use on November 5. The same day, three of the top ten hashtags on the platform promoted claims of election fraud, and the most-shared links led to hyper-partisan sites including Breitbart News and The Gateway Pundit.[44] On YouTube, related videos generated nearly 300,000 engagements across other platforms and drew in millions of views in the weeks between the election and YouTube’s decision to take action on December 9. Stop the Steal engagement online spiked around a series of rallies in November and December that eventually culminated in rioters storming the U.S. Capitol on January 6, 2021.[45]

While some of the blame for the virulent spread of false election narratives lies at the platforms’ feet, much of it belongs elsewhere. Election disinformation originating with domestic actors, especially disinformation endorsed by political leaders at the highest levels, poses an especially fraught challenge for platforms. That’s because these activities implicate constitutionally protected political speech. Companies do not want to be in the position of removing political speech, and citizens should not want them to. Unlike foreign interference operations, domestic activity of this sort often does not rely on coordinated inauthentic behavior that violates platform policies and can be policed as such.

Labeling: A Favored But Fraught Approach

Ahead of the 2020 election, platforms regularly deployed labels to check false information and inform users without removing or restricting content. For both Facebook and Twitter, they were the most frequent tool for countering false narratives around the election.[46] Labels are an enticing solution for platforms, enabling them to take action to counter false narratives without removing or hiding content, which can have stark implications for free speech and prompt swift backlash. Yet platform labeling efforts were less than fully effective, and at times potentially counterproductive, for three main reasons.

First, labels often proved ineffective at reducing or slowing the spread of false information. For example, according to internal data from Facebook, labels on President Trump’s claims of election fraud had only a marginal effect on reducing engagement, but did nothing to “change shares by orders of magnitude.”[47] One analysis found that tweets from President Trump with labels spread widely—more than tweets from the president without them.[48] Delays in the application of warning labels as a result of difficulties with fact-checking or verification may be a contributing factor.[49]

Second, while certain labels can help reduce the sharing of false information, implementing labeling consistently and comprehensively is nearly impossible at scale. As a result, platforms often fail to label some harmful content or accidentally mislabel truthful posts. Research indicates that placing labels on just a limited selection of harmful content is counterproductive, as it leads users to believe that all content without a label has been checked and verified, even if it has not.[50] The use of AI-driven labeling systems, which greatly increase labeling capacity, also poses problems. Ahead of the 2020 election, Facebook used an AI system to apply labels to election-related content. The system applied generic labels to most relevant content, but it struggled to identify and properly label some false content, resulting in mislabeling that undermined the company’s efforts.[51]

Third, as the Election Integrity Partnership observed, the use of labels was inconsistent across platforms, even when the platforms had similar policies.[52] This created discrepancies between the way content was treated on varying platforms, allowing false information to thrive.

Platform Architecture Drives Profits and Engagement with Conspiracies

Changes to platform architecture were among the most interesting interventions in the 2020 election cycle. These policies included Twitter's introduction of "speedbumps" to slow down sharing by prompting users to quote tweets instead of sharing them without context.[53] Facebook's changes to its newsfeed algorithm after election day led to greater visibility for established publishers, such as NPR, CNN, and the New York Times, while reducing the spread of content from hyper-partisan sites.[54] That algorithm adjustments were necessary to limit damage to trust in democratic institutions suggests that more permanent changes are necessary.[55]

Platforms have been reluctant to make fundamental changes to their algorithms on their own, because doing so would cut against their business interests. Facebook reportedly rejected stronger changes to its architecture and newsfeed algorithm that could have further reduced the spread of harmful information because it would limit engagement, and as early as mid-December reversed the changes it made to promote authoritative content after the election.[56] The company also reportedly knew that its "Groups" feature was plagued with conspiratorial narratives, hateful content, and calls for violence, but took only limited action ahead of the election and the events of January 6, despite warnings from employees and researchers.[57] In December, Twitter similarly rolled back its feature prompting users to "quote" tweets rather than retweet, citing in part an overall decrease in sharing.[58] This suggests that platforms will not make necessary adjustments under the current set of incentives.

When platforms do adjust their architecture, transparency is often lacking. Facebook provided little information about adjustments to its algorithms surrounding the election, leaving both users and researchers unsure of the nature and duration of the changes and without data on their impacts.[59] As a result, assessments of any such changes tend to be made by the platforms themselves without external review or input. For example, despite Facebook's claims that it had stopped recommending all "political content or social groups" ahead of the election, researchers discovered that the platform continued to recommend such groups through December, including some containing conspiracy theories about election fraud and calls to violence against public officials.[60]

This reluctance to share information comes in part because when platforms have taken action to address architecture, they have often come under fire from politicians claiming targeted censorship, despite a lack of evidence to support such claims.[61] As researchers have noted, fears of this criticism may have led platforms to pursue less aggressive labeling strategies ahead of the election.[62]

There is another, perhaps more fundamental dynamic at play. Conspiratorial and false content drive engagement and keep users coming back. The spread of that content is not driven by manipulation but by algorithms doing what they are designed to: keep users clicking so that they see more ads. Policies that restrict the spread of bad information improve the quality of conversation on social media platforms, but decrease engagement and draw partisan criticism, thus harming profitability. Around the 2020 election, adjustments to platform architecture were too little and too late to stop the spread of false narratives questioning the integrity of the election. Without independent, non-partisan oversight and incentives to prioritize the public good—as well as disincentives for ignoring negative externalities—it is unlikely that platform companies will take the necessary steps to close off vulnerabilities to disinformation.

Finding 2: Civil Society Conducts Resilience-Building Activity in the Information Space That Is Essential, But Potentially Unsustainable

Throughout the 2020 election cycle, civil society organizations conducted resilience-building activity that filled important gaps between the government and the private sector—monitoring the domestic information space, informing citizens of emerging disinformation tactics and preparing them for false narratives, and facilitating information sharing and coordination across sectors. These activities were fueled by a high degree of public interest and considerable philanthropic support. It is a model that generated substantial, impactful activity, but it may not be a sustainable one. Institutionalizing these efforts would pose considerable challenges, given concerns around rights to privacy and free expression.

High Impact Efforts

Among the most impactful civil society efforts in this space was the Election Integrity Partnership (EIP), a coalition of research organizations that aimed to foster real-time information sharing between researchers, civil society organizations, social media platforms, government agencies, and election officials.[63] It played an important role in flagging harmful content for social media companies. And it communicated regularly with the public, producing real-time analyses of disinformation tactics and narratives and holding frequent public briefings.[64]

Myriad other civil society organizations—from Election SOS to the National Task Force on Election Crises —provided election officials, journalists, and domestic audiences with tools to identify and counter mis- and disinformation.[65] The Disinfo Defense League, a network of civil rights and media literacy groups, created and distributed educational materials to help build resilience to false narratives in communities of color, recognizing that those communities are often disproportionately targeted by disinformation.[66] The bipartisan National Council on Election Integrity launched a $20 million public education campaign aimed to emphasize the security of the 2020 election.[67]

These efforts amounted to a higher degree of coordination and preparedness across sectors than in 2016 when information was siloed and little was shared with the public. For example, in 2016 one of the Kremlin's most impactful fake personas, "Alice Donovan"—which was used to leak stolen materials on Facebook in the months before election day—was identified and tracked by the FBI as early as the spring of 2016.[68] But it was not terminated until the New York Times flagged it in late 2017, 15 months after the Kremlin's operation burst into public view.[69] Donovan's corresponding Twitter account remained active until July 2018, when the Department of Justice exposed the persona in a public indictment of Russian military intelligence officers.[70] In 2020, independent civil society coalitions worked to prevent similar failures by closing coordination gaps between government, media, and private sector actors, while providing regular updates to the public.

Civil society efforts to protect the 2020 election were both innovative and inspiring. The challenges posed by concerns about foreign interference, false and anti-democratic claims by then-President Trump, and the coronavirus galvanized an intense, whole-of-society focus on protecting the election. These efforts need to be sustained and solidified in ways that ensure coordination and communication continue in future election cycles without compromising the independent credibility of civil society in the information space. That is important, because while government agencies can provide important attribution or analytical capabilities to help identify foreign threats and intentions, democratic values rightfully limit government activity in investigating domestic content or guiding platform decisions regarding content takedowns.

Finding 3: Communication and Coordination on Cyber and Election Infrastructure Security Increased Substantially, But There Is Still Room for Improvement

Ahead of the 2020 election, the U.S. government, private sector, and civil society organizations made substantial progress in coordinating on election infrastructure and cybersecurity. New institutions and agencies played an important role in facilitating communication and cooperation among federal, state, and local officials, and with political campaigns.

Improvements in 2020: Cross-Cutting Coordination and Assistance

Among the most shocking and apparent failures in 2016 was the lack of cross-government and cross-sector communication and coordination regarding imminent, active threats. For example, as the Senate Intelligence Committee's (SSCI) investigation into Russian interference in 2016 revealed, Russian cyberattacks actively "exploited the seams between federal authorities and capabilities, and protections for the states."[71] The FBI and Department of Homeland Security (DHS) alerted states to ongoing and potential cyberattacks targeting election infrastructure, but SSCI reported that these warnings "did not provide enough information or go to the right people." [72] In the wake of this dereliction, the federal government and civil society partners established new mechanisms to close gaps between federal and state authorities, including CISA and the EI-ISAC. These mechanisms were established prior to the window of analysis for this project, but their subsequent activity provided substantial data for analysis.

Coordination Across and Between Levels of Government

In 2020, coordination among federal, state, and local officials, as well as with stakeholders in other sectors, increased dramatically. CISA and EI-ISAC built and maintained extensive relationships to open lines of communication for sharing information and best practices. This began well before election day. In February 2020, CISA launched its #Protect2020 Strategic Plan, which centered on direct engagement with state and local officials to prepare for and mitigate threats to the upcoming election.[73] As part of the plan, CISA provided regular situational awareness updates and shared guidance for security and incident response with state and local jurisdictions.[74] EI-ISAC also provided weekly news alerts and cybersecurity spotlights for members, as well as access to secure portals for information sharing.[75]

These efforts picked up as election day approached. EI-ISAC hosted a joint "virtual situational awareness room" that brought together hundreds of election officials, CISA and EI-ISAC staff, social media company staff, and political party representatives to share information, monitor threats, and provide guidance around election security in the hours before, during, and after the election.[76] EI-ISAC also operated an election day war room with incident-response, intelligence, and engineering teams on standby to monitor threats and provide support to state and local members as needed.[77]

Assistance to Election and Campaign Officials

Federal agencies and civil society partners offered a wealth of resources and assistance to state and local jurisdictions, as well as to campaigns, to help secure and carry out the election, providing support that officials may not have otherwise had. CISA offered a number of services, including cybersecurity advisers and vulnerability assessments, continuous system monitoring, cybersecurity intrusion and detection services, risk assessment tools, and tabletop exercises.[78] And as the coronavirus arrived in the United States in the spring of 2020, CISA worked closely with the Election Assistance Commission (EAC) to prepare states for a substantial shift to voting by mail and changes to in-person voting using guidelines developed by the Centers for Disease Control and Prevention (CDC). These efforts included plans for how to initiate a substantial vote-by-mail program and cybersecurity checklists tailored for individual states.[79] The Office of the Director of National Intelligence (ODNI) also provided security briefings and support—along with other federal partners—to political campaigns ahead of the election.[80]

EI-ISAC provided members with a similar range of services, often in concert with federal and private sector partners. This included end-point detection and response capabilities, network monitoring, domain blocking and reporting services, technology recommendations and guides for equipment procurement, free training opportunities, vulnerability assessments, and consulting services, among many others.[81] A post-election report from the U.S. Intelligence Community credited improved cyber defenses and trainings for officials with helping to thwart foreign cyber operations.[82] Looking forward, the EI-ISAC also partnered with the EAC and election leaders in several states to pilot a technology verification program that will hopefully lead to rapid security assessments for non-voting election technologies, including electronic poll books, election night reporting websites, and electronic ballot delivery systems.[83]

Other civil society organizations, often in cooperation with federal and private sector partners, provided training and resources to election and campaign officials. Professional organizations, including the National Association of Secretaries of State, the National Association of State Election Directors, and the National Association of Counties offered best practices and helped inform and prepare members, while entities such as the Center for Tech and Civic Life and the National Association of Election Officials offered training and other support to state and local officials.[84] Organizations like Defending Digital Campaigns worked with private sector partners, including major tech and cybersecurity companies, to provide low-cost and free cybersecurity services, training, and guidance to political campaigns.[85]

Remaining Gaps: Building Capacity, Strengthening Cyber Defense, Protecting Election Workers

These efforts should be applauded, but there is still more to do. The first place to start is expanding on the success of outreach to election jurisdictions in 2020. Almost 3,000 state and local election authorities had joined the EI-ISAC as of November 2020, but there are more than 10,000 jurisdictions that run elections across the country.[86] These jurisdictions range in size from towns with just a few hundred registered voters to Los Angeles County, which has nearly five million.[87] As a result, the cyber defensive capacity of these authorities to stymie bad actors varies greatly.[88] Jurisdictions also have varying levels of appreciation for the threat that nation-state attacks pose and getting federal security resources to small and medium-sized counties, as well as smaller voting technology vendors remains a challenge.[89] According to a report by the Department of Homeland Security Inspector General, despite substantial progress, CISA did not have the capacity to provide adequate support to all of these authorities as they worked to secure their infrastructure ahead of the election.[90] As the report notes, insufficient resources and staffing "hindered CISA's ability to provide timely assistance to state and local election officials."[91]

Second, the United States needs a layered defensive strategy to more successfully prevent or limit future cyberattacks, as is clear in the wake of the recent SolarWinds hack, which went undetected by the U.S. government.[92] While there is currently no evidence that the SolarWinds attack impacted election offices, election systems in the United States remain a potential target for foreign state-sponsored actors and are vulnerable to similar supply chain attacks.[93] As director of the Stanford Internet Observatory Alex Stamos has pointed out, the United States still disproportionately invests in cyber offense as opposed to defensive security efforts.[94] Going forward, the U.S. government will need to make additional investments in cyber and election security, as well as efforts to harden the election technology supply chain against potential attack.[95]

Finally, more must be done to protect election workers and other staff who play an essential role in election security.[96] In the wake of the 2020 election, President Trump and allies targeted local and state election workers with an unfounded domestic disinformation campaign, leading to targeted harassment and threats of violence against poll workers across the country.[97] These attacks greatly reduced trust in election workers and many officials worry will hamper future recruitment efforts for positions that are often stressful, require long-hours, and offer low pay.[98] Ahead of future elections, federal and state lawmakers should work to strengthen existing laws to protect election officials and should consider providing additional funding to assist with election administration.

Finding 4: Politicization Undermines Efforts to Shore Up Vulnerabilities, Provides Fodder for Foreign Influence Campaigns, and Reduces Trust in Democratic Institutions

Ahead of the 2016 election, partisan disagreements over whether to disclose interference activity hindered communication with the public regarding Russian activities.[99] As a result, the extent of Russia's interference was not publicly known until months and years later. While a number of policies and an increased focus on foreign efforts to undermine the election made threat information sharing more prevalent in 2020, continued politicization of the threat inhibited countermeasures, undermined confidence in election security, and may even have misinformed the public.

Ahead of the Election, Several Officials Took Actions That Politicized the Threat of Foreign Interference

- In February 2020, Attorney General William Bar announced that he would require any investigations into campaigns receiving foreign assistance to gain his personal approval, drawing concern given his close relationship with then-President Trump and previous Russian attempts to support the Trump campaign.[100]
- In August 2020, the Director of National Intelligence announced that he would scale back congressional election security briefings.[101]
- In fall 2020, Trump Administration officials' public statements regarding foreign interference threats seemed to elevate the threat posed by China, based on little evidence, while downplaying the threat from Russia.[102] Post-election reporting from the Intelligence Community revealed that China did not engage in election interference or influence operations targeting the election, while both Russia and Iran did so actively.[103]
- In January 2021, a post-election report from the analytic ombudsman in the Office of the Director of National Intelligence (ODNI) confirmed that both analysts and political officials acted based on politicized interests in the assessment and briefing of election threats. The report noted that a hyper-partisan environment and pressure from political leaders led to actions that "had the effect of politicizing intelligence, hindering objective analysis, or injecting bias into the intelligence process." It argued that analysts became reluctant to share analysis that would support policies they disagreed with, while political appointees sought at times to politicize and misrepresent intelligence to Congress and the public.[104]

Ahead of and in the aftermath of the election, President Trump and other officials, including members of Congress, also called into question the security and legitimacy of the election, often in direct contrast to statements from election officials highlighting facts otherwise.[105] President Trump and his allies turned the White House stage into a megaphone for a disinformation campaign to undermine confidence in election results for his own benefit. Lawyers linked to the Trump campaign weaponized absurd and unfounded false claims of foreign interference in the election, supposedly from Venezuela and Germany.[106] A substantial number of members of Congress picked up on and shared these narratives, deliberately misleading the public to support President Trump at the cost of trust in the country's democratic institutions. In the wake of the election, President Trump also fired officials that publicly refuted his claims of election fraud, including most notably CISA Director Christopher Krebs.[107] Krebs and other officials held critical roles in election security, but were dismissed for daring to refute falsehoods about the integrity and results of the election.

Politicization similarly inhibited Congress from passing substantial legislation to combat foreign interference ahead of the election. Several bills focused on countering foreign attempts to undermine the election never moved past the Senate, while even small provisions related to the subject were cut from the National Defense Authorization Act (NDAA) to appease President Trump.[108] Politicization undermined congressional attempts to fund adaptations to election security and processes during the coronavirus pandemic. Despite pleas by experts and bipartisan election officials for additional funding, Congress failed to provide adequate support.[109] While Congress did include additional funds in the CARES Act, these funds were subject to a required state match, leaving many states unable to use them as quickly or effectively as they otherwise could have.[110] Additional election security funding and language to remove the state required match was included in the HEROES Act, which passed the House, though no compromise bill was passed ahead of the election.[111] Due to a lack of funding, many election officials turned to civil society groups, like the Center for Tech and Civic Life, which provided hundreds of millions in funds through grants to 2,500 jurisdictions.[112]

The failure of U.S. lawmakers to adequately support state and local election officials during the coronavirus pandemic could have led to an election meltdown amid worries over the pandemic and a president who openly questioned the election without justification, while the politicization of foreign interference from the White House and other national political figures damaged confidence in the election results, process, and officials.[113]

These failures left the door open for foreign actors to seize on false narratives and to discredit democracy writlarge, while lies about the election eventually culminated in the storming of the Capitol on January 6 by conspiracy theorists bent on overturning the election.[114]

Finding 5: Cross-sector Communication About and Public Exposure of Foreign Interference Has Improved Since 2016

In the months leading up to the 2020 election, government, media, and private sector actors took proactive steps to communicate with the American people about the developing threat of foreign interference.

In 2016, both government and private sector actors repeatedly missed opportunities to inform the public about foreign interference activity, leaving citizens in the dark about foreign efforts to target and influence them. The Obama Administration, concerned that a public announcement of Russian actions could damage trust in the election and unable to reach bipartisan agreement with Republican congressional leaders who were against publicly exposing Russian cyberattacks, instead delayed announcing evidence of interference.[115] While it is impossible to know what the impact of more public exposure would have been, without such information journalists readily reported on stolen material leaked by Russian intelligence services without proper contextualization. Meanwhile, social media companies failed to recognize the malign activity taking place on their platforms or downplayed it.[116]

In contrast, in 2020, government actors regularly communicated with the public about malign actors and activity. Officials from the Office of the Director of National Intelligence (ODNI), FBI, CISA, and others provided regular public updates highlighting threat actors, exposing influence efforts and activities, flagging potential avenues for interference, and updating the public on the steps that federal agencies were taking to secure the election.[117] In the wake of an Iranian campaign to impersonate a far-right group and intimidate voters, U.S. officials provided rapid attribution for the operation, publicly identifying the Iranian effort within 27 hours of the incident—the fastest disclosure of attribution by U.S. officials to date—quickly informing citizens.[118] Officials also reassured the public that the campaign posed no threat to the election, and the FBI and CISA followed up days later with a cybersecurity advisory revealing how Iranian actors had accessed voter information and providing guidance on mitigating the threat.[119]

In the months before the election, the U.S. Treasury also sanctioned Ukrainian lawmaker Andrii Derkach, who it described as a "Russian agent," for attempting to interfere in the election by spreading false information and narratives about then-candidate Joe Biden.[120] Derkach's efforts were previously exposed by National Counterintelligence and Security Center (NCSC) Director William Evanina.[121] These actions sparked bipartisan calls for domestic actors not to weaponize Derkach's narratives, which may have deterred or weakened attempts by U.S. lawmakers and political actors to seize on the Kremlin-backed operation to influence the election.[122]

Private sector actors also provided regular, public reports on foreign interference throughout the election cycle. Technology companies and cybersecurity firms like Microsoft, Google, and Cloudflare monitored for hacking attempts targeting presidential campaigns, often publicly flagging attempted hacks and probing attempts and providing attribution when possible.[123] Facebook and Twitter also took steps to remove inauthentic accounts and networks from their platforms ahead of the election, with Facebook providing short explanations, along with sample content and tentative attribution to foreign actors.[124] A post-election report from the U.S. Intelligence Community also noted that proactive information sharing between government and social media platforms facilitated quick takedowns and exposure of foreign interference efforts.[125]

Apart from exposing foreign interference, government, private sector, and civil society actors also took action to point voters to trusted sources and information about the election. The #TrustedInfo2020 campaign played a major role in this effort. The campaign—organized by the National Association of Secretaries of State (NASS)—helped spur action from actors across the spectrum, including platform companies, government agencies, research institutes, and other civil society organizations to help direct voters to local government and election officials for information about voting processes and results.[126] Journalists and media companies also played an important role, in large part preparing voters for interference threats and for adjusted election processes, timelines, and the delayed reporting of results. News outlets also dealt much more successfully with reporting on potentially stolen material, with major reputable organizations publicizing improved policies and many journalists producing careful and reserved coverage of the New York Post's Hunter Biden story and other election-related stories.[127]

This improvement in public communication represents important progress, but it was also hampered at times by politicization, which distracted from efforts to expose malign activity. Disputes over congressional briefings and public statements on interference from the Director of National Intelligence and other officials also undermined public trust in election security efforts.

Finding 6: Current Mechanisms to Protect Electoral Legitimacy Assume Good Faith Leadership from the Top

Current mechanisms and norms to preserve election security and maintain confidence in the legitimacy of the vote rely heavily on good faith leadership. In the lead-up to and aftermath of the 2020 election, state and local election officials around the country and key executive branch leaders worked diligently to protect the election and to build trust among citizens in the electoral process. Bad faith efforts from the White House and from some members of Congress undermined public confidence. These efforts accomplished the goals of malign foreign actors for them, as officials and state media from Russia, China, and Iran seized on the false claims of fraud and chaotic transition to denigrate democracy in the United States and around the world.[128] The U.S. electoral process proved to be resilient in spite of these attacks. However, the President's actions to undermine the election also revealed the fragility of our democracy. The presidency is a persuasive tool and political power in the hands of bad faith actors is a significant threat to democratic norms, as the events of January 6 showed.

Recommendations: Building Stronger Resilience

Preventing the continuation of attacks on democracy will require changes and recommendations that go beyond the scope of this analysis. However, it is clear that an important starting point will be to generate a renewed interest, faith, and investment in democracy and democratic values. It will also require substantial efforts to reconstruct an information space that elevates the truth and that is conducive to the healthy public discourse on which democracy depends. Finally, it will require the United States to assess with humility the shortcomings of its current institutions and to institute reforms as necessary to ensure that its government transparently delivers upon its promises to citizens.

Energetic and dedicated activity from public, private, and civil society actors contributed to securing the 2020 election. To close remaining vulnerabilities, keep pace with a rapidly shifting threat landscape, and build resilience to current challenges, action will be required from all corners of American society—from platform companies to Congress, the executive branch, state and local officials, and civil society, including researchers and journalists. This activity should include addressing platform architecture, strengthening civil society efforts in the information space, expanding on progress in cyber and election infrastructure coordination, and constructing a safety net against the politicization around election security.

Recommendation 1: Address Platform Architecture and Moderation

Platforms made numerous changes to their policies in an effort to curb mis- and disinformation around the 2020 election. But in several circumstances—some of them predictable—responses were flat footed. Inconsistent enforcement of unclear policies around difficult challenges, as well as weak interventions to counter emerging false narratives, undermined efforts to stem those narratives, reduced platforms' credibility, and eroded the public's trust. In the future, platforms must do more to improve transparency, slow the spread of election disinformation before it achieves virality, and enable credible independent oversight. Government must take an active role in creating incentives for platforms to employ architecture that supports, rather than undermines democratic institutions.

Platforms Should Emphasize Policies to Slow the Spread of Election Related Disinformation Before It Achieves Virality

To better counter mis- and disinformation around future elections, platforms should embrace policies to slow the spread of harmful content before it achieves virality. This should include constructing mechanisms to identify potentially harmful content before it goes fully viral and introduce measures to slow its spread to give fact-checkers the time to review and address false information—as Facebook attempted to do around the New York Post story.[129] This oversight will need to be built into newsfeed and recommendation algorithms to ensure that content is identified quickly, but companies should also expand targeted human moderation of influential accounts with the greatest potential for public harm.[130]

Platforms can also do more to restrict the spread of conspiracy theories while protecting free expression by implementing "Do Not Recommend" policies that remove false and misleading content from recommendation algorithms without stripping it from the site, as Renee DiResta has noted.[131] Where companies do decide to attach labels to content, platforms will need to use strong, decisive language, and should consider implementing policies to introduce friction to sharing provably false claims. Platforms could also work together to establish standards for label language and format and to coordinate consistent enforcement during election periods. As the Election Integrity Partnership has recommended, platforms should also consider punishing repeat offenders for sharing false content by applying warning labels to the accounts themselves that appear on all shared content.[132]

Platforms Should Increase Transparency and Information-Sharing with Researchers

To build credibility and trust in their decisions, platforms should increase their transparency around content moderation approaches by educating users on mis- and disinformation policies, providing examples and case studies to illustrate them, and creating consolidated and navigable guides for their rules and standards that are accessible to both users and researchers.[133] Platforms can also do a better job of explaining moderation decisions in real-time, providing consistent communication about important actions to label, remove, or restrict content. They can also share evidence and the rationale behind major decisions and changes, rather than simply point to policy language.[134] Finally, platforms should improve communication about the nuts and bolts of major algorithm and architecture changes, including information on the duration, specific changes, intended effects, and follow-up reports on impacts.

Platforms can also improve information sharing and transparency with trusted researchers, who can help identify emerging trends and evaluate the effectiveness of policy responses. Platforms could share removed or labeled content, for example, while taking appropriate steps to protect user privacy, as well as policy details, and results of internal assessments on their efficacy to advance the development of evidence-based responses.[135]

Platforms Should Amplify Authoritative Voices

Ahead of 2020, platforms engaged in a range of activities to "prebunk" false narratives and steer users to authoritative content. Companies should build on these efforts, taking steps to identify, verify, and amplify the accounts of relevant officials. Election officials could be prioritized in recommendation and newsfeed algorithms, and they could be given advertisement credits to share educational information within their jurisdiction, as suggested by the Election Integrity Partnership.[136] To help combat false narratives writ-large, platforms should consider permanent changes to algorithms to help boost authoritative news sources and content, as Facebook did temporarily in reaction to the rise of conspiracy theories after the election.

Platforms Should Empower Credibly Independent Oversight

As 2020 illustrated, companies often make quick decisions in response to public pressure based on unclear, inconsistently enforced policies, leaving them open to criticism and resulting in backtracking. Credibly independent oversight bodies, modeled after the one Facebook has created, but with some important differences, could ensure that platform executives are not solely responsible for important content moderation decisions. Oversight bodies could insulate important content moderation decisions from business interests; improve transparency around those decisions, thereby building public confidence; and ensure executives do not bear sole responsibility for politically contentious fallout. In short, it could serve the public interest as well as the companies'.

Oversight bodies should be tailored to specific platforms. They should be made up of diverse civil society leaders with expertise on democracy and the information space. Most importantly, these bodies should be credibly independent of the companies, insulated from business interests, and empowered with broad jurisdiction to take up cases and be responsive to users who identify issues and appeal platform decisions, rather than to the platforms themselves. While Facebook has launched a version of such a body, its Oversight Board lacks the independent authority and jurisdiction to make it responsive to users, instead relying on the company to refer cases for review outside of its narrow scope of work.[137] Oversight bodies should be clear and transparent in their decision-making processes, favoring candor, context, and detail in justifying decisions. And platforms should commit to adhering to and enforcing the precedence of decisions going forward. The ultimate guiding principle of the bodies should be to promote healthy online discussion and protect the interests of users and the public.

While oversight bodies will never be able to make decisions at the speed that is required from platforms during an election, they can help increase transparency and consistency around platform policies and can bring an independent, user-focused perspective to decision-making. In the long-term, oversight bodies can help establish moderation policies to guide platforms through difficult challenges during election seasons.

Congress Should Consider Establishing an Independent Federal Regulator for Social Media Platforms

Countering the spread of mis- and disinformation across platforms will require government to incentivize companies to address elements of platform architecture driving trends that are detrimental to the public interest. Accomplishing this task will demand independent, dedicated, and professional oversight that is likely beyond the means of Congress.

Congress could establish an independent federal regulator to conduct oversight of digital platforms in the public interest, as researchers at the German Marshall Fund and Harvard University's Shorenstein Center have recommended.[138] The mandate of this agency should focus on protecting consumers and promoting a healthy information space. The agency could:

- Provide oversight for platform architecture, conducting audits of algorithms—focusing on those with the largest potential impact—to make sure that they provide some degree of transparency and prioritize the public good.
- Confirm that companies are taking sufficient action to mitigate negative externalities, such as the spread of misinformation, hate speech, and harmful conspiracy theories.[139]
- Address other issues where polarization has prevented Congress from taking action, such as on online advertisements.[140]

Recognizing a wide degree of variation among platforms, the regulator could embark on a joint public-private effort with companies to establish enforceable codes of conduct for specific digital practices.[141] To give teeth to enforcement, Congress could consider amending Section 230 of the Communications Decency Act to require companies to adhere to codes of conduct in order to retain safe harbor from liability for content published on their platforms.[142]

Recommendation 2: Sustain and Build on Civil Society Efforts in the Information Space

To make civil society initiatives sustainable without compromising their independent credibility, civil society organizations should consider establishing a permanent coordinating center to bring together researchers, platform representatives, and government liaisons to share information and insights. Such a center, which could base its structure on initiatives like the Election Integrity Partnership, could take an active role in identifying, tracking, and flagging harmful mis- and disinformation narratives for platform action and serve as a clearinghouse for cross-sector information-sharing. It could work closely with the EI-ISAC to provide support to election officials in identifying and dealing with false narratives. Importantly, though the Center should facilitate information exchange with and between government and platform companies, to retain its independence it should not take funding from either source. Foundations focused on democracy, the information space, and elections should support this work. To ensure that the center is permanent and maximally apolitical, its scope of work should be broader than elections and cover broader trends in the information space.

Recommendation 3: Build on Improvements in Cyber and Election Security Coordination

Coordination and cooperation among federal, state, and local officials working to improve election security increased substantially during this election cycle. But vulnerabilities persist. The U.S. government should provide additional support to authorities responsible for election security, while incentivizing stronger cybersecurity standards for actors across the election supply chain. Federal, state, and local authorities can also do more to protect election workers, who play an essential role in protecting and administering the voting process.

Congress Should Provide Additional Support to Authorities Responsible for Election Security

Congress should work to provide sufficient funding—including in non-election years—to help states and local jurisdictions update election systems and improve their security. Ahead of the 2020 election, Congress failed to fulfill this duty, forcing many election officials to turn to civil society actors for philanthropic support.[143] The security of U.S. elections should not depend on private actors to fill gaps where Congress fails to act. Congress should take bipartisan action to ensure that appropriate funding is allocated to states consistently, including in non-federal election years, rather than on an ad-hoc basis.[144] In addition, Congress should:

- Ensure that CISA is resourced to deliver comprehensive support to every state and local jurisdiction, election official, or campaigns that requires it.
- Resource the EI-ISAC—via CISA—and the EAC to expand outreach and support for capacity-building to state and local officials in the critical periods between elections.
- Consider clarifying responsibilities and authorities for federal agencies supporting election security by consolidating all election infrastructure-related responsibilities within CISA's Election Security Initiative (ESI) and solidifying the EAC as the national hub for information and resources on election administration, as the Defending Digital Democracy Project has recommended.[145]

Congress Should Strengthen Security Standards and Incentivize Local Jurisdictions to Innovate

Given the importance of transparency and auditability for retaining trust in the democratic process, Congress should use future election funding opportunities to solidify voting technology standards that will improve the security of future elections and promote confidence. Congress should:

- Fund state and local officials to replace paperless voting machines with machines that produce paper records and should prohibit the use of funds for non-paper-based voting systems.[146]
- Support the implementation of risk-limiting audits, which are invaluable for mitigating potential interference and building public confidence.[147]
- Resource the EAC to expand its Voluntary Voting System Guidelines, which provide security standards recommendations for voting equipment, to include election technologies other than voting systems, such as electronic pollbooks, voter registration databases, and election night reporting systems.
- Equip CISA to investigate threats to the election security supply chain.
- Establish "federal innovation block grants" to help incentivize state and local governments to implement new election administration technologies.[148]
- Consider ways to encourage states to centralize election security efforts to lower procurement costs for jurisdictions and help monitor the implementation of security standards.[149]

Federal and State Lawmakers Should Invest in the Protection, Recruitment, and Training of Election Workers

Ahead of future elections, federal and state lawmakers should conduct hearings on election worker safety and provide additional funding to state and local election officials to ensure that they can administer elections safely and at no cost to themselves. Federal and state lawmakers should also examine the current laws that exist to protect their election officials and consider adopting stronger ones that could deter threats like those that were widely reported during the 2020 election cycle.[150]

Lawmakers should also invest in developing and retaining talent in election administration by expanding training opportunities for election officials, including in how to counter misinformation.[151] Training for cybersecurity should be offered on an ongoing basis to make sure that officials retain skills and maintain awareness of evolving threats.[152] As recommended by the Defending Digital Democracy Project, the federal government could partner with accredited institutions to standardize and expand election and cybersecurity certification programs and consider establishing a fellowship program to bring talented young professionals into election administration.[153]

Finally, lawmakers should fund state and local election officials to develop comprehensive communications plans ahead of future elections, as recommended by the Election Integrity Partnership.[154] These plans should include outreach to citizens to help voters understand the voting, counting, reporting, and security processes. They should also include secure, well-structured websites where voters can go for all election information, including information to dispel common false narrative about the voting process.

Recommendation 4: Develop A Safety Net Against Politicization of Election Security

The U.S. government should reassert the traditional distance that separates national security and government officials from politics, which was degraded during the Trump administration. To that end, Congress should explore ways to strengthen independent reporting requirements on foreign interference and the administration should institutionalize non-partisan public reporting on threats to elections and follow long-standing norms that separate the White House from political campaigns. Both Congress and the White House should work to reconstruct civic infrastructure and generate a renewed investment in democratic institutions and values.

Congress Should Explore Methods to Depoliticize Reporting on Foreign Interference

Ahead of the 2020 election, reporting from government officials on foreign interference helped keep the public and media up to date about emerging threats, operations, and narratives. However, these communication efforts were hampered by politicization—often from political appointees—raising concerns about the separation of national security and President Trump's campaign interests. To rebuild trust in public communication and better depoliticize reporting on foreign interference, Congress should investigate methods to empower non-partisan reporting. One model it could draw on is Canada's Security and Intelligence Threats to Elections Task Force (SITE). SITE is an interagency body that monitors foreign efforts to interfere in Canadian elections. Through a special protocol, during an election cycle, senior civil servants on the task force can decide whether to disclose foreign interference operations to the public.[155] By taking such decisions out of the hands of political appointees, this approach helps insulate reporting from political concerns. A U.S. government version of SITE could build on existing interagency monitoring bodies such as the Malign Foreign Influence Response Center within the Office of the Director of National Intelligence.[156]

Congress Should Reinforce CISA's Independence

CISA earned bipartisan praise for its actions to secure the 2020 election, but President Trump fired its Director, Christopher Krebs, before the end of the election cycle after he contradicted the President's false claims.[157] To help insulate CISA from potential future political pressure, Congress should restructure the CISA Director position to provide for one, 10-year term, similar to the FBI Director.[158] Congress should also require that other high-ranking positions within CISA, including the Deputy Director, Executive Assistant Director, and Assistant Director positions are held by career officials rather than political appointees. Finally, Congress should ensure that CISA's "Rumor vs. Reality" webpage, which refuted false claims about the election process and results, remains a permanent fixture. To better insulate the site from partisan attacks, responsibility for controlling the site could be shifted to the EI-ISAC.

Americans Must Renew Their Democratic Culture

The success of the 2020 election was the result of energetic and dedicated action by American citizens across civil society, the private sector, and government. As Norm Eisen described, the story of the election was "the thousands of people of both parties who accomplished the triumph of American democracy at its very foundation." At the same time, domestic attacks on the election served as a reminder of the fragility of democratic institutions. None of the recommendations outlined in this paper will be possible or fully successful without a reconstitution of belief in U.S. democracy. To this end, the United States must reinvest in democratic values, institutions, and processes. While a full accounting of how to do that is beyond the scope of this paper, one thing is clear: an important first step will be to reconstruct civic infrastructure and community programs to bring citizens back together outside of the online environment.[159] The U.S. government should also embrace civic education and service learning and should launch a public campaign to rebuild faith and investment in democracy and democratic values.[160] Rebuilding the American community will be a long, slow process, but without it, the fragility of U.S. democracy will be tested again soon.

Conclusion

The 2020 election was the most secure in U.S. history. That was the assessment of the Election Infrastructure Government Coordinating Council, a broad committee of government, private sector, and civil society stakeholders who oversaw the elections.[161] The election faced threats both foreign and domestic, from covert Russian attempts to funnel weaponized information into U.S. news feeds, to Iranian hacking ventures and efforts from President Trump and his allies to undermine public confidence in the security of the vote. Democracy prevailed because of the energy and dedication of leaders from all corners of American society.

To build on this success, close outstanding vulnerabilities, and get ahead of emerging challenges, policymakers, platform companies, and citizens will need to harness their energy once more to address platform architecture, strengthen civil society efforts in the information space, expand on progress in cyber and election infrastructure coordination, and construct a safety net that can protect against the politicization of election security. That is how they can rebuild confidence in U.S. democracy.

Appendix A: Actions to Secure the 2020 Election

This appendix includes a compendium of documentable actions taken by government, private sector, and civil society actors to secure the 2020 election against foreign interference. While we aimed to capture a comprehensive breakdown of such actions, this list is not exhaustive. Some information about countering foreign interference is not and may never be in the public domain. In other cases, for example at the state and local levels, actions were taken by such a broad range of actors that collecting each instance would be impossible. In many cases, we relied by necessity on self-reported information. We have not evaluated the effectiveness of each measure.

Public Sector

Executive Branch

Public Announcements and Communication

Information Sharing, Threat Assessments, and Warnings

In the days and months leading up to the election, agencies involved in election security released numerous statements clarifying their priorities, delivering threat assessments, and sharing the steps taken to secure the 2020 election.[162] Among them:

- On March 2, 2020, the **State Department, Department of Justice (DOJ), Defense Department (DOD), Department of Homeland Security (DHS), Office of the Director of National Intelligence (ODNI), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA)** released a joint press release detailing the federal government's efforts in coordination with state, local and private sector partners, to protect against threats to Super Tuesday.
    - The statement warned Americans to "remain aware that foreign actors continue to try to influence public sentiment and shape voter perceptions." The statement also promoted state and local election officials as the most trusted source for election material.[163]
- On July 24, 2020, marking 100 days before the 2020 general election, **National Counterintelligence and Security Center (NCSC) Director William Evanina** detailed the state of foreign threats facing the election, as well as measures **ODNI** had taken to address them, including the provision of robust intelligence-based briefings on election security to the presidential campaigns, political committees, and Congressional audiences.
    - Evanina detailed how foreign actors, particularly from Russia, China, and Iran, were seeking to undermine the election process.
    - Evanina also cautioned that the American public should remain vigilant against foreign interference by consuming information "with a critical eye" and reporting suspicious election-related activity to authorities.[164]
    - Evanina also pledged that the Intelligence Community (IC) would strive to update the American public on the evolving election threat landscape.
- On August 7, 2020, **NCSC Director William Evanina** said that "foreign states will continue to use covert and overt influence measures in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic process."
    - Evanina said that the IC was primarily concerned with the ongoing and potential activity from China, Russia, and Iran and issued differential threat assessments for these three foreign actors, saying China prefers that "President Trump...does not win reelection"; Russia is taking measures to "denigrate" Joe Biden; and Iran is "seeking to undermine U.S. democratic institutions, President Trump, and to divide the country."[165]

- On August 20, 2020, the members of the **Election Infrastructure Government Coordinating Council (GCC) Executive Committee,** which includes **CISA,** the **Election Assistance Commission (EAC), National Association of Secretaries of State (NASS), National Association of State Election Directors (NASED), and some state election officials,** released a statement saying that the U.S. election community is "more unified, more coordinated, and better prepared than ever before."[166]
    - The statement also shared recent actions to protect election infrastructure, including that all public and private sector cybersecurity professionals have conducted hundreds of assessments on state and local networks; a nationwide "Tabletop the Vote" exercise reached 37 states and 2,100 participants; and that every state and more than 2,700 local jurisdictions are now members of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).
- On August 20, 2020, **NCSC Director William Evanina** said that, in addition to Russia, China, and Iran, other countries including Cuba, Saudi Arabia, and North Korea were also seeking to sow discord in the U.S.[167]
- On October 20, 2020, **CISA Director Christopher Krebs** shared CISA's ongoing efforts in coordination with public and private sector partners to protect the 2020 elections from foreign interference.
    - Krebs emphasized that, although they remained "confident" that no foreign actor could change votes, actors might try to introduce chaos in our elections and sensationally overstate their capabilities of interference.[168]
- On October 21, 2020 **FBI Director Christopher Wray** assured the public that the FBI had been leveraging partnerships to investigate malicious cyber activity against election infrastructure, malign foreign influence operations, and election-related crimes, such as voter fraud and voter suppression or intimidation.
    - Wray said, "We're not going to tolerate foreign interference in our elections or any criminal activity that threatens the sanctity of your vote or undermines public confidence in the outcome of the election."[169]
- On October 22, 2020, the **DHS Office of Inspector General** published an audit of CISA's actions to increase election security. The investigation found shortcomings in CISA's plans to mitigate threats to election infrastructure, including preparations for physical security, terrorism, and targeted violence.
    - It also identified problems in limited staffing, inadequate classification authority, and duplicative data sharing. The audit attributes the shortcomings to DHS senior leadership turnover and ongoing CISA reorganization.
    - In a response to the report, CISA Director Chris Krebs said that while the agency concurred with the recommendations, the audit was published less than one month before the 2020 election. Krebs urged DHS to account for the entirety of an election cycle in future audits.[170]
- On November 4, 2020, **CISA Director Christopher Krebs** issued a statement declaring that there was "no evidence any foreign adversary was capable of preventing Americans from voting or changing vote tallies."
    - Krebs also said that CISA would "remain vigilant" against foreign actors' attempts to disrupt vote counting and election certification by continuing to monitor malign cyber activity after Election Day.[171]
- On November 12, 2020, the **Election Infrastructure GCC Executive Committee** released a statement saying that the "the November 3rd election was the most secure in American history." The committee also emphasized election officials as trusted voices of information.[172]
- On January 8, the **ODNI** ombudsman, Barry A. Zulauf, released a report detailing a conflict between President Trump's political appointees and career intelligence analysts over politicization of Russian and Chinese interference in the 2020 election.[173]

The **FBI** and **CISA** issued regular public statements on their websites and in press conferences that aimed to warn the public about election-related threats, including:

- False election-related Internet domains used by malign actors to spread malware and disinformation to voters.[174]

- Online journals backed by foreign intelligence services and malign foreign actors to spread election-related disinformation.[175]
- Distributed denial-of-service attacks on election infrastructure that could have hindered access to voting.[176]
- Claims of hacked voter registration databases intended to decrease voter confidence or dissuade registration.[177]
- Attempts by cyber actors to compromise election infrastructure that could have slowed the voting process but not prevent voting.[178]

On September 24, 2020, the **FBI** also issued a press release detailing election crimes and methods of voter suppression, and how the public could report violations online.[179] The guide directed readers to authoritative sources of election-related information and detailed recommendations for readers to secure their votes.

Public Awareness and Confidence-Building

CISA delivered materials sharing factual information about the 2020 election to the public:

- CISA's "Rumor vs. Reality" website aimed to debunk common misinformation and disinformation narratives related to the security of election infrastructure and other related processes. CISA addressed these rumors by continuously sharing and citing factual information. For example, the website responded to the "rumor" that "a bad actor could change election results without detection" by sharing the "reality:" "Robust safeguards including canvassing and auditing procedures help ensure the accuracy of official election results" alongside more detailed information and a list of useful sources.[180]
- The "Resilience Series" graphic novels sought to communicate the dangers and risk of dis- and misinformation through fictional stories inspired by real-world events. For example, "Real Fake" shared how threat actors "capitalize on political and social issues" to plant doubt and steer the minds of targeted audiences.[181]
- Through "Election Infographic Products," CISA sought to equip election officials, stakeholders, and voters with information on the mail-in voting, post-election, and election results processes as well as 2020 election security measures.[182]
- A collection of "Foreign Interference" guides shared individualized counter-disinformation measures, such as "Understanding Foreign Interference in 5 Steps."[183]
- The "Election Disinformation Toolkit" aimed to teach election officials how to emphasize their role as the trusted source of election information. The toolkit also highlighted foreign government-backed disinformation campaigns.[184]

The **FBI** launched the "Protected Voices Initiative," which provided tools and resources to political campaigns and American voters with the aim of protecting them against online foreign influence operations and cybersecurity threats.

- "Protected Voices" resources included videos on critical cybersecurity and foreign influence topics from the FBI, DHS, and the Director of National Intelligence.[185]
- Between September 14 and November 3, the FBI also initiated public awareness messaging about election security across its social media platforms.[186]

The **FBI and NCSC** worked to increase awareness of foreign intelligence threats on professional networking sites and other social media platforms and help the private sector, academic community, and other government agencies guard against this threat.

- They released a movie called the "The Nevernight Connection," detailing a fictional account of how a foreign intelligence service targeted a former IC official via a fake profile on a professional networking site.[187]

The **Election Infrastructure GCC** released public statements sharing and supporting the "#Protect2020" and "Trusted Info" initiatives, which aimed to bolster confidence among voters in government election security efforts.[188]

Coordination, Training, and Intelligence-Sharing

Coordination with and Support for Local and State Officials

CISA aimed to strengthen partnerships with state and local election officials through the "#Protect2020" campaign, which established a national framework to enhance election security. The strategic plan, released in February 2020, centered on direct engagement with state and local officials responsible for operations in over 8,000 election jurisdictions to identify cyber vulnerabilities and plan responses to potential attacks.

Over the year leading up to the election, CISA offered free election security-related products and services to state and local election authorities, including:[189]

- Cybersecurity Advisers, who aimed to help private sector and local entities recognize and prepare for cyber threats.
- Cybersecurity Assessments, which evaluated an entity's cyber resilience, cybersecurity practices, and capability to meet threats.
- The National Cyber Awareness System, which provided subscription-based information products to stakeholders to improve situational awareness among a broad audience.
- The Enhanced Cybersecurity Services program aimed to help protect IT networks through intrusion detection and analysis services (offered at low or no cost to state and local organizations eligible for FEMA Homeland Security Grant Program funds).

CISA also offered scalable, customizable tools that sought to improve local stakeholders' communication efforts and election security planning capabilities through its "The Last Mile" and "Planning Guide" products. Tools included templates, posters, and infographics that were openly accessible on the Internet ahead of the election. The campaign included the following:

- "Physical Security of Voting Locations and Election Facilities," a general guide for election officials to improve the physical security of election facilities through four actionable steps: connect, plan, train, and report. The guide detailed steps and expectations for poll workers, election officials, and election facility operators.[190]
- "Election Infrastructure Cyber Risk Assessment and Infographic," a set of voluntary resources to help stakeholders manage risks associated with critical election systems. The assessment included details regarding key points of election preparation, including ballot and poll book preparation, voting system programming, and tabulation. It provided tables that summarize the potential targets for cyberattacks and the levels of associated threat.[191]
- "Election Risk Profile Tool," a user-friendly risk assessment tool created through a partnership with the **EAC**. The assessment aims to help local and state officials prioritize risks to specific jurisdictions and identify mitigation options. The tool helped create a "Risk Profile" report that outlines the highest priority risks.[192]
- "Mail-in Voting in 2020 Infrastructure Risk Assessment and Infographic," a set of voluntary resources aiming to inform stakeholders on mitigating risks associated with mail-in voting. The resource explicitly outlined how election officials and related facilities can anticipate, control, and respond to common risks.[193]
- "Cyber Incident Detection and Notification Planning Guide for Election Security," voluntary resources for election offices to help develop a cyber response plan.[194]
- "Guide to Vulnerability Reporting for America's Election Administrators," a step-by-step guide for administrators to help establish a vulnerability disclosure program.[195]

CISA deployed a "situational awareness room" starting November 2, 2020 with the goal of creating open lines of communication with election officials nationwide. State and local election officials could report cyber, man-made, or natural disaster threats to federal officials.[196]

CISA conducted a limited pilot of Crossfeed, an open-source tool that continued operating after Election Day to detect vulnerabilities in public-facing state election infrastructure by directly interfacing with software and using web-scraping.[197]

CISA partnered with the **EAC** in response to the coronavirus pandemic to prepare states for the sudden shift to voting by mail and safe in-person voting practices.[198]

The **EAC** also offered free training for state and local officials in the following areas:

- Video and written materials, separated into three modules, Cybersecurity 101, 201, and 301, that shared foundational knowledge on cybersecurity terminology, best practices in election offices, practical application, and communication.[199]
- A Cybersecurity Risk Management webinar for election officials to raise awareness of election security-related threats.[200]
- Cybersecurity Crisis Management modules including pre-election preparedness, an Election Day "War Room," and a post-election debrief to inform election officials of methods to respond against cybersecurity crises.
- State voter file accessibility information, which aimed to dispel "false positives" of data breaches on the dark web.[201]

The **EAC** distributed $400 million in election security grants to states for the purpose of protecting the 2020 election cycle from the effects of the coronavirus pandemic, particularly to expand vote-by-mail infrastructure.[202]

- **Congress** passed this supplemental appropriation funding and **President Trump** signed it into law in late March 2020 as part of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act).
- The CARES Act also included a $10 billion line of credit from the **Treasury Department** to ensure the financial solvency of the U.S. Postal Service and guarantee continued operations, effectively ensuring the continuation of basic vote-by-mail infrastructure.[203]

Coordination Among Federal Actors

U.S. Cyber Command (CYBERCOM) and **NSA** occupied a "mission center" that connected all federal agencies involved in election security. The agencies sought to develop open streams of communication and provide real time information in case an election security incident occurred on election day.[204]

CYBERCOM and the **National Guard** formed a partnership with the aim of opening lines of communication between state and local governments and the military's top cyber force to address 2020 election security.[205]

- As part of this partnership effort, the agencies established "Cyber-9-line," a template of questions used by participating National Guard units to quickly communicate a cyber incident to CYBERCOM, who could use the data to diagnose a foreign attack and then provide timely, unclassified feedback back to the state and county governments through the National Guard to address the cyber incident.[206]

The **ODNI's Cyber Threat Intelligence Integration Center** created a new lexicon of cyber terms in an effort to better synchronize communications between the IC, election officials, and the public on cyber threats.[207]

CISA, **EAC**, **FBI**, and **National Institute of Standards and Technology** coordinated to send guidance to states about the major security challenges posed by voting systems that use the internet.[208]

The **EAC**, in coordination with the **Election Infrastructure GCC** and the **Election Infrastructure Sector Coordinating Council (SCC),** published a series of documents following the 2020 presidential primaries, sharing lessons learned and best practices that state and local level election officials identified during the coronavirus pandemic.[209]

Other Coordination Efforts

CISA, **FBI**, **DOJ**, and **ODNI** offered support and election security-related information to all campaigns registered with the **Federal Election Commission** (**FEC**).[210]

ODNI, in coordination with **DHS** and **FBI**, announced that the IC would lead all intelligence-based threat briefings to candidates, campaigns, and political organizations under the U.S. Government's notification framework.[211] Previously, the FBI and DHS had been tasked with intelligence briefings for candidates and political parties.[212] The change sought to simplify the threat notification process, according to the announcement.

CISA's Countering Foreign Influence Task Force (CFITF) worked directly with public, private, and government stakeholders to raise public awareness of the scale and scope of foreign influence campaigns. Leading up to the election, the CFITF acted as a "switchboard" for directing threat reports to relevant private and public stakeholders.[213]

CISA also reported that it coordinated with:[214]

- Election technology vendors
- National political party committees
- Non-governmental organizations (NGOs)
- Think tanks and academia
- Media and social media companies
- Private cybersecurity firms
- Coordinating bodies, such as the Election Infrastructure GCC and the Election Infrastructure SCC

The **EAC** partnered with cybersecurity-focused nonprofit **Center for Internet Security (CIS)** beginning in June 2020 to launch a program to improve election technology verification.[215] Their proposal for the "Rapid Architecture-Based Election Technology Verification" pilot program focused on improving the cybersecurity in non-voting technology, including electronic poll books, election night reporting websites, and electronic ballot delivery systems.

Investigations, Sanctions, and Proactive Defense

The **FBI** worked to investigate and respond to incidents in which foreign adversaries deployed cyber operations seeking to undermine the security of and public confidence in the 2020 election:

- The FBI investigated reports of apparent voter suppression robocalls across the nation. With estimates of 10 million calls sharing false information about voting, the FBI urged the American public to "verify any election and voting information they may receive through their local election officials."[216]
- The **FBI** and **CISA** revealed in October 2020 that Russian cyberattacks, attributed to Energetic Bear or FireFly, targeted U.S. government networks, including those involved with the election.[217]
- The **FBI** and **ODNI** attributed the October 2020 "spoofed" email campaign to Iran within 27 hours of the incident, including additional video content suggesting that individuals could cast fraudulent ballots.[218] DNI Ratcliffe and FBI Director Wray also confirmed that Russia and Iran had separately obtained some voter registration information. In response to these threats, Wray and Ratcliffe emphasized that the IC caught the activity "immediately" and "acted swiftly."[219]
- The FBI investigated and determined that Iranian cyber actors were "almost certainly" responsible for creating a website, called "Enemies of the People," which contained death threats aimed at U.S. election officials in mid-December 2020.[220]
  - This was the fastest public disclosure of attribution for a foreign interference operation by U.S. officials to date.[221]

On November 9, **Attorney General William Barr** wrote a memorandum authorizing federal prosecutors to investigate allegations of voting irregularities prior to 2020 election certification in December.[222] Barr subsequently closed the case and said no widespread irregularities were found.[223]

In September 2020, the **Treasury Department** sanctioned Andrii Derkach, a Ukrainian politician with close ties to Rudy Giuliani, and three members of the Internet Research Agency after the IC indicated that Derkach acted as part of a Russian-backed operation to smear President-elect Joe Biden and the Democratic Party.[224] On January 11, the Treasury Department placed additional sanctions on Derkach's inner circle. Targets of these sanctions include seven individuals and four entities connected with Derkach.

The **State Department's** Diplomatic Security Service launched the "Rewards for Justice" program in August 2020 with the goal of gaining information on foreign interference in U.S. elections. The program offered a reward of up to $10 million in return for information identifying or locating any person who was working with or for a foreign government actor to interfere with any U.S. election.[225]

CYBERCOM took offensive steps aimed at protecting the 2020 election from foreign cyber operations.

- **CYBERCOM** reportedly deployed "Hunt Forward" teams to operate on European networks to identify and observe Russian Advanced Persistent Threat (APT) actors. These operations aimed to gain further information about the APT actors' tools and to obtain malware samples that could be shared with state and local elections officials and their vendors to better protect election systems.[226]
- **CYBERCOM**, and separately **Microsoft**, carried out an operation that sought to hinder the ability of Trickbot, an infamous ransomware distributor, to attack U.S. targets.[227]
- Following an Iranian operation that delivered threatening emails to American voters while posing as a far-right group, **NSA** and **CYBERCOM leader General Paul Nakasone** shared that he was "not surprised" by Iran's actions, and that NSA-CYBERCOM "provided early warning and followed [them very closely]."[228]
- In testimony to Congress after the election, **General Nakasone** reported that **CYBERCOM** had carried out more than two dozen operations to get ahead of foreign threats to the 2020 election.[229]

Congress

Legislation

As part of the CARES Act of 2020, **Congress** passed $400 million in additional Help America Vote Act (HAVA) funds to support states in administering the 2020 elections. While the EAC gave broad authority for states to employ the funds, the language also required a 20 percent match from states to receive funding.[230]

Congress passed the National Defense Authorization Act for Fiscal Year 2021 in December 2020. Although the sprawling defense authorization bill included relevant provisions to confront foreign interference, these measures did not come into effect within the timeline of this audit.[231]

Hearings

Congressional committees held more than ten hearings on election security and related matters with testimony from speakers including civil society actors, major tech companies, and states' chief election officials. The hearings covered topics including:

- Oversight of social media companies (see below for more information).
- Potential foreign disinformation threats to elections.[232]
- Adapting election systems to expanded vote-by-mail.[233]
- Ensuring election security and integrity during the pandemic.[234]

Congressional committees also held several hearings that questioned representatives from major technology companies, including Facebook, Google, and Twitter, about online threats. The companies faced questions regarding:[235]

- Their actions since 2016 to identify and root out foreign influence operations online and protect against election interference.

- The current state of data sharing among private-sector actors.
- Collaboration between the tech sector and U.S. government authorities to address the threat of covert foreign influence and election interference activities.
- How disinformation advances strategic narratives.
- Recently identified foreign-linked misinformation efforts.

Reports, Statements, and Letters

The Senate Select Intelligence Committee published volumes three, four, and five of its bipartisan investigation into Russian interference in the 2016 election on February 6, April 21, and August 18, 2020, respectively.[236] The reports exposed Russian tactics and efforts to target U.S. election infrastructure, citizens, and officials to undermine the election process. The investigation expanded upon the work of Special Counsel Robert Mueller. It also revealed previously unknown details on Russian attempts to solicit engagement with the Trump administration, including declaring Konstantin Kilimnik, a longtime partner of Trump campaign chairman Paul Manafort, as a Russian agent and providing evidence that Kilimnik may have been directly involved in the Russian intelligence operation to hack into Democratic Party computer networks.[237]

House and Senate Democratic leadership sent letters and issued statements to U.S. Intelligence officials, including:

- On July 24, **House Speaker Nancy Pelosi (D-CA), Senate Minority Leader Chuck Schumer (D-NY), House Intelligence Committee Chairman Adam Schiff (D-CA), and Senate Intelligence Committee Vice Chairman Mark Warner (D-VA)** signed a joint request asking the FBI for an all-lawmaker briefing about foreign election interference efforts that may have been targeting Congress.[238]
- On July 24, **Speaker Pelosi, Minority Leader Schumer, Chairman Schiff, and Vice Chairman Warner** issued a joint statement in response to an ODNI update regarding election security and foreign threats 100 days before the election saying, "Director William Evanina does not go nearly far enough in arming the American people with the knowledge they need about how foreign powers are seeking to influence our political process."[239]
- On September 1, **Speaker Pelosi, Chairman Schiff, and Chairman Pete Visclosky (D-IN)** sent a letter to Director of National Intelligence John Ratcliffe calling on the IC to uphold its responsibility to keep the American people and their elected representatives informed of foreign threats to the 2020 election through reinstating election-related intelligence briefings to Congress.[240] The letter came after ODNI announced it would be cancelling scheduled election-related briefings.
- On September 11, **Chairman Schiff** sent a letter to Joseph B. Maher, the senior official performing the duties of the under secretary for intelligence and analysis, advising DHS that the committee had expanded its investigation into intelligence activities, including politicization of intelligence (as it relates to foreign influence, interference, and threats regarding the 2020 U.S. elections).[241]

Members of Congress also shared joint statements expressing concern regarding disinformation:[242]

- In August 2020, **Senators Marco Rubio (R-FL) and Mark Warner** released a joint statement in response to NCSC Director Bill Evanina's August 7 statement on election security. Their statement emphasized that Evanina's remarks highlighted the serious and ongoing threats to the U.S. election from China, Russia, and Iran. The senators also thanked Evanina and other members of the IC for delivering additional briefings to most congressional members and urged them to continue to keep them informed.[243]
- In October 2020, **Senators Rubio and Warner** released a joint statement ahead of the 2020 election warning that foreign actors may seek to use disinformation to undermine confidence in the electoral process. The statement urged citizens to be wary of misinformation and emphasized that national and local officials continued working together closely to secure the election.[244]
- In December 2020, a group of **Senate Democrats**, including Senators **Amy Klobuchar (D-MN)** and **Warner**, sent a letter to Google urging the company to enforce its ad policies and to restrict ads spreading

disinformation about the 2020 election. The senators also called on the company to halt ad services for sites pushing election disinformation.[245]

State and Local Officials

This section does not capture all actions taken by the more than 10,000 state and local jurisdictions that comprise the United States.[246] It captures a representative sample of the types of public-facing messaging that election officials engaged in before, during, and after the election. Other relevant information on state and local election officials is available in Appendix A.[247]

Public Messaging

Pre-Election Messaging

Leading up to election day, **state and local election officials** routinely pushed back on disinformation narratives—including false claims of fraud—surrounding the conduct of the 2020 election.

- Officials including Colorado Secretary of State Jena Griswold pushed back on President Trump's claims that mail-in voting or ballot drop boxes would lead to voter fraud, assuring voters that these systems are secure, effective, and that there is no evidence they could be manipulated.[248]
- The Michigan Department of State quickly refuted claims that foreign actors had hacked voter rolls after U.S. journalists and outlets errantly promoted a poorly sourced Moscow Times story claiming that such information was available for sale on the Russian dark web.[249]
- In the week before the election, Florida, Alaska, and Arizona officials responded to an Iranian voter intimidation campaign that targeted voters in their respective states by announcing that there had been no breaches to voter rolls and reminding the public that some voter registration information was considered public information to varying degrees.[250]

Election Day Messaging

On the day of the election, **local and state election officials** sought to quickly refute claims by sharing trusted information online.

- In Kansas, New York, Nevada, and Michigan, state officials quickly refuted and launched investigations into robocalls encouraging voters to stay home on election day.[251]
- In Philadelphia, officials provided rapid response to online claims of election violations, quickly refuting false claims.[252]
- Officials in Erie County, Pennsylvania refuted a video claiming to show an Erie official discarding hundreds of ballots for Trump, noting that the individual involved was in no way related to Erie's election administration and was not even a registered voter or resident in the county.[253]

Post-Election Day Messaging

In the aftermath of the election—and in the wake of false claims of fraud from the Trump Administration—**local and state election officials** across the country pushed back on false claims.

- Officials in every state communicated that there was no evidence of systemic voter fraud.[254]
- In Georgia, the lieutenant governor responded to false claims of voter fraud by emphasizing that the state has not seen a single credible incident during the presidential election.[255]
- Another top official in Georgia described claims of fraud as "hoaxes and nonsense," encouraging citizens to look to trusted sources instead.[256]
- In Arizona, multiple bipartisan officials, including the state's attorney general, quickly and flatly rejected claims of voter fraud and allegations that officials threw out ballots marked in sharpie—a conspiracy theory that members of the Trump campaign spread.[257]

- In Nevada, election officials continued to field questions from reporters and voters in the days following the election and responded by emphasizing confidence in the election results.[258]

Private Sector

Cybersecurity and Technology Companies

Assistance and Training

Cybersecurity firm **Cloudflare** provided free support to state and local election officials through its Athenian Project, reportedly delivering protection to 229 state and local governments across 28 states.[259]

- The "Interactive Guide to Protecting Your Election Website" was openly accessible and aimed to inform users on steps to take to protect voter data, stay online during peak Internet traffic, and prevent brute force login attacks throughout the election cycle. It also provided instructions on enrolling in Cloudflare's free services.[260]
- Through its Cloudflare for Campaigns program, the company offered free cybersecurity services with the aim of bolstering political campaigns' data security, blocking hacking and malicious attack attempts, and ensuring website performance during high-traffic periods.[261] In partnership with the non-profit project **Defending Digital Campaigns (DDC)**, the firm supplied free cyber protections to 50 political campaigns across the political spectrum.[262]
- In June and September 2020, the firm reported a record number of cyberattacks targeting the Trump campaign. Following these reports, the company shared that they provided services to the Trump and Biden campaigns to prevent more sophisticated and consequential attacks.[263] The company and campaigns declined to comment on the nature of the services or specific threats.
- Cloudflare also created a public dashboard on its blog to highlight the nature of emerging cyberattacks.[264]

In the months before the 2020 election, endpoint threat detection and response vendor **Cybereason** held election security tabletop exercises through "Operation Blackout: Protect the Vote."[265] The simulation guided teams of cybersecurity professionals and government officials to pre-empt and respond to threats from a team of experienced hackers. For example, the company's August exercise focused on the readiness of local governments to respond to disinformation.

Google collaborated with civil society groups, cybersecurity firms, government agencies, and academia to train campaign staff and election officials.[266]

- Google partnered with **DDC** to give federal campaigns access to free security keys, the strongest form of two-factor authentication.[267] The company also distributed more than 10,500 Advanced Protection kits to help campaigns defend against targeted online attacks.[268] The effort emphasized the necessity of cybersecurity training not only for core campaign staff, but also for vendors, consultants, and support staff.
- Google provided trainings for nearly 4,000 campaign and election officials in every state to prevent digital attacks, phishing campaigns, and hacking attempts through a partnership with the **University of Southern California's Annenberg School**.[269]

Microsoft offered free and low-cost tools for campaigns and election officials.

- Services included AccountGuard for threat monitoring, Microsoft 365 for campaigns, and Election Security Advisors meant to train election officials and campaign staff in cybersecurity preparedness and remediation.[270]
- In partnership with **DDC**, Microsoft announced in June 2020 that AccountGuard would incorporate Microsoft's enterprise-grade identity and access management protections at no additional cost.[271] Authorized by the Federal Elections Commission, this service aimed to provide greater security against hack and leak operations.

- In June 2020, Microsoft announced that its cloud computing provider Microsoft Azure was compatible with Albert Network Monitoring, the service that CISA and the EI-ISAC used to monitor internet traffic and connection attempts on networks owned and run by election officials.[272]

Threat Detection and Response

Microsoft worked with partners across sectors to share information on detected cyberthreats and made some of these reports public.

- In September 2020, Microsoft reported that it had detected increased cyberattacks originating in Russia, China, and Iran targeting political groups as well as the Trump and Biden campaigns.[273] The announcement emphasized that these attacks were part of a larger effort to disrupt the 2020 election. According to Microsoft, Russia-based hacking group Strontium targeted over 200 political organizations, China-based hacking group Zirconium attacked high-profile individuals associated with the Biden campaign, and Iran-based hacking group Phosphorus continued attacks on personal accounts of individuals associated with the Trump campaign. According to Microsoft, its security tools detected and stopped most of these attacks.
- In October 2020, Microsoft announced that, alongside law enforcement and private sector partners, it had disrupted TrickBot, an infamous ransomware distributor.[274] After a court order granted the disruption request, Microsoft disabled more than 90 percent of TrickBot's machines, so the botnet would no longer be able to initiate new infections ahead of the election.[275] **CYBERCOM** reportedly pursued a separate but parallel effort to disrupt TrickBot.[276]
- In September 2020, Microsoft launched a "deepfake" detector tool ahead of the election called the "Video Authenticator."[277] The tool aimed to prevent the dissemination of election-related disinformation.

Google's Threat Analysis Group (TAG) aimed to identify bad actors, disable their accounts, and inform relevant government officials and law enforcement.

- TAG reportedly tracked more than 270 targeted or state-backed attacker groups from more than 50 countries and updated a quarterly bulletin with new information.[278] Relevant threats included phishing campaigns, zero-day vulnerabilities, hacking, and disinformation.
- TAG claimed it worked in close partnership with the FBI's Foreign Influence Task Force, among other government agencies.[279]
- In June 2020, the group publicly shared that a Chinese APT group targeted Biden campaign staff, and an Iranian APT targeted the Trump campaign staff through a phishing campaign.[280]

Cybersecurity firm **Trustwave** identified detailed information about millions of U.S. voters for sale on hacker forums.[281]

- The firm claimed that the detected database includes 186 million records and that a separate U.S. consumer database includes 245 million records, with over 400 data points provided about each person. The firm discovered that these databases include not only illegally obtained data, but also publicly available information on citizens.
- Trustwave reported its findings to the North Carolina Board of Elections because of the security concerns associated with making all voter information public, but the board responded that its website includes only public records.[282]

Cloudflare publicly reported and exposed a record number of cyberattacks targeting the Trump campaign in June 2020. [283]

Social Media Companies

Regulating Political Advertisements

Google introduced new changes to its advertisement policies during the election cycle.

- In April 2020, **Google** began requiring advertisers to complete a verification program to buy ads. Users could then see disclosures that list this information about the advertiser.[284]
- Following Election Day, Google limited political ads by prohibiting advertisers from running ads "referencing candidates, the election, or its outcome" across all of Google's ad serving platforms, including YouTube.[285] This policy continued until December 10, 2020.[286]

Facebook sought to secure its advertisements from interference and disinformation by:

- Prohibiting advertisers from creating and running new advertisements on politics, social issues, and elections from October 27 through Election Day.
- Temporarily banning all ads with content related to social issues, elections, or politics from running following the close of polls on November 4 at 12:00 a.m.[287]
    - The company made an exception for the Georgia Senate runoff and lifted its ad prohibition in the state until polls closed in the January 5 runoff election.[288]
- Prohibiting advertisements that discourage voting or participating in the U.S. 2020 Census, delegitimize lawful voting procedures, delegitimize election results due to failure to tabulate on Election Day, claim widespread voter fraud, claim that the election date can be moved, declare victory prematurely, and include information inconsistent with health authorities' recommendations on voting safety.[289]
- Allowing users in the United States to opt out of viewing electoral, political, or social issue ads from candidates or political action committees in their Facebook or Instagram feeds.[290] [291]
- Blocking foreign state-controlled media from running ads in the United States starting in Fall 2020.[292]

Pre-bunking

Facebook "pre-bunked" voting information across its platforms by launching the "Voting Information Center" (VIC) and featuring it across the top of users' dashboards on both Instagram and Facebook. The center:

- Shared authoritative information, including how and when to vote, as well as details about voter registration, voting by mail and early voting."[293]
- Advised users that it relied on non-partisan information from multiple sources.
- Encouraged users to visit one's own state election website for official government information.
- Included a library of facts about the elections, such as "election results have taken longer this year. Millions of people across the United States voted by mail, and mail ballots take longer to count."[294]
- Ran notifications at the top of their dashboards directing people in the United States to visit the VIC for information about the vote-counting process.

Google shared authoritative information on voting across its platforms by:[295]

- Working with the Associated Press (AP) to provide authoritative election results on Google for both federal and state level races in more than 70 languages.
- Partnering with the National Voter Registration Day to spread awareness about voter registration and increase the accessibility of information.
- Delivering voting information across Google Search, Maps, and Assistant features.

YouTube delivered authoritative election information by:

- Providing information panels at the top of search results on the election and videos that discussed the election. The panels included information about federal or presidential candidates, voter registration, and how to vote.

- Sharing up-to-date and contextualized election information in panels:
    - Prior to an official outcome, the panel noted that "election results may not be final" and linked to Google's election results feature and to CISA's "Rumor Control" page for debunking election integrity misinformation.
    - On Saturday, November 7, YouTube altered the panel to note that "the AP has called the Presidential race for Joe Biden," with a link to a Google page with the results.[296]
    - On December 9, YouTube updated the panel, linking to the "2020 Electoral College Results" page from the Office of the Federal Register, noting that states have certified presidential election results, with Joe Biden as the President-elect. It also continued to include a link to CISA, explaining that states certify results after ensuring ballots are properly counted and correcting irregularities and errors.[297]

Twitter pre-emptively debunked false information by:

- Running authoritative information panels across the top of users' feeds.[298]
    - The week before the election, Twitter placed warnings on all U.S. users' timelines that the results of the election may be delayed and that users may encounter misinformation on mail-in voting.[299]
    - When users searched for key terms related to voter registration around the time of the election, they saw a prompt in English or Spanish pointing them to official sources.
- Launching a 2020 elections hub including curated news from reputable outlets, live streams of major election events, information on candidates for congressional and gubernatorial elections in users' states, and localized news.[300]
    - The hub also included voter education public service announcements, including factual information on voter registration and requesting absentee ballots.

TikTok launched an in-app U.S. election guide in September 2020 that worked to provide authoritative information on the election by:[301]

- Sharing trusted information about voting and political candidates from the National Association of Secretaries of State and BallotReady.
- Providing education videos about misinformation, media literacy, and the elections process, powered by MediaWise.

Highlighting Foreign State-Affiliated Accounts

Facebook sought to increase transparency around foreign state-affiliated media and officials by:

- Labeling ads from state-affiliated media that were "wholly or partially under the editorial control of their government."[302]
- Extending the 2019 Facebook policy of labeling foreign state-affiliated media to Instagram pages, posts, and profiles, as well as to advertisements.
- Blocking ads from these publishers from running in the United States.[303]

Twitter labeled accounts of key government officials (such as foreign ministers and official spokespeople) as well as accounts belonging to state-affiliated media entities, including their editors-in-chief and/or their senior staff.[304]

- These labels only applied to accounts from the countries represented in the five permanent members of the UN Security Council; labeled accounts included China's Xinhua News and Russia's Sputnik and RT.[305]

Altering Algorithms and Architecture

Facebook enacted preemptive policy changes and applied protocols that altered the company's algorithm with the goal of restricting the circulation of false content.

- Ahead of the election, Facebook developed “break glass measures’” that would treat “repeatedly fact-checked hoaxes” (RFH) uniquely. For the measures to be applied, RFH had to have met three eligibility criteria—falsity, virality, and severity—as well as have gained policy leadership approval.[306]
  - The “break glass measures” included adding more “friction” to sharing false content, demoting content on the News Feed if it contained election-related misinformation to make it less visible and limiting the distribution of election-related Facebook Live streams.
- On November 5, Facebook deployed these “break glass measures” following the rampant spread of mis- and disinformation, such as the “Stop the Steal” Facebook group. According to The New York Times, Facebook:[307]
  - Demoted content that may have contained misinformation, “including debunked claims about voting.”
  - Limited the distribution of Live videos that may have related to the election.
  - Increased friction through requiring additional steps to share posts.
- In mid-December, Facebook confirmed that it had reversed these algorithmic changes.[308] Facebook reportedly told The New York Times that the measures had promoted authoritative news sources over hyperpartisan outlets but were “never supposed to be permanent.”[309]

Facebook also made other changes to its typical protocols for Facebook Groups and Messenger features:

- In September 2020, Facebook set a forwarding limit on Facebook Messenger with the goal of slowing the spread of viral misinformation.[310]
- On October 1, Facebook increased “Group Admin” tools, allowing group administrators greater control over content posted to group pages, while also providing administrators with educational resources.[311] In addition, Facebook made it easier for users to discover and join conversations in public groups.
- On October 30, Facebook suspended recommendations for users to join groups dealing with social and political issues ahead of the presidential election.[312]
- Starting around November 7, Facebook began applying new rules to groups with “too many” posts in violation of Facebook’s community standards. The new policy required applicable groups (public or private) to have administrators and moderators approve each submission manually for 60 days following implementation.[313]

On October 29, 2020, **Instagram** removed the “recent” tab that gathers recently uploaded content tagged with a given hashtag. The company sought to reduce the “real-time spread” of potentially false and harmful content around the election.[314]

Twitter developed and implemented policies designed to “increase context and encourage more thoughtful consideration before Tweets are amplified.”[315]

- In October 2020, Twitter instituted a new policy to encourage users to add their own commentary when sharing content by prompting them to “Quote” all Tweets instead of “Retweet.”[316]
  - Twitter announced it was removing this feature on December 16, 2020, citing a decrease in sharing and a prevalence of short and low-character quote Tweets.[317]
- In October 2020, Twitter also announced that Tweets labeled as misleading from U.S. political figures and influential U.S. accounts would be restricted from Replies and Retweets, would require users to click through a warning to view the Tweet, and would not be included in recommendations.[318]
  - For other tweets labeled due to a violation of Twitter’s policies against misleading information, users were given a prompt pointing them to credible information about the topic before they were able to retweet.
  - Twitter also noted in the announcement that Tweets that were labeled for including misleading content were automatically de-amplified in the company’s recommendation systems.
- In October 2020, Twitter said it would prevent recommendations from accounts that are not followed from showing up in users’ timelines and not allow notifications for these Tweets.[319]

  - Twitter also stated that it would include added context in the "For You" tab in the United States which "added a description, representative Tweet, or article" to "Trends."[320]

YouTube took steps to raise up authoritative information with the goal of limiting the spread of election (and coronavirus) related misinformation. The company:

- Expanded the "Fact Check feature" to the United States.[321] YouTube added information panels containing articles from its network of third-party fact checkers, among them FactCheck.org, PolitiFact, and The Washington Post Fact Checker.[322]
- Elevated authoritative sources from publishers such as CNN and Fox News.[323]
- Shared information on how to register and vote in the election as well as information from the EAC on how to volunteer at the polls.[324]

Moderating Content

Facebook sought to tackle foreign interference on its platform by removing "coordinated inauthentic behavior and subsequently publishing reports to inform the public.[325]

- On March 12, Facebook removed 49 Facebook accounts, 69 Pages, and 85 Instagram accounts attributed to actors in Ghana and Nigeria working on behalf of Russian individuals for "engaging in foreign interference." According to Facebook, the network primarily targeted the United States. The network was "in the early stages of building an audience and was operated by local nationals—some wittingly and some unwittingly—on behalf of individuals in Russia."[326]
- On July 8, Facebook removed 54 Facebook accounts, 50 Pages, and 4 Instagram accounts affiliated with Republican operative Roger Stone that engaged in coordinated inauthentic behavior in the United States.[327]
- On September 22, Facebook removed 155 accounts, 11 Pages, 9 Groups, and 6 Instagram accounts originating in China. This network "focused primarily on the Philippines and Southeast Asia more broadly, and also on the United States."[328]
- On October 8, Facebook removed 200 Facebook accounts, 55 Pages, and 76 Instagram accounts originating in the United States. This activity "focused primarily on domestic U.S. audiences and also on Kenya and Botswana."[329]
- On October 27, Facebook removed 2 Facebook Pages and 22 Instagram accounts originating from Mexico and Venezuela for violating its policy against foreign interference. The small network was in the "early stages of building an audience" primarily targeted the United States.[330]

Twitter updated and applied its Civic Integrity Policy.

- In October 2020, Twitter updated its Civic Integrity Policy stating that it would remove tweets that encouraged violence or that called for interference with election results or polling places.[331]
- Twitter took action to enforce its Civic Integrity Policy around the election.
  - On November 4, 2020, Twitter suspended an account after it posted a video of a man supposedly burning ballots cast for President Trump.[332] The video was debunked by Politifact, which found that the material in the video was actually a collection of sample ballots.[333]
  - On November 4, Twitter suspended several fake accounts posing as news organizations and reporting fake results for the U.S. elections.[334] Several accounts mimicked the logos and account name of the Associated Press, and at least one mimicked CNN. Most of these accounts worked to prematurely declare Joe Biden the winner in various states; however, one account announced that Trump had won reelection.[335]
  - On December 11, Twitter prevented users from liking and replying to a series of tweets from President Trump in which he falsely claimed that he won the election.[336]
    - On January 8, Twitter permanently banned Donald Trump for violating its "Glorification of Violence" policy.[337]

YouTube adapted and applied its content removal policies at different stages throughout the election cycle.

- In the months leading up to and month after the election, YouTube's policy for content removal remained consistent with its existing "Community Guidelines" that prohibit "content that intends to scam, mislead, spam, or defraud other users" or "content that promotes harmful or dangerous behavior."[338]
    - On February 3, the day of the Iowa Caucus, YouTube clarified how its "Community Guidelines" would be applied to election-related content, sharing that it would remove content that delivers misleading information about voting processes or advances false claims regarding a candidate or elected official's eligibility to serve in office.[339]
    - Between September and December 2020, YouTube banned over 8,000 channels and "thousands" of election-related videos that violated its policies.[340]
- On December 9, 2020, YouTube said that it would begin removing newly uploaded content that alleged widespread fraud or errors changed the 2020 U.S. presidential election outcome.[341] YouTube said that the safe harbor deadline preempted this policy.[342]

Applying Labels

Twitter applied labels to identify misinformation on its platform before and after the 2020 election.

- Twitter introduced and updated several new labeling policies, including:
    - In February 2020, Twitter introduced a new rule that banned sharing synthetic or manipulated media likely to cause harm and said that the company may label tweets containing synthetic and manipulated media to provide context. [343]
        - The policy responded to data gathered from Twitter users who indicated that they would like Twitter to provide more information to them and label significantly altered content.[344]
    - In September 2020, Twitter announced a new policy through which it will "label or remove false or misleading information intended to undermine public confidence in an election or other civic process."[345]
        - According to Twitter, posts that violate this policy include false or misleading information that could cause confusion about civic processes, disputed claims that could undermine faith in the election, claims of victory before results were certified, and calls for unlawful conduct to prevent a peaceful transfer of power.[346]
    - In October 2020, Twitter clarified that its labeling policy would apply to all accounts that tweet false claims of victory for any candidate and for any tweet meant to incite interference in the election process or implementation of election results.[347] Twitter also announced and confirmed several policies to restrict sharing and spread of labeled accounts.
    - On November 4, Twitter hid several of President Trump's tweets behind warning labels saying that the claims made in the tweets were disputed and possibly misleading.[348] Twitter limited users' ability to "like" and reply to the posts.[349]
    - On November 7, The Washington Post reported that Twitter would no longer apply labels to false claims of victory from President Trump, as it previously had before the election had been called in Joe Biden's favor.[350]
    - On November 12, Twitter said that it would continue policies to place warning labels on misleading or disputed content about the election and to limit how these claims could be shared.[351] Twitter indicated that during the period of time from October 27 to November 11, it labeled roughly 300,000 tweets containing "disputed and potentially misleading information."[352]
- As part of its labeling efforts, Twitter notably labeled numerous tweets from President Trump and his allies, including:
    - Several of President Trump's tweets in the months leading up to and the days following the 2020 election for violating the company's rules, including terms of service and "civic and election integrity" rules.[353] Between November 3 and November 5, Twitter placed labels on 38 percent of president Trump's tweets/retweets (11 in total).[354]

    - Posts from Trump's allies sharing false claims around the election results and security, including premature claims of victory in Pennsylvania on November 4, 2020 and Senators Lindsey Graham and Ted Cruz's claims of voter fraud.[355]

Facebook instituted new policies to apply information labels to content that shared false or harmful information about the election. Its policies included:

- In September 2020, the company stated it would apply labels to posts that delegitimize the outcome of the election or discuss the legitimacy of voting methods.
- Facebook also announced that it would apply labels to posts in which any candidate or campaign tried to declare victory before the determination of final results and directed users to Reuters and the National Election Pool official results.[356]

Coordinating with Partners

Major tech companies—including **Facebook, Google, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn, and Wikimedia**—coordinated with U.S. government officials. The companies met to discuss trends with the U.S. government agencies tasked with protecting the integrity of the election.

- On August 12, 2020, the companies' representatives and U.S. government partners discussed "preparations for the upcoming conventions and scenario planning related to election results."[357]
- On September 16, 2020, the companies' representatives met to share ways to help provide "real-time clear information about the voting process and election results"; to "counter targeted attempts to undermine the election conversation before, during, and after the election," including hack and leak operations; and to detect "efforts for potential cyberattacks targeting campaigns, voting agencies, and agencies responsible for voting infrastructure."[358]

Strengthening Cybersecurity

Twitter faced a coordinated attack targeting its employees with "access to internal systems and tools" in July 2020. The attack compromised several prominent Twitter accounts, including those of Joe Biden, Bill Gates, and Elon Musk. In response, Twitter worked to tighten its cybersecurity protocols by:

- Requiring all Twitter employees to use physical two-factor authentication.[359]
- Requiring members of the U.S. executive branch, Congress, presidential campaigns, and political parties to adhere to more stringent security measures, including developing a strong password and encouraging each account to enable two-factor authentication.[360]
    - Twitter also created a default setting preventing unauthorized password changes.
- Hiring a head of security with responsibilities including information security, site integrity, physical security, platform integrity, and engineering.[361]

Civil Society and Media

Civil Society Organizations

Civil society organizations reinforced election security efforts by supporting election officials through funding initiatives, training, and resources; by helping to improve campaign cybersecurity; and by reinforcing trust in election officials and processes. Given the broad range of civil society actors that played a role in this effort, this section does not capture every instance of civil society support for the election, but instead aims to highlight a representative subset.

Support for Election Officials

Trainings, Workshops, and Best Practices

During its 2020 Legislative Conference, the **National Association of Counties (NACo)** invited election experts from **CISA** and **DHS** to brief NACo members on threats and best practices for securely administering elections.[362]

- In March 2020, NACo held a workshop in which national and county election officials shared opportunities and best practices for securing elections.[363]
- Through a series of virtual town halls, the organization also invited local election officials to share their own best practices.[364]

In the months leading up to the 2020 election, the **NASED** and **NASS** released several joint statements highlighting efforts by state and local election officials to prepare to safely conduct elections during the coronavirus pandemic.[365]

- **NASED** and **NASS** also announced partnerships with the American Bar Association (ABA) to encourage ABA members to serve as poll workers.[366]
- **NASED** also held a virtual conference for members and the public to highlight efforts and best practices to ensure safe and secure voting in 2020.[367]
- **NASS** held similar conferences and workshops at a national virtual conference to help state election officials prepare for the election.[368]
- **NASS** provided members with online issue briefs for key issues around the election and cybersecurity[369], including on HAVA grants[370], cyber threats to elections, and preparing for elections during the coronavirus pandemic.[371]
- **NASS** held a virtual cybersecurity workshop and offered cybersecurity guidance and resources for members.[372]
- **NASS** issued public statements on election preparations, asserting confidence in executing elections during the pandemic.[373]

The **Election Center**, a nonprofit whose members almost exclusively include elections officials and government administrators, offered resources, certified training, and consulting services (for a fee) to local and state election officials to help improve election administration around the country. The Election Center also offered regional workshops for government elections units.[374]

The **Center for Tech and Civic Life (CTCL)**, a civic engagement advocacy nonprofit, aimed to offer low-cost and free courses for elections and campaigns offices through professional development and skills courses.

- Coursework covered topics as they apply to elections offices, including "Cybersecurity for Election Officials" and "Poll Worker Management Best Practices.
- Two online series were free in 2020, including "Communicating Trusted Election Information" and "COVID-19 Webinars for Election Officials." The other courses cost $50 each.[375]

Google partnered with the **University of Southern California's Annenberg School** to offer nonpartisan training to nearly 4,000 elections officials, secretaries of state, campaign staffers, and other officials in all 50 states.[376] The training included preventing digital attacks, phishing campaigns, and hacking attempts.[377]

The **National Task Force on Election Crises**, a cross-partisan group of more than 50 elections experts, published guidance and recommendations for election officials, journalists, and voters leading up to the 2020 election to ensure preparedness in handling potential crises and disinformation.[378]

The joint **Stanford-MIT Healthy Elections Project** brought together academics, civic organizations, election administrators, and election experts together to identify and promote best practices for safely and securely conducting the 2020 election.[379] **NYU's Brennan Center for Justice** carried out similar efforts, providing guidance for election officials on how to spend funds wisely to secure elections and advocating for additional support from Congress.[380]

Support for Election Infrastructure and Cybersecurity

In June 2020, the nonprofit **Center for Internet Security (CIS)** announced a partnership with **Microsoft** to make Microsoft's Azure cloud platform compatible with the EI-ISAC's "Albert Sensors" network monitoring program.[381]

CIS also partnered with the **EAC** to pilot a technology verification program focused on non-voting election technology including electronic poll books, election night reporting websites, and electronic ballot delivery systems.[382]

In fall 2020, **CIS,** through grant funding from CISA, launched its Malicious Domain Blocking and Reporting (MDBR) service. The service prevents government devices from connecting to web domains known to be affiliated with ransomware, other forms of malware, phishing campaigns, and other threats. It was available free-of-charge to members of both the **Multi-State Information Sharing and Analysis Center and the Elections Infrastructure ISAC**. According to CIS, it could potentially prevent a ransomware attack by preventing an employee who opens a phishing email from connecting to a link that would ordinarily trigger a payload.[383]

Ahead of the 2020 elections, the **Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)** offered a range of resources for election officials, including weekly news alerts, cybersecurity spotlights, election security self-assessments, election security checklists, incident report checklists, guides for election security/ equipment procurement, video tutorials, technology recommendations, and tabletop exercises.[384]

- The **EI-ISAC** also offered members services including a 24/7 Security Operation Center, access to secure portals for sharing and communicating, incident response services, free training opportunities, access to its malicious code analysis platform, and vulnerability management updates.[385] For additional fees, officials could receive consulting and vulnerability assessments.
- The **EI-ISAC** also offers a Cybersecurity Toolkit for Elections in partnership with the **Global Cyber Alliance**.[386] This toolkit, launched in 2019, offers free operational tools and guidance to support implementation of CIS's recommendations for election infrastructure security.[387]

The **EI-ISAC**, in cooperation with **CISA**, operated an election day "virtual situational awareness room," which brought together "500 election and voter-protection officials, IT staff, vendors and representatives from social media companies and political parties."[388] It aimed to share information around election security, monitor threats, and provide support and guidance.[389]

Funding and Advocacy

CTCL offered grants to assist local election officials' administration of the 2020 elections.[390] CTCL began accepting grant applications in early September 2020, and all recipients received at least $5,000. 2,500 jurisdictions across the country received grants to expand voter registration and outreach, recruit and train poll workers, and maintain safety protocols.[391] Other election-related civil society organizations, including **NACo**, publicized the grants.[392]

In July 2020, **NACo** briefed members of Congress on the role that county-level officials play in elections and that additional support was required. Ahead of the meeting, NACo's election subcommittee sent a letter to Congress requesting additional funding to support county officials in administering the 2020 election.[393]

Public Communication and Education

NASS organized the #TrustedInfo2020 campaign starting in November 2019 to amplify state and local election officials as authoritative sources of election-related information. [394] The goal was to drive voters directly to election officials' websites and social media pages to ensure voters received accurate election information and cut down on mis/disinformation.[395] More than 40 supporting partners from across sectors were asked to support the initiative by amplifying the message on their social media pages, websites, and other communications channels.[396] Among the partners were:

- Technology organizations: **Google, Facebook, and Twitter.**
- Federal departments working in elections: **EAC, DHS, Federal Voting Assistance Program.**
- Research and advocacy organizations: **Alliance for Securing Democracy, Brennan Center for Justice, Bipartisan Policy Center, and the Carter Center,** among others.
- National associations: **NASED, National Association of Attorneys General, NACo, National Conference of State Legislatures, and National Governors Association**, among others.
- Election and civic engagement nonprofits: **Democracy Fund, Verified Voting**, among others.

NASED and **NASS** published several statements on election officials' role in combatting disinformation:

- On July 30, 2020, **NASS** called on Congress to support the federal law that stipulates that federal elections are to be held on the first Tuesday after the first Monday in November.[397] The statement highlighted the diligent work that election officials were doing to conduct the 2020 election safely and securely.
- On October 30, 2020, **NASS** and **NASED** shared their confidence in the nation's "elections systems, processes, safety, and security."[398] The statement highlighted the work done by election officials to prepare for the election and encouraged voters to be wary of disinformation and look to local and state election officials for trustworthy information.
- On November 4, 2020, **NASED** and **NASS** highlighted the safe and secure execution of the 2020 election and encouraged citizens to look to election officials for trusted information on results.[399]

On October 14, 2020, **NASS** held a "Virtual Elections 101" briefing with members of the media to educate reporters on election preparations overall, discuss the decentralized nature of elections, and to address election cybersecurity, voting by mail, and other important topics reporters should know when covering the 2020 election.[400]

Ahead of the 2020 election, the **National Council on Election Integrity**—a bipartisan organization made up of former political, government, and civic leaders—launched a $20 million public education campaign aimed to emphasize the security of the 2020 election and the need for all votes to be counted.[401] Efforts included a $4 million ad buy to run in battleground states to stress the security of the 2020 election.

NACo published data highlighting how local election officials "work diligently and tirelessly to process and count ballots, and thereby execute a fair, secure and accurate election" through its Election Center and County Explorer program.[402]

- NACo highlighted the positive steps taken by officials to prepare for elections in several blog posts, suggested best practices, and shared resources.[403]

Various civil society organizations, including multi-denominational faith-based organizations,[404] as well as major business groups, associations, and leaders, published joint statements encouraging confidence in the 2020 elections and officials, calling on leaders to avoid spreading false information, and urging voters to be patient while votes were counted.[405] Statements also called on voters to look to local officials for trusted information.[406]

A broad network of civil rights and media literacy organizations established the **Disinfo Defense League** to develop ways to protect communities of color from racialized disinformation.[407] The group created specialized memes, videos, and webinars and has distributed multilingual informational materials including a "Disinfo Defense Toolkit" to help give minority communities accurate information.[408]

Civil society organizations, including **Election SOS, Over Zero, and the National Task Force on Election Crises** gathered and published resources to help guide journalists in safely and responsibly reporting on the 2020 election, including how to avoid spreading mis and disinformation and how to build public trust in reporting.[409] **The Stanford Cyber Policy Center** also released guidelines on how newsrooms should "report responsibly on hacks and disinformation."[410]

Cross-Sector Coordination

On July 27, a coalition of research organizations launched the **Election Integrity Partnership (EIP)**, aimed to facilitate information-sharing between the research community, election officials, government agencies, civil society organizations, and social media platforms. The coalition targeted efforts toward detecting and mitigating attempts to delegitimize election results or deter people from voting. Members of the coalition include the **Stanford Internet Observatory and Program on Democracy and the Internet, Graphika, the Atlantic Council's Digital Forensic Research Lab, and the University of Washington's Center for an Informed Public.**[411]

- **EIP** published regular reports and quick-turn analyses on disinformation efforts targeting the election process and flagged disinformation for online platforms.[412]
- Ahead of the election, **EIP** published a handbook to guide election officials in navigating and mitigating election day misinformation.[413]
- **EIP** identified major lines of effort to delegitimize the election and held regular briefings on threats in the lead-up to, on, and after election day.[414]
    - Following the rise of reports that voters in Florida and Alaska received threatening emails demanding that they vote for President Trump, allegedly from the far-right group the Proud Boys, **EIP** provided a quick rebuttal of the emails, stating that the emails were part of an active measure campaign perpetrated by a foreign actor.[415]
    - On Election Day, **EIP** published a report highlighting Russian Internet Research Agency efforts to amplify narratives of voter fraud.[416] The report was picked up by the New York Times; however, the networks it exposed were minimal in impact (typically garnering only single-digit engagement) and the coverage of the network may have spread its efforts further than the operation itself.[417]
- On Election Day, **EIP** identified and exposed several prominent livestreams claiming to showcase election results that garnered significant traffic and attention.[418] YouTube eventually removed the videos for violating its community guidelines.
- In the wake of the election, the group rebutted varying claims of election fraud through interviews, blog posts, and tweet threads.

Campaign Cybersecurity

On July 10, 2020, the **Biden campaign** hired former White House senior cybersecurity adviser Chris DeRusha to oversee secure campaign technology and opened other cybersecurity staff positions, including a senior cyber incident response and threat analyst and a senior cloud security architect. The Biden team confirmed that all staff underwent cybersecurity training and were tested with regular mock phishing attempts.[419]

In response to questions following news of the Biden campaign's public hiring of a new senior cybersecurity adviser, the **Trump campaign** confirmed to reporters that it had also hired a full-time cybersecurity professional; although, it did not provide further details.[420]

The bipartisan nonprofit **Defending Digital Campaigns (DDC)** offered free and low-cost cybersecurity services to both the Trump and Biden campaigns.[421]

- Recognizing the heightened threat of moving campaign work online due to the coronavirus pandemic, the group worked to lower the cost of credible vendors' services, provide education and training resources for campaign staff, and share information on current threats and concerns.

- **DDC** partnered with several major tech companies to provide free support to campaigns, including with cybersecurity firm Cloudflare to provide cyber protections to 50 political campaigns from candidates across the political spectrum in 27 states.[422]
- Board members include former government officials, campaign staff, and private sector professionals.
- **DDC** received special permission from the FEC to provide all campaigns, regardless of party, with the support they need within the limits of campaign finance law.[423]

The nonpartisan nonprofit organization **Cyberdome** was established in March 2020 to provide cybersecurity support to political campaigns.

- The organization offered a range of cybersecurity resources and services through its Political Campaign Information Sharing and Analysis Organization, which required an annual fee to access.[424]
- Cyberdome also reportedly donated funds to qualified cybersecurity vendors to help campaigns.
- The firm's advisory board includes former U.S. defense officials, including former cabinet members.[425]

News Media

This section captures snapshots of media coverage around inflection points in the election cycle to provide a general overview of coverage. More research is necessary to construct a complete picture of both fringe and conventional media coverage of narratives throughout the election cycle.

Coverage of Major Inflection Points

Iowa Caucuses

During the Iowa Caucuses, major news outlets across the political spectrum expressed concern about the delayed reporting of election results, though they refrained from suggestions that results may have been hacked.[426] Some examples of reactions to the Caucuses include:

- **Fox News's** Molly Hemingway said, "Of course, the old-fashioned way used to provide results at this hour so that is interesting and it's worth thinking about why Iowa is so important."[427]
- **CNN's** Van Jones remarked, "This is starting to feel like possibly a real debacle. Technical problems they're not disclosing we could be late on this."[428]

New York Post's Hunter Biden Laptop Story

Following the New York Post's publication of an unverified story claiming to rely on a laptop belonging to then-candidate Joe Biden's son, reporters generally approached the story with caution, with many holding off on reporting or stressing the unverified nature of the story and importance of the provenance of the information.

- For example, outlets like The New York Times and Washington Post kept the story off their homepage.[429]
- Fox News reportedly "passed" on publishing the original story after being approached by Rudy Giuliani.[430]
- Two prominent reporters—Maggie Haberman of The New York Times and Jake Sherman of Politico—quoted or shared the story on their personal Twitter accounts.[431]
- Notably, several outlets had publicized updated processes and guidelines for how they planned to report on potential hack and leak operations or stolen information in the election cycle.
    - For example, **Marty Baron, Executive Editor of The Washington Post,** implemented five "principles for covering potential hacked or leaked material ahead of the election."[432] These principles required the newsroom to review "the newsworthiness of the information, its authenticity and whether" reporters can determine the material's provenance. Baron noted, "We should resist the instinct to post a story simply because a competitor has done so. We should not tweet or retweet reports or comments on hacked or leaked material without first reporting them out."[433]

  - **New York Times reporters** developed guidelines called "The EMAIL Method," or Evidence, Motive, Activity, Intent, and Labels, to depict how the outlet should cover political hack and leaks.[434]

Iran's Proud Boys Email Operation

On October 20, local and national news organizations began reporting that Democratic voters in Florida and Alaska had reported receiving emails from the far-right group known as the "Proud Boys" demanding that they vote for President Trump.[435] The reports detailed:

- Statements from elections officials.[436]
- That the emails came from a host associated with an Estonian domain.[437]
- The local, state, and federal investigations of the intimidation incidents.[438]
- That voter intimidation is a federal offense subject to up to one year imprisonment.[439]

After government officials provided rapid attribution of the operation to Iran, reporters quickly shared the updated story and attribution, focusing on Iranian goals and intentions.

Election Night Reporting

On election night, conventional media used similar processes as those in prior elections to report and predict results beginning in the early evening as polls began to close. In the leadup to election night, news media organizations had largely cautioned viewers that results would arrive slower than in the past due in part to a large increase in mail-in ballots.[440]

After the Associated Press called Florida for President Trump on election night, outlets provided a range of reactions.

- **MSNB**C minimized the win, whereas Tucker Carlson of Fox News called it the "future of the country."[441]
- At the same time, many news outlets expressed the need to stay patient and calm.[442]
- **Fox News** recognized that the election outcome was still undecided, and **CNN** noted that a "close election may come down to AZ, PA, MI, WI."[443]

Most media outlets displayed caution in declaring victory for any candidate, instead reminding viewers that final results would take days and that the election would not be decided on that night.[444]

Post-Election Reporting Covering President Trump

Starting election night, and in the weeks that followed, news broadcasters made varied decisions about whether to air Trump's speeches when he shared false information on the election.[445] News outlets gave varying levels of credence to Trump's and his allies' voter fraud claims. Most dismissed the accusations[446] or refuted previous accusations,[447] but some provided them more attention.[448]

- On the morning of November 4, 2020, President Trump appeared to declare a premature victory. This led some networks to take action, including:
  - **MSNBC** cut off their coverage of Trump's speech, saying that the network was "duty-bound to point out that when he says 'we did win this election, we've already won,' that is not based in the facts at all."[449]
  - **NBC** cut away from the speech to explain why Trump could not claim victory in Pennsylvania and Michigan since votes were still being tabulated.
- On November 5, 2020, during a Trump speech where he again cast doubt on the election process, news outlets made similar decisions.
  - As Nieman Lab reports, "**NBC, ABC, and CBS** all cut their feeds mid-way through Trump's sixteen-minute speech, taking the decision to stop broadcasting it to their viewers because of concerns over baseless claims about election fraud."[450]

    - Other networks, including **CNN** and **Fox**, broadcast the whole speech, but reported afterwards that the President had "offered no evidence for his accusations."
- On November 9th, **Fox News** cut away from Kayleigh McEnany, the White House press secretary, saying "the network could not in good conscience continue to air her false claims, for which she has provided no supporting evidence."[451]
- **Conventional media** also largely framed Trump's victory declaration as false in headlines, according to the EIP.[452]

Throughout the following weeks, Trump, his allies, and his surrogates pushed unfounded allegations of election fraud and foreign interference. These efforts drew varying levels of coverage from conventional outlets, though many strongly rebuked the President and his lawyers' claims.

Appendix B: Acronyms

APT: Advanced Persistent Threat

CARES Act: Coronavirus Aid, Relief, and Economic Security Act

CFITF: Countering Foreign Influence Task Force

CIS: Center for Internet Security

CISA: Cybersecurity and Infrastructure Security Agency

CTCL: Center for Tech and Civic Life

CTIIC: Cyber Threat Intelligence Integration Center

CYBERCOM: U.S. Cyber Command

DDC: Defending Digital Campaigns

DHS: Department of Homeland Security

DOJ: Department of Justice

EAC: Election Assistance Commission

EI-ISAC: Election Infrastructure Information Sharing and Analysis Center

EIP: Election Integrity Partnership

FBI: Federal Bureau of Investigation

FEC: Federal Election Commission

GCC: Election Infrastructure Government Coordinating Council

HAVA: Help America Vote Act

IC: Intelligence Community

MDBR: Malicious Domain Blocking and Reporting

NACo: National Association of Counties

NASED: National Association of State Election Directors

NASS: National Association of Secretaries of State

NCSC: National Counterintelligence and Security Center

NSA: National Security Agency

ODNI: Office of the Director of National Intelligence

RFH: Repeatedly Fact Checked Hoaxes (Facebook)

SCC: Election Infrastructure Sector Coordinating Council

TAG: Google's Threat Analysis Group

VIC: Voting Information Center (Facebook)

Acknowledgements

The authors would like to thank Lindsay Gorman, David Levine, David Salvo, and Bret Schafer who read and commented on drafts of this report. Their expertise helped sharpen its findings and recommendations. We are also grateful to Kayla Goodson and Thomas Morley, who provided crucial assistance with the production of the final paper. Our deepest thanks are reserved for Matthew Cohen, Conor Cunningham, and Katya Sankow, who collected the data that shaped all aspects of this paper, and for Jennifer Gurev, whose diligent analysis informed its insights.

Endnotes

[1] National Intelligence Council, Foreign Threats to 2020 US Federal Elections, Intelligence Community Assessment, March 16, 2021.

[2] Bret Schafer, “Foreign Amplification of Voter Fraud Narratives: How Russian, Iranian, and Chinese Messengers Have Leveraged Post-Election Unrest in the United States,” Alliance for Securing Democracy, November 24, 2020; DFR Lab, “#StopTheSteal: Timeline of Social Media and Extremist Activities Leading to 1/6 Insurrection,” Just Security, February 10, 2021.

[3] Special Counsel Robert S. Mueller, Report on the Investigation into Russian Interference in the 2016 Presidential Election, U.S. Department of Justice, March 2019. (“Mueller Report”).

[4] United States Senate, Select Committee on Intelligence, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views, 2020; United States Senate, Select Committee on Intelligence, Volume 3: U.S. Government Response to Russian Activities, 2020. (“SSCI Report”).

[5] Steven Levy, “When is it OK to Mine Hacked Emails?” Wired, October 17, 2016; Josephine Lukito and Chris Wells, “Most major outlets have used Russian tweets as sources for partisan opinion: study,” Columbia Journalism Review, March 8, 2018.

[6] Nicole Perlroth, et al., “Facebook Exit Hints at Dissent on Handling of Russian Trolls,” The New York Times, March 19, 2018; Brennan Weiss, “September 27: Zuckerberg regrets dismissing Russian misinformation,” Business Insider, September 27, 2017; Jon Swaine, “Twitter admits far more Russian bots posted on election than it had disclosed,” The Guardian, January 19, 2018.

[7] 2018 Year in Review, Election Infrastructure ISAC, Center for Internet Security, 2018; Julian E. Barnes, “Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections,” The New York Times, February 26, 2019.

[8] Election Infrastructure ISAC, 2018.

[9] Josh Rudolph and Thomas Morley, Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies, Washington: Alliance for Securing Democracy, August 18, 2020; David Levine, “The election went remarkably well. Here’s how to make the next one even better,” The Fulcrum, November 13, 2020; United States Department of Homeland Security, Homeland Threat Assessment October 2020, October 2020 (“Homeland Threat Assessment 2020”).

[10] Jessica Brandt and Josh Rudolph, Spies and Money: Legal Defenses Against Foreign Interference in Political Campaigns, Washington: Alliance for Securing Democracy, January 2021.

[11] Nicholas Fandos and Michael D. Shear, “Trump Impeached for Abuse of Power and Obstruction of Congress,” The New York Times, December 18, 2019; Mary Clare Jalonick, “Congress’ fight over election security bills,” AP, August 3, 2019; Jordain Carney, “Senate GOP blocks three election security bills,” The Hill, February 11, 2020.

[12] Matt Schrader, Friends and Enemies: A Framework for Understanding Chinese Political Interference in Democratic Countries, Washington: Alliance for Securing Democracy, April 22, 2020; Ariane Tabatabai, Iran’s Authoritarian Playbook: The Tactics, Doctrine, and Objectives behind Iran’s Influence Operations, Washington: Alliance for Securing Democracy, September 17, 2020.

[13] Jessica Brandt and Amber Frankland, Leaks, Lies, and Altered Tape: Russia’s Maturing Information Manipulation Playbook, Washington: Alliance for Securing Democracy, October 14, 2020.

[14] National Intelligence Council, 2021; Ellen Nakashima, et al., “U.S. government concludes Iran was behind threatening emails sent to Democrats,” The Washington Post, October 22, 2020.

[15] Brandt and Rudolph, 2020.

[16] National Intelligence Council, 2021.

[17] Fandos and Shear, 2019; Zaid Shoorbajee, “Election infrastructure ISAC created to share threats specific to voting systems,” CyberScoop, March 16, 2018; Kate Conger, “Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says,” The New York Times, October 30, 2019.

[18] See Appendix A, Section II: Private Sector.

[19] See Appendix A, Section II: Private Sector, “Social Media Companies”

[20] Ryan Mac and Craig Silverman, "Facebook Quietly Suspended Political Group Recommendations Ahead Of The US Presidential Election," Buzzfeed, October 30. 2020; Renee Diresta, "Social Network Algorithms Are Distorting Reality By Boosting Conspiracy Theories," Fast Company, May 11, 2016.

[21] Vijaya Gadde and Kayvon Beykpour, "Additional steps we're taking ahead of the 2020 US Election," Twitter, October 9, 2020.

[22] Mike Isaac, "Facebook, Alarmed by Discord Over Vote Count, Is Said to Be Taking Action," The New York Times, November 5, 2020.

[23] Andy Stone, Twitter post, October 14, 2020, 11:10 AM.

[24] Mike Isaac and Kate Conger, "Twitter Changes Course After Republicans Claim 'Election Interference,'" The New York Times, October 15, 2020.

[25] Bret Schafer, "The hack-and-leak conundrum: There's no good way to combat the latest form of dirty trick," The New York Daily News, October 20, 2020.

[26] Sara Fischer, "Twitter changes hacked materials rules after banning N.Y. Post story," Axios, October 16, 2020

[27] Isaac and Conger, 2020; Natasha Lomas, "Twitter changes its hacked materials policy in wake of New York Post controversy," TechCrunch, October 16, 2020.

[28] Elizabeth Dwoskin, "Facebook and Twitter take unusual steps to limit spread of New York Post story," The Washington Post, October 15, 2020.

[29] Dwoskin, 2020; Isaac and Conger, 2020; Abram Brown, "You Haven't Heard More About Hunter Biden's Emails Because Twitter And Facebook Didn't Want You To," Forbes, October 15, 2020; Audrey Conklin, "Facebook manually limited New York Post Hunter Biden story: Report," Fox News, October 30, 2020.

[30] Daisuke Wakabayashi, "In Hubbub Over New York Post Report, YouTube Stands Apart," The New York Times, October 15, 2020.

[31] National Intelligence Council, 2021.

[32] Schafer, 2020.

[33] DFR Lab, 2021.

[34] Charles Davis, "Election officials debunked the Arizona 'SharpieGate' conspiracy theory that right-wing activists spread online," Business Insider, November 6, 2020.

[35] Sheera Frenkel, "The Rise and Fall of the 'Stop the Steal' Facebook Group," The New York Times, November 5, 2020.

[36] Jessica Guynn, "Facebook deploys emergency measures to curb misinformation as nation awaits election results," USA Today, November 5, 2020.

[37] Kevin Roose, "Facebook reverses postelection algorithm changes that boosted news from authoritative sources," December 16, 2020.

[38] Chris Mills Rodrigo, "Twitter says it labeled 300,000 posts around the election," The Hill, November 12, 2020; Isaac, 2020.

[39] Barbara Ortutay, "Weeks after election, YouTube cracks down on misinformation," AP, December 9, 2020.

[40] "Supporting the 2020 U.S. election," YouTube, December 9, 2020.

[41] Mark Sullivan, "The pro-Trump 'Stop the Steal' movement is still growing on Facebook," Fast Company, November 5, 2020; Jack Brewster, "Facebook Banned 'Stop The Steal'—Then Other Groups Popped Up In Its Place," Forbes, November 6, 2020.

[42] DFR Lab, 2021.

[43] Ibid., Marjorie Taylor Greene, Twitter Feed, November 7, 2020 (archived by Wayback Machine – Internet Archive); Paul Gosar, Twitter Post, November 6, 2020, 1:41 PM.

[44] Donie O'Sullivan, et al., "Misinformation Watch," CNN, accessed March 16, 2021; Guynn, 2020.

[45] DFR Lab, 2021.

[46] The Long Fuse: Disinformation and the 2020 Election, Election Integrity Partnership, 2021. ("The Long Fuse")

[47] Craig Silverman and Ryan Mac, "Facebook Knows That Adding Labels To Trump's False Claims Does Little To Stop Their Spread," Buzzfeed, November 16, 2020.

[48] Megan A. Brown, et al., "Twitter put warning labels on hundreds of thousands of tweets. Our research examined which worked best," The Washington Post, December 9. 2020.

[49] Election Integrity Partnership, 2021.

[50] Peter Dizikes, “The catch to putting warning labels on fake news,” MIT, March 2, 2020; Thomas Nugent, “Are Facebook And Twitter Ready For The US Election?” BusinessBecause, October 30, 2020.

[51] Election Integrity Partnership, 2021.

[52] Ibid.

[53] Gadde and Beykpour, 2020.

[54] Roose, December 16, 2020.

[55] Roose, December 16, 2020; Isaac, 2020.

[56] Kevin Roose, et al., “Facebook Struggles to Balance Civility and Growth,” The New York Times, November 24, 2020; Roose, December 16, 2020.

[57] Jeff Horwitz, “Facebook Knew Calls for Violence Plagued ‘Groups,’ Now Plans Overhaul,” The Wall Street Journal, January 31, 2021.

[58] Twitter Support, Twitter post, December 16, 2020, 6:22 PM.

[59] Roose, December 16, 2020.

[60] Leon Yin and Alfred Ng, “Facebook Said It Would Stop Pushing Users to Join Partisan Political Groups. It Didn’t,” The Markup, January 19, 2021.

[61] Laura Hazard Owen, “Two new studies show, again, that Facebook doesn’t censor conservatives,” Nieman Lab, October 30, 2020; Cale Guthrie Weissman, “Facebook’s algorithm change had an impact on politicians, but not the ones you think,” Fast Company, May 31, 2018.

[62] Jon Keegan, et al., “Trump’s False Posts Were Treated with Kid Gloves by Facebook,” The Markup, February 16, 2021.

[63] “Announcing the EIP,” Election Integrity Partnership, July 27, 2020. [Disclosure: The Alliance for Securing Democracy was a participating member of the Election Integrity Partnership.]

[64] Samantha Bradshaw, et al., “Election Delegitimization: Coming to you Live,” Election Integrity Partnership, November 17, 2020; Joe Bak-Coleman, et al., “Weaponizing projections as tools of election delegitimization,” Election Integrity Partnership, November 3, 2020.

[65] Emily Birnbaum, “Meet the researchers and activists fighting misinformation,” Protocol, November 3, 2020; “The Fight Against Disinformation Requires the Right Tools,” PEN America, October 27, 2020; “Resources,” National Task Force on Election Crises, accessed March 17, 2021; Ashley Quarcoo, “Three New Ways Civil Society Is Protecting the U.S. Election,” Carnegie Endowment for International Peace, October 28, 2020.

[66] Birnbaum, 2020.

[67] Brian Naylor, “Former Public Officials Group To Spend $20 Million To Highlight Secure Elections,” NPR, October 7, 2020.

[68] Adam Entous, et al., “Kremlin trolls burned across the Internet as Washington debated options,” The Washington Post, December 25, 2017; Adam Entous, “The Rise and Fall of a Kremlin Troll,” The New Yorker, July 19, 2018.

[69] Scott Shane, “The Fake Americans Russia Created to Influence the Election,” The New York Times, September 7, 2017.

[70] Entous, July 19, 2018; Indictment, United States v. Netyshko, No. 1:18-cr-215 (D.D.C. July 13, 2018), Doc. 1.

[71] SSCI Report, Volume 1.

[72] Ibid.

[73] “#Protect2020 Strategic Plan,” Cybersecurity and Infrastructure Security Agency, February 2020.

[74] See Appendix A, Section I Public Sector, Executive Branch

[75] “EI-ISAC™ Services,” Center for Internet Security, accessed February 16, 2021.

[76] Benjamin Freed, “‘No bar’ to what election officials shared on Election Day, DHS says,” StateScoop, November 4, 2020; Benjamin Freed, “‘This is how it was all supposed to work’: The EI-ISAC readies for Election Day,” StateScoop, November 3, 2020; Sean Lyngaas, “How US security officials are watching for threats ahead of Election Day,” Cyberscoop, October 20, 2020.

[77] Freed, November 3, 2020

[78] See Appendix A, Section I: Public Sector, Executive Branch, “Coordination, Training, and Intelligence-Shar-

ing"; "DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections," Government Accountability Office, GAO-20-267, February 2020.

79 Kevin Collier, "Despite Trump's claims, federal agencies foresee a secure election," NBC, October 9, 2020.

80 "U.S. Election Assistance Commission Offers No-Cost Online Cybersecurity Training For Election Officials," Election Assistance Commission, June 22, 2020; "Election Security 2020 – Congressional Members Talking Points," Office of the Director of National Intelligence, accessed March 17, 2021.

81 See Appendix A, Section III: Civil Society and Media

82 National Intelligence Council, 2021.

83 "U.S. Election Assistance Commission and the Center for Internet Security Partner on Non-Voting Election Technology Verification Pilot Program," Center for Internet Security, June 17, 2020; Phil Goldstein, "Microsoft Makes Azure Compatible with Election Security Sensors," StateTech, July 23, 2020.

84 See Appendix A, Section III: Civil Society and Media; "About Us," National Association of Election Officials, accessed March 17, 2021; "Our Work," Center For Tech and Civic Life, accessed March 17, 2021.

85 "What We Do," Defending Digital Campaigns, accessed March 17, 2021; Amanda Storey, "Following the 2020 U.S. Election with Google," Google, October 27, 2020.

86 Benjamin Freed, "MS-ISAC hits 10,000 members, eyes continued growth with local governments," StateScoop, November 20, 2020; "Statement of Preliminary Findings and Conclusions," International Elections Observer Mission, OSCE, November 3, 2020; "Election Administration at State and Local Levels," National Conference of State Legislatures, accessed March 17, 2021.

87 "Election Administration at State and Local Levels," National Conference of State Legislatures.

88 Homeland Threat Assessment October 2020.

89 Kevin Collier, "Gov't election security struggles to reach some counties," NBC, August 17, 2020; Sean Lyngaas, "Matt Masterson, CISA's top election security official, to step down," CyberScoop, December 10, 2020.

90 The timing of the publication of this report in October 2020 drew significant criticism, including from CISA Director Christopher Krebs, who noted that the release of the report before Election Day fails to include CISA's actions through the entirety of the election cycle. Executive Director of the National Association of State Election Directors (NASED) also criticized the report for failing to adequately represent the progress in coordination between CISA and the election community. For more, see: Sean Lyngaas, "CISA chief rips IG report, touts election security efforts," CyberScoop, October 27, 2020.

91 Joseph V. Cuffari to Christopher C. Krebs, October 22, 2020, Department of Homeland Security, Office of the Inspector General, "DHS Has Secured the Nation's Election Systems, but Work Remains to Protect the Infrastructure," OIG-21-01.

92 "Center for Internet Security Releases New Elections Technology Cybersecurity Supply Chain Guide," Homeland Security Today, February 11, 2021.

93 Ibid.

94 Alex Stamos, "Enough is enough. Here's what we should do to defend against the next Russian cyberattacks," The Washington Post, December 15, 2020.

95 Joseph Bodnar and Bradley Hanlon, "Three Takeaways for Defending Against Foreign Interference from the SolarWinds Hacks," Alliance for Securing Democracy, December 22, 2020; For more, see Appendix A, Section II: Private Sector, Cybersecurity and Technology Companies; Appendix A, Section I: Public Sector, Executive Branch.

96 David Levine, The Election Official's Handbook: Six steps local officials can take to safeguard America's election system, Washington: Alliance for Securing Democracy, February 13, 2020.

97 Jane C. Timm, "Election workers weren't surprised by the Capitol riot. Trump's supporters targeted them first," NBC, February 3, 2021.

98 Johnny Kaufman, "'You Better Run': After Trump's False Attacks, Election Workers Faced Threats," NPR, February 5, 2021.

99 Edward-Isaac Dovere, "Biden: McConnell stopped Obama from calling out Russians," Politico, January 23, 2018.

100 Pete Williams, "Barr says no investigations into 2020 candidates, campaigns without his approval," NBC,

February 6, 2020.

[101] Betsy Woodruff Swan, et al., "Dems outraged as Trump administration scales back election security briefings," Politico, August 29, 2020.

[102] William Evanina, "Statement By NCSC Director William Evanina: Election Threat Update For The American Public," Office of the Director of National Intelligence, August 7, 2020; Mark Moore, "Mike Pompeo warns that China poses bigger threat to US election than Russia," New York Post, September 3, 2020.

[103] National Intelligence Council, 2021.

[104] Barry A. Zulauf to Marco Rubio and Mark Warner, January 6, 2021, Office of the Director of National Intelligence, IC Analytical Ombudsman, "RE: SSCI# 2020-3029"; Ellen Nakashima, "Political appointees, career analysts clashed over assessments of Russian, Chinese interference in 2020 election," The Washington Post, January 8, 2021.

[105] Jen Kirby, "Trump's own officials say 2020 was America's most secure election in history," Vox, November 13, 2020.

[106] Nick Corasaniti, "Four falsehoods Giuliani spread about Dominion," The New York Times, January 25, 2021.

[107] David E. Sanger and Nicole Perlroth, "Trump Fires Christopher Krebs, Official Who Disputed Election Fraud Claims," The New York Times, November 17, 2021.

[108] Savannah Behrmann, "Senate removes measure demanding campaigns report foreign election help," USA Today, June 30, 2020.

[109] Maggie Miller, "State and local officials beg Congress to send more election funds ahead of November," The Hill, July 8, 2020.

[110] Paul M. Krawzak, "New election security funds won't come easy for hard-hit states," Roll Call, April 2, 2020.

[111] "HEROES Act Includes Funding Election Officials Need to Run Safe, Secure Elections in 2020," Brennan Center for Justice, May 12, 2020.

[112] Tom Scheck, et al., "How Private Money From Facebook's CEO Saved The 2020 Election," NPR, December 8, 2020.

[113] Ibid.

[114] Schafer, November 24, 2020.

[115] Julian E. Barnes, "Senate Report Criticizes Response to Russian Meddling and Blames Partisanship," The New York Times, February 6, 2020.

[116] Perlroth, et al., 2018; Weiss, 2017, Swaine, 2018.

[117] Internet Crime Complaint Center (IC3), Federal Bureau of Investigation, accessed March 17, 2021; See Appendix A, Section I: Public Sector, Executive Branch, "Public Announcements and Communication"; Appendix A, Section I: Public Sector, Executive Branch, "Investigations, Sanctions, and Proactive Defense."

[118] Ellen Nakashima, "U.S. undertook cyber operation against Iran as part of effort to secure the 2020 election," The Washington Post, November 3, 2020; Ellen Nakashima, et al., "U.S. government concludes Iran was behind threatening emails sent to Democrats," The Washington Post, October 22, 2020.

[119] "Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data," FBI and CISA, Joint Cybersecurity Advisory, AA20-304A, October 30, 2020.

[120] "Treasury Sanctions Russia-Linked Election Interference Actors," Department of the Treasury, September 10, 2020; the Treasury Department also sanctioned several of Derkach's associates in January 2021, see Appendix A, Section I: Public Sector, Executive Branch, "Investigations, Sanctions, and Proactive Defense."

[121] Olivia Beavers, "US intelligence says Russia seeking to 'denigrate' Biden," The Hill, August 7, 2020; a U.S. Intelligence Community report later revealed that Derkach was likely acting under the purview of Russian President Vladimir Putin: National Intelligence Council, 2021.

[122] "Rubio, Warner Release Joint Statement in Response to NCSC Director Evanina," U.S. Senate Select Committee on Intelligence, August 10, 2020.

[123] See Appendix A, Section II: Private Sector, Cybersecurity and Technology Companies, "Threat Detection and Response."

[124] See Appendix A, Section II: Private Sector, Social Media Companies, "Moderating Content."

[125] National Intelligence Council, 2021.

[126] “#TrustedInfo,” National Association of Secretaries of State, accessed March 17, 2021.

[127] Joe Pompeo, ““Connect The Dots”: Marty Baron Warns Washington Post Staff About Covering Hacked Materials,” Vanity Fair, September 23, 2020; Lauren Jackson and Desiree Ibekwe, “Covering Political Hacks and Leaks Ahead of the Election,” The New York Times, October 23, 2020; See Appendix A, Section III: Civil Society and Media, News Media.

[128] Schafer, November 24, 2020.

[129] “Evaluating Platform Election-Related Speech Policies,” Election Integrity Partnership, October 28, 2020.

[130] Paul M. Barrett and J. Grant Sims, False Accusation: The Unfounded Claim That Social Media Sites Censor Conservatives, New York: New York University Center for Business and Human Rights, February 2021, p. 21-23.

[131] Renee DiResta, How misinformation spreads online — and what we can do about it, Emerson Collective, 2020.

[132] “Repeat Offenders: Voting Misinformation on Twitter in the 2020 United States Election,” Election Integrity Partnership, October 29, 2020.

[133] The Long Fuse; Carly Miller, “Facebook, It’s Time to Put the Rules in One Place,” Lawfare, March 15, 2021.

[134] The Long Fuse.

[135] Irene V. Pasquetto, et al., “Tackling misinformation: What researchers could do with social media data,” Harvard Misinformation Review, December 9, 2020.

[136] The Long Fuse.

[137] Evelyn Douek, “The Facebook Oversight Board Should Review Trump’s Suspension,” Lawfare, January 11, 2021; Faiza Patel and Laura Hecht-Felella, “Oversight Board’s First Rulings Show Facebook’s Rules Are a Mess,” Just Security, February 19. 2021.

[138] Karen Kornbluh and Ellen P. Goodman, “Bringing Truth to the Internet,” Democracy, 2019. For an additional proposal for a federal regulator, see: Tom Wheeler, et al., New Digital Realities; New Oversight Solutions in the U.S., Cambridge, MA; Harvard Shorenstein Center, August 2020.

[139] Dipayan Ghosh, “The Commercialization of Decision-Making: Towards a Regulatory Framework to Address Machine Bias over the Internet,” Harvard Shorenstein Center, April 24, 2020; Kevin Roose, “How the Biden Administration Can Help Solve Our Reality Crisis,” The New York Times, February 2, 2021.

[140] Dipayan Ghosh, et al., The Weaponized Web: Tech Policy Through the Lens of National Security, Washington: Alliance for Securing Democracy and the Harvard Mossavar-Rahmani Center, December 2020.

[141] Wheeler, et al., 2020.

[142] Kornbluh and Goodman, 2019; Barrett and Sims, 2021.

[143] Andrea Córdova McCadney, et al., “2020’s Lessons for Election Security,” Brennan Center for Justice, December 16, 2020.

[144] Córdova McCadney, et al., 2020; Defending Digital Democracy Project, Beyond 2020 Policy Recommendations for the Future of Election Security, Cambridge, MA: Harvard Belfer Center, February 2021.

[145] Defending Digital Democracy Project, 2021.

[146] Córdova McCadney, et al., 2020; Eric Geller, “Forget the conspiracy theories — here are the real election security lessons of 2020,” Politico, December 27, 2020.

[147] Córdova McCadney, et al., 2020; Geller, 2020.

[148] Defending Digital Democracy Project, 2021.

[149] Ibid.

[150] Michael Wines, “Here Are the Threats Terrorizing Election Workers,” The New York Times, December 3, 2020.

[151] Elections 2030: A Nonpartisan Blueprint For Effective U.S. Election Administration, Open Source Election Technology Institute, December 2020.

[152] Jon Mazella, “Cybersecurity Lessons Learned from the 2020 Election Season,” StateTech, December 9, 2020.

[153] Defending Digital Democracy Project, 2021.

[154] The Long Fuse.

155 David Salvo and Heidi Tworek, "The Next North American Election: How Canada Is Protecting Itself and What Can Still Be Done," Alliance for Securing Democracy, March 5, 2019.
156 "Following Passage of their Provision to Establish a Center to Combat Foreign Influence Campaigns, Klobuchar, Reed Ask Director of National Intelligence for Progress Report on Establishment of the Center," Office of Senator Amy Klobuchar, February 14, 2020.
157 Alana Wise, "Trump Fires Election Security Director Who Corrected Voter Fraud Disinformation," NPR, November 17, 2020.
158 Similar legislation to establish a maximum of two five-year terms for the CISA Director position received bipartisan support in the House of Representatives, see: Justin Katz, "House lawmaker stumps for 5-year term for CISA's director," FCW, November 17, 2020.
159 Roose, February 2, 2021.
160 "Commission on the Practice of Democratic Citizenship," American Academy of Arts and Sciences, June 2020.
161 "Joint Statement from Elections Infrastructure Government Coordinating Council & The Election Infrastructure Sector Coordinating Executive Committees," Cybersecurity and Infrastructure Security Agency, November 12, 2020.
162 For more communications by Executive Branch actors, see "Investigations, Sanctions, and Proactive Defense."
163 "Joint Statement From DOS, DOJ, DOD, DHS, ODNI, FBI, NSA, and CISA On Preparations For Super Tuesday," Office of the Director of National Intelligence, March 2, 2020.
164 William Evanina, "Statement By NCSC Director William Evanina: 100 Days Until Election 2020," Office of the Director of National Intelligence, July 24, 2020.
165 William Evanina, "Statement By NCSC Director William Evanina: Election Threat Update For The American Public," Office of the Director of National Intelligence, August 7, 2020.
166 "Joint Statement from Elections Infrastructure Government Coordinating Council Executive Committee," National Association of State Election Directors, August 20, 2020.
167 Shannon Vavra, "List of 2020 election meddlers includes Cuba, Saudi Arabia and North Korea, US intelligence official says," CyberScoop, August 20, 2020.
168 Christopher Krebs, "Statement From CISA Director Krebs On Security And Resilience Of 2020 Elections," Cybersecurity and Infrastructure Security Agency, October 20, 2020.
169 Christopher Wray, "FBI Director Christopher Wray's Remarks at Press Conference on Election Security," Federal Bureau of Investigation, October 21, 2020.
170 "DHS Has Secured the Nation's Election Systems, but Work Remains to Protect the Infrastructure," Department of Homeland Security Office of Inspector General, October 22, 2020.
171 Christopher Krebs, "Statement From CISA Director Krebs Following Final Day Of Voting," Cybersecurity and Infrastructure Security Agency, November 4, 2020; Mariam Baksh, "CISA's Elections Operations Center to Remain Open for Another 45 Days," Nextgov, November 3, 2020.
172 "Joint Statement From Elections Infrastructure Government Coordinating Council & The Election Infrastructure Sector Coordinating Executive Committees," Cybersecurity and Infrastructure Security Agency, November 12, 2020.
173 Ellen Nakashima, "Political appointees, career analysts clashed over assessments of Russian, Chinese interference in 2020 election," The Washington Post, January 8, 2021.
174 "Spoofed Internet Domains Pose Cyber and Disinformation Risks to Voters," Cybersecurity and Infrastructure Security Agency, October 2, 2020.
175 "Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Elections," Cybersecurity and Infrastructure Security Agency, October 1, 2020.
176 "Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting," Cybersecurity and Infrastructure Security Agency, September 30, 2020.
177 "False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections," Cybersecurity and Infrastructure Security Agency, September 28, 2020.

178 “Cyber Threats to Voting Processes Could Slow But Not Prevent Voting,” Cybersecurity and Infrastructure Security Agency, September 24, 2020.

179 “FBI Warns Voters About Election Crimes Ahead of the November 2020 Election,” Federal Bureau of Investigation, September 24, 2020.

180 “#PROTECT2020 Rumor vs. Reality,” Cybersecurity and Infrastructure Security Agency, accessed February 11, 2021.

181 “Resilience Series Graphic Novels,” Cybersecurity and Infrastructure Security Agency, accessed February 11, 2021.

182 “Electronic Infographic Products,” Cybersecurity and Infrastructure Security Agency, accessed February 11, 2021.

183 “Foreign Interference,” Cybersecurity and Infrastructure Security Agency, accessed February 11, 2021.

184 “Election Disinformation Toolkit,” Cybersecurity and Infrastructure Security Agency, accessed February 11, 2021.

185 “Protected Voices,” Federal Bureau of Investigation, accessed February 11, 2021.

186 “FBI Washington Field Office Educates Citizens About Election Security and Foreign Malign Influence in Advance of the November Election,” Federal Bureau of Investigation, September 14, 2020.

187 “FBI And NCSC Release New Movie To Increase Awareness Of Foreign Intelligence Threats On Professional Networking Sites And Other Social Media Platforms,” Office of the Director of National Intelligence, September 29, 2020.

188 “Joint Statement from Elections Infrastructure Government Coordinating Council Executive Committee,” National Association of State Election Directors, October 22, 2020.

189 Election Infrastructure Security Resource Guide, Washington: Cybersecurity and Infrastructure Security Agency, May 2020.

190 Election Security – Physical Security of Voting Locations and Election Facilities, Washington: Cybersecurity and Infrastructure Security Agency, 2020.

191 Election Infrastructure Cyber Risk Assessment, Washington, Cybersecurity and Infrastructure Security Agency, June 28, 2020.

192 “How to use,” The U.S. Election Assistance Commission, accessed February 11, 2021.

193 Mail-In Voting In 2020 Infrastructure Risk Assessment, Washington: Cybersecurity and Infrastructure Security Agency, July 28, 2020.

194 “Cyber Incident Detection And Notification Planning Guide For Election Security,” Cybersecurity and Infrastructure Security Agency, accessed February 12, 2021.

195 “Guide To Vulnerability Reporting For America’s Election Administrators,” Cybersecurity and Infrastructure Security Agency, accessed July 12, 2021.

196 Sean Lyngaas, “How US security officials are watching for threats ahead of Election Day,” CyberScoop, October 20, 2020.

197 “Crossfeed Pilot,” Cybersecurity and Infrastructure Security Agency, accessed February 11, 2021.

198 Kevin Collier, “Despite Trump’s claims, federal agencies foresee a secure election,” NBC News, October 9, 2020.

199 “U.S. Election Assistance Commission Offers No-Cost Online Cybersecurity Training For Election Officials,” United States Election Assistance Commission, June 22, 2020.

200 “Election Security Preparedness,” U.S. Election Assistance Commission, September 2020.

201 “Availability of State Voter File and other Confidential Information,” Washington, United States Election Assistance Commission, October 29, 2020.

202 “2020 CARES Act Grants,” United States Election Assistance Commission, accessed February 12, 2021.

203 “U.S. Treasury makes $10 billion loan available to postal service as part of coronavirus relief,” Reuters, July 29, 2020.

204 Mark Pomerlau, “The US military is targeting foreign actors to defend the presidential election,” C4ISRNET, October 30, 2020.

205 Dwight Weingarten, “CYBERCOM, National Guard Partner to Secure Elections, Address Ransomware,”

MeriTalk, June 10, 2020.

206 ""Cyber 9-Line" Improves Cybersecurity and Enables Election Integrity," United States Cyber Command, June 9, 2020.

207 Cyber Threats To Elections: A Lexicon, Washington: Office of the Director of National Intelligence, 2018.

208 Risk Management For Electronic Ballot Delivery, Marking, And Return, Washington: Cybersecurity and Infrastructure Security Agency, May 8, 2020.

209 "Coronavirus (COVID-19) Resources," United States Election Assistance Commission, accessed February 11, 2021.

210 Election Security 2020: Congressional Members Talking Points, Washington: Office of the Director of National Intelligence, 2020.

211 "Director Of National Intelligence Announces Changes To Election Security Briefings," Office of the Director of National Intelligence, May 15, 2020.

212 Alex Marquardt and Zachary Cohen, "Top intelligence official to take charge of briefing candidates on election threats," CNN, May 15, 2020.

213 "Countering Foreign Influence Task Force," Cybersecurity and Infrastructure Security Agency, accessed February 11, 2021.

214 "#Protect2020 Strategic Plan," Cybersecurity and Infrastructure Security Agency, February 2020.

215 "U.S. Election Assistance Commission and the Center for Internet Security Partner on Non-Voting Election Technology Verification Pilot Program," Center for Internet Security, June 17, 2020.

216 Tim Starks, "Robocalls urging voters to skip Election Day are subject of FBI investigation, DHS official says," CyberScoop, November 3, 2020.

217 Philip Ewing, "Russian Hackers Break Into 2 County Systems, Stoking Election Security Fears," NPR, October 22, 2020.

218 Ellen Nakashima, "U.S. undertook cyber operation against Iran as part of effort to secure the 2020 election," The Washington Post, November 3, 2020.

219 John Ratcliffe, "DNI John Ratcliffe's Remarks At Press Conference On Election Security," Office of the Director of National Intelligence, October 22, 2020.

220 "Iranian Cyber Actors Responsible for Website Threatening U.S. Election Officials," Federal Bureau of Investigation, December 23, 2020.

221 Nakashima, November 3, 2020.

222 "Barr Tells DOJ to Probe Election Fraud Claims if They Exist," AP, November 9, 2020.

223 "Disputing Trump, Barr says no widespread election fraud," AP, December 1, 2020.

224 Laura Kelly, "Treasury Department sanctions inner circle of Russian agent Derkach for election interference," The Hill, January 11, 2021.

225 "Wanted: Information that brings to justice… Foreign Election Interference," United States Department of State Rewards for Justice Program, accessed February 16, 2021; "Rewards for Justice – Reward Offer for Information on Foreign Interference in U.S. Elections," United States Department of State, August 5, 2020 (retrieved from the Internet Archive Wayback Machine).

226 Cal Biesecker, "Cyber Command's Hunt Forward Teams Bolster Election Security, CISA Officials Say," IIOT Connection, November 3, 2020.

227 Lyngaas, 2020.

228 Nakashima, November 3, 2020.

229 United States Senate, Committee on Armed Services, *United States Special Operations Command and United States Cyber Command,* Testimony of General Paul M. Nakasone, March 25, 2021.

230 "2020 CARES Act Grants," United States Election Assistance Commission, accessed February 12, 2021.

231 Nathan Kohlenberg and Thomas Morley, "2021 NDAA: Malign Finance, Cyber Operations, and Artificial Intelligence Take Center Stage in Congress' Fight against Authoritarian Interference," Alliance For Securing Democracy, December 15, 2020.

232 "Securing the 2020 Election," Senate Republican Policy Committee, September 22, 2020; Joshua Barajas, "Experts testify on spread of online misinformation, conspiracy theories ahead of election," PBS, October 15,

2020.

233 United States House of Representatives, Committee on Homeland Security, Protecting America's Democracy: Ensuring Every Vote Counts, August 28, 2020.

234 Barajas, 2020.

235 "House Intelligence Committee to Hold Virtual Open Hearing with Facebook, Google and Twitter on Foreign Influence and Election Security," United States House of Representatives Permanent Select Committee on Intelligence, June 16, 2020; Tony Romm, et al., "Facebook, Google, Twitter CEOs clash with Congress in pre-election showdown," The Washington Post, October 28, 2020.

236 United States Senate, Select Committee on Intelligence, Russian Active Measures Campaigns And Interference In The 2016 U.S. Election, Vol. I-V, 116th Cong., 2nd Session, Washington: Government Printing Office, 2020.

237 Greg Miller, et al., "Senate report details security risk posed by 2016 Trump campaign's Russia contacts," The Washington Post, August 18, 2020.

238 Philip Ewing, "Pelosi, Dems Cite Election Interference In Request For Info From FBI," NPR, July 20, 2020.

239 Evanina, July 24, 2020; "Pelosi, Schumer, Schiff, Warner Joint Statement Following ODNI Announcement Regarding Election Security and Foreign Threats," Office of Senator Mark Warner, July 24, 2020.

240 "Pelosi, Schiff and Visclosky Demand Ratcliffe Resume Election-Related Intelligence Briefings to Congress," United States House of Representatives Permanent Select Committee on Intelligence, September 1, 2020.

241 "House Intelligence Committee Expands Investigation into Political Interference and Politicization of Intelligence at Department of Homeland Security and Office of Intelligence and Analysis," United States House of Representatives Permanent Select Committee on Intelligence, September 11, 2020.

242 Note: This list is not exhaustive, but provides a sample set of member letters on disinformation and other election threats.

243 "Rubio, Warner Release Joint Statement in Response to NCSC Director Evanina," United States Senate, Select Committee on Intelligence, August 10, 2020.

244 "Rubio, Warner Statement on Threats to Election Systems and Infrastructure," Office of Senator Marco Rubio, October 21, 2020.

245 Rebecca Klar, "Senate Democrats urge Google to improve ad policies to combat election disinformation," The Hill, December 7, 2020.

246 "Election Administration at State and Local Levels," National Conference Of State Legislatures, February 3, 2020.

247 For more on the National Association of Secretaries of State, National Association of State Election Directors, and other organizations for election officials, see Section III: Civil Society and Media, Civil Society Organizations. For more on local and state coordination with the executive branch, see Executive Branch, "Coordination, Training, and Intelligence-Sharing."

248 Luke Barr, "Elections officials push back on voter fraud claims," ABC, August 27, 2020; Steven Allen Adams, "State officials push back on Trump voter fraud claims in W.Va.," The Times Leader, October 1, 2020.

249 Zack Budryk, "Michigan denies hack after public voter information found on Russian online forum," The Hill, September 1, 2020.

250 Melissa Quinn, et al., "3 states targeted in Iranian email scheme report no evidence of breaches," CBS, October 22, 2020.

251 KS Sec. of State, Twitter post, November 3, 2020, 1:17 PM; Dana Nessel, Twitter post, November 3, 2020, 10:41 PM; NY AG James, Twitter post, November 3, 2020, 3:29 PM; Peter Salter, "State investigating reports of robocalls telling Nebraska voters to stay home," The Lincoln Journal Star, November 3, 2020; "State Officials Urge Voters To Ignore Robocalls," NPR, November 3, 2020.

252 Philadelphia DAO, Twitter post, November 3, 2020, 10:15 AM; "Pennsylvania Officials Debunk 'Deliberately Deceptive' Misinformation Spread By Trump Allies," NPR, November 3, 2020.

253 Amanda Seitz and Barbara Ortutay, "Pennsylvania emerges as online misinformation hot spot," AP, November 3, 2020.

254 Nick Corasaniti, et al., "The Times Called Officials in Every State: No Evidence of Voter Fraud," New York

Times, November 19, 2020.

255 Orion Rummler, "Georgia's Republican Lt. Gov.: No "credible incidents" of systemic voter fraud," Axios, November 9, 2020.

256 Amber Phillips, "The Republican election officials pushing back on Trump's baseless voter fraud claims," The Washington Post, November 13, 2020.

257 Beatrice Dupuy, "'SharpieGate' Debunked: Arizona State Officials Dispute Claim That Sharpie Pens Invalidate State's Ballots," NBC, November 5, 2020; Hannah Knowles, et al., "Election officials in Arizona rebut claims that ballots marked with Sharpies were disqualified," The Washington Post, November 4, 2020.

258 Travis M. Andrews and Ashley Fetters, "Local campaign officials are becoming election-week celebrities. They're too busy to notice," The Washington Post, November 5, 2020.

259 "Athenian Project," Cloudflare, accessed February 11, 2021.

260 "The Interactive Guide to Protecting Your Election Website," Cloudflare, accessed February 11, 2021.

261 "Cloudflare for Campaigns," Cloudflare, accessed February 11, 2021.

262 Jocelyn Woolbright, "Election Cybersecurity: Protecting the 2020 U.S. Elections," Cloudflare, August 17, 2020.

263 Jack Stubbs, "Hackers test defenses of Trump campaign websites ahead of U.S. election, security staff warn," Reuters, September 1, 2020.

264 Woolbright, 2020.

265 Jessica Lyons Hardcastle, "Election War Games Show Cyber Chaos Doesn't Cost Much," SDXCentral, August 24, 2020.

266 Amanda Storey, "Our work on the 2020 U.S. election," Google, February 11, 2021.

267 Mark Risher, "Teaming up with Defending Digital Campaigns on election security," Google, February 11, 2020.

268 Jordan Novet, "No emails have leaked from the 2020 election campaigns yet — tiny USB sticks may be one reason why," CNBC, December 23, 2020.

269 Amanda Storey, "An update on our 2020 U.S. election efforts," Google, August 13, 2020.

270 "Microsoft AccountGuard," Microsoft, accessed February 11, 2021; Jan Neutze, "Protecting democracy, especially in a time of crisis," Microsoft, April 2, 2020.

271 Jan Neutze, "New tools to secure democracy," Microsoft, June 18, 2020.

272 Ethan Chumley, "Increasing election security monitoring in cloud computing," Microsoft, June 22, 2020.

273 Tom Burt, "New cyberattacks targeting U.S. elections," Microsoft, September 10, 2020.

274 Tom Burt, "New action to combat ransomware ahead of U.S. elections," Microsoft, October 12, 2021.

275 Joseph Menn, "Microsoft disables most of cybercriminals' control over massive computer network," Reuters, October 20, 2020.

276 David E. Sanger and Nicole Perlroth, "Microsoft Takes Down a Risk to the Election, and Finds the U.S. Doing the Same," The New York Times, October 21, 2020.

277 Natasha Lomas, "Microsoft launches a deepfake detector tool ahead of US election," TechCrunch, September 2, 2020.

278 Shane Huntley, "Updates about government-backed hacking and disinformation," Google, May 27, 2020.

279 Amanda Storey, "Our work on the 2020 U.S. election," Google, December 9, 2020.

280 Shane Huntley, Twitter post, June 4, 2020, 1:03 PM.

281 Ziv Mador, "Massive US Voters and Consumers Databases Circulate Among Hackers," Trustwave, October 21, 2020.

282 "Voter Search," North Carolina State Board of Elections, accessed February 11, 2021.

283 Jack Stubbs, "Hackers test defenses of Trump campaign websites ahead of U.S. election, security staff warn," Reuters, September 1, 2020.

284 John Canfield, "Increasing transparency through advertiser identity verification," Google, April 23, 2020.

285 Amanda Storey, "Following the 2020 U.S. Election with Google," Google, October 27, 2020.

286 Chris Mills Rodrigo, "Google lifting political ad freeze Thursday," The Hill, December 9, 2020.

287 The policies regulating political advertisements on and around the election also applied to boosted posts.

Facebook said that because boosted posts are a form of paid promotion, they are considered ads; "Information on Ads About Social Issues, Elections or Politics in the United States During 2020 Election," Facebook, accessed February 11, 2021; Mike Isaac, "Facebook Widens Ban on Political Ads as Alarm Rises Over Election," The New York Times, October 7, 2020.

288 Taylor Hatmaker, "Facebook will turn all US political advertising off again after Georgia runoffs," TechCrunch, January 5, 2021.

289 "Information on Ads," Facebook.

290 Facebook began rolling out this option for users in other countries in 2020.

291 Mike Isaac, "Now You Can Opt Out of Seeing Political Ads on Facebook," The New York Times, August 21, 2020.

292 "Facebook to block foreign state media ads for US election," AFP, June 17, 2020. For more on company treatment of foreign state media and officials, see "Highlighting Foreign State-affiliated Accounts."

293 Mark Zuckerberg, "Historic Facebook campaign will boost voter registration, turnout and voices," USA Today, June 16, 2020.

294 "Voting Information Center," Facebook, accessed February 11, 2021.

295 Storey, October 27, 2020.

296 Daisuke Wakabayashi, "Election misinformation continues staying up on YouTube," The New York Times, November 10, 2020.

297 "Supporting the 2020 U.S. Election," YouTube, December 9, 2020.

298 David Ingram, "Twitter launches 'pre-bunks' to get ahead of voting misinformation," NBC, October 26, 2020.

299 Orion Rummler, "Twitter launches warnings on election misinformation and delays," Axios, October 26, 2020.

300 Bridget Coyne and Sam Toizer, "Helping you find accurate US Election News and Information," Twitter, September 15, 2020.

301 Michael Beckerman, "TikTok launches in-app guide to the 2020 US elections," TikTok, September 29, 2020.

302 Guy Rosen, et al., "Helping to Protect the 2020 US Elections," Facebook, October 21, 2019; Nathaniel Gleicher, "Labeling State-Controlled Media On Facebook," Facebook, June 4, 2020.

303 AFP, June 17, 2020.

304 Elizabeth Culliford, "Twitter labels state media, government officials' accounts," Reuters, August 6, 2020.

305 Ibid.

306 Alex Hern, "Facebook leak reveals policies on restricting New York Post's Biden story," The Guardian, October 30, 2020.

307 Mike Isaac, "Facebook, Alarmed by Discord Over Vote Count, Is Said to Be Taking Action," The New York Times, November 5, 2020.

308 Kevin Roose, "Facebook reverses postelection algorithm changes that boosted news from authoritative sources," The New York Times, December 16, 2020.

309 Ibid.

310 Jay Sullivan, "Introducing a Forwarding Limit on Messenger," Facebook, September 3, 2020.

311 Sarah Perez, "Facebook Groups to gain suite of new tools for managing discussions, surfacing public content," TechCrunch, October 1, 2020.

312 Ryan Mac and Craig Silverman, "Facebook Quietly Suspended Political Group Recommendations Ahead Of The US Presidential Election," Buzzfeed, October 30, 2020.

313 Heather Kelly, "Facebook's latest attempt to slow disinformation means probation for groups," The Washington Post, November 7, 2020.

314 Instagram Comms, Twitter post, October 29, 2020, 7:30 PM.

315 Vijaya Gadde and Kayvon Beykpour, "An update on our work around the 2020 US Elections," Twitter, November 12, 2020.

316 Vijaya Gadde and Kayvon Beykpour, "Additional steps we're taking ahead of the 2020 US Election," Twitter, October 9, 2020.

[317] Twitter Support, Twitter post, December 16, 2020, 6:22 PM.

[318] Gadde and Beykpour, October 9, 2020.

[319] Ibid.

[320] Ibid.

[321] “Expanding fact checks on YouTube to the United States,” YouTube, April 28, 2020.

[322] Casey Newton, “YouTube brings fact-check panels to searches in the United States,” The Verge, April 28, 2020.

[323] Leslie Miller, “Our approach to Election Day on YouTube,” YouTube, October 27, 2020.

[324] Leslie Miller, “Authoritative voting information on YouTube,” YouTube, September 24, 2020.

[325] Nathaniel Gleicher, “Coordinated Inauthentic Behavior Explained,” Facebook, December 6, 2018.

[326] Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior From Russia,” Facebook, March 12, 2020.

[327] Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior,” Facebook, July 8, 2020; Craig Timberg and Isaac Stanley-Becker, “Facebook closes network of accounts and pages affiliated with Roger Stone for manipulation,” The Washington Post, July 8, 2020.

[328] Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior,” Facebook, September 22, 2020.

[329] Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior,” Facebook, October 8, 2020.

[330] Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior,” Facebook, October 27, 2020.

[331] Gadde and Beykpour, October 9, 2020. For more details on Twitter’s Civic Integrity Policy, see “Algorithms and Architecture.”

[332] Isaac Stanley-Becker, et al., “Trump’s campaign and family boost bogus conspiracy theories in a bid to undermine vote count,” The Washington Post, November 4, 2020.

[333] Bill McCarthy, “Eric Trump retweets video falsely claiming man burned 80 Trump ballots,” Politifact, November 4, 2020.

[334] Dustin Volz, et al., “Fake Twitter Accounts Posing as News Organizations Prematurely Declare Election Victories,” The Wall Street Journal, November 5, 2020.

[335] Ibid.

[336] Celine Castronuovo, “Twitter briefly limits users interacting with Trump’s tweets about ‘stolen’ election,” The Hill, December 12, 2020.

[337] “Permanent suspension of @realDonaldTrump,” Twitter, January 8, 2021.

[338] “YouTube’s Community Guidelines,” Google, accessed February 16, 2021.

[339] Leslie Miller, “How YouTube Supports Elections,” YouTube, accessed February 16, 2021.

[340] “Supporting the 2020 U.S. election,” YouTube, December 9, 2020.

[341] Barbara Ortutay, “Weeks after election, YouTube cracks down on misinformation.” AP, December 9, 2020.

[342] YouTube, December 9, 2020.

[343] Twitter Safety, Twitter post, February 4, 2020, 4:00 PM.

[344] Yoel Roth and Ashita Achuthan, “Building rules in public: Our approach to synthetic & manipulated media,” Twitter, February 4, 2020.

[345] “Expanding our policies to further protect the civic conversation.” Twitter Safety, Accessed February 22, 2021.

[346] Elizabeth Culliford, “Twitter expands misinformation rules ahead of U.S. election,” September 10, 2020.

[347] Gadde and Beykpour, October 9, 2020.

[348] “US Election: Twitter hides Trump tweet about ‘disappearing’ lead,” BBC, November 4, 2020.

[349] For more on these policies, see “Altering Algorithms and Architecture.”

[350] Cat Zakrzewski, “The Technology 202: Trump’s refusal to concede presents a new test for social networks,” The Washington Post, November 10, 2020.

[351] Georgia Wells, “Twitter Says Labels and Warnings Slowed Spread of False Election Claims,” The Wall Street Journal, November 12, 2020; Shannon Bond, “Twitter Says Steps To Curb Election Misinformation Worked,” NPR, November 12, 2020.

[352] Chris Mills Rodrigo, “Twitter says it labeled 300,000 posts around the election,” The Hill, November 12, 2020.

353 "Twitter attaches disclaimer on Trump's 'mail drop boxes' tweet," Reuters, August 23, 2020.

354 Kate Conger, "Twitter Has Labeled 38% of Trump's Tweets Since Tuesday," The New York Times, November 5, 2020.

355 Chris Mills Rodrigo, "Twitter, Facebook label Trump camp's posts prematurely claiming victory in Pennsylvania," The Hill, November 4, 2020.

356 "New Steps to Protect the US Elections," Facebook, September 3, 2020.

357 Twitter Public Policy, Twitter post, August 12, 2020, 3:38 PM.

358 Google Public Policy, Twitter post, September 16, 2020, 4:48 PM.

359 Nicholas Thompson and Brian Barrett, "How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One," Wired, September 24, 2020.

360 Elizabeth Culliford, "Twitter will make key U.S. political accounts adopt tighter account security," Reuters, September 17, 2020.

361 Joseph Menn, "Twitter names famed hacker 'Mudge' as head of security," Reuters, November 16, 2020.

362 Rachel Looker, "Election officials talk security, funding, voter confidence," National Association of Counties, February 29, 2020.

363 "Protecting the Vote: How to Secure Your County's Election System," National Association of Counties, March 2, 2020.

364 "NACo Federal Policy Summit: Elections Town Hall," National Association of Counties, October 21, 2020.

365 "Joint NASS and NASED Statement on Voting Methods During COVID-19 Pandemic," National Association of State Election Directors, May 20, 2020.

366 "NASS and NASED Announce Joint Effort with ABA to Promote the Need for Poll Workers for 2020 General Election," National Association of State Election Directors, August 26, 2020; "Joint NASS and NASED Release: Hand Sanitizer in Support of 2020 Elections," National Association of State Election Directors, August 13, 2020.

367 "NASS 2020 Virtual Summer Conference Highlights," National Association of Secretaries of State, July 27, 2020.

368 Ibid.

369 "Election Security Resources and Briefings," National Association of Secretaries of State, accessed February 16, 2021; "Cybersecurity Resources and Briefings," National Association of Secretaries of State, accessed February 16, 2021.

370 "ISSUE BRIEFING: State Spending of Election Security Grant Funds," National Association of Secretaries of State, April 2020.

371 "NASS President Paul Pate & President-elect Maggie Toulouse Oliver Open Letter to Congress and American Voters on COVID-19 Election Preparations," National Association of Secretaries of State, March 25, 2020.

372 "Cybersecurity Resources and Briefings," National Association of Secretaries of State, accessed February 16, 2021.

373 "NASS and NASED 2020 Election Preparations and Reminders," National Association of Secretaries of State, October 30, 2020.

374 "About Us," The Election Center, accessed February 16, 2021.

375 "Courses," Center for Tech and Civic Life, Accessed February 17, 2021.

376 "Election Cybersecurity Initiative," University of Southern California, accessed February 16, 2021.

377 Storey, October 27, 2020.

378 "Resources," National Task Force on Election Crises, accessed February 16, 2021.

379 Stanford-MIT Healthy Elections Project, accessed February 16, 2021.

380 "Election Security," Brennan Center for Justice, accessed February 16, 2021.

381 Phil Goldstein, "Microsoft Makes Azure Compatible with Election Security Sensors," StateTech, July 23, 2020. For more information on this program, see Section II: Private Sector, Cybersecurity and Technology Companies.

382 "U.S. Election Assistance Commission and the Center for Internet Security Partner on Non-Voting Election Technology Verification Pilot Program," Center for Internet Security, June 17, 2020. For more information on

this program, see Section I: Government, Executive Branch, "Coordination, Training, and Intelligence-Sharing."

383 Benjamin Freed, "MS-ISAC adds domain-blocking service for state and local governments," StateScoop, September 8, 2020.

384 "EI-ISAC™ Services," Center for Internet Security, accessed February 16, 2021.

385 Ibid.

386 "Global Cyber Alliance And Center For Internet Security Launch Free Toolkit To Help States And Local Election Offices Bolster Cybersecurity," Global Cyber Alliance, June 25, 2019.

387 "The GCA Cybersecurity Toolkit for Elections," Center for Internet Security, accessed February 16, 2021.

388 Benjamin Freed, "'No bar' to what election officials shared on Election Day, DHS says," StateScoop, November 4, 2020.

389 Benjamin Freed, "'This is how it was all supposed to work': The EI-ISAC readies for Election Day," StateScoop, November 3, 2021.

390 Eryn Hurley and Aaliyah Nedd, "New $250 million grant program available to Local Election Officials," National Association of Counties, September 1, 2020.

391 Tom Scheck, et al., "How Private Money From Facebook's CEO Saved The 2020 Election," NPR, December 8, 2020.

392 Hurley and Nedd, 2020.

393 Eryn Hurley, "County officials ask Congress to provide additional funding to administer and secure elections," National Association of Counties, August 3, 2020.

394 "#TrustedInfo," NASS, accessed February 16, 2021.

395 Ibid.

396 Jessica Mulholland, "Secretaries of State Unite to Fight Election Misinformation," Government Technology, December 12, 2019.

397 3 U.S. Code § 1; "NASS Statement Addressing Suggestion of General Election Delay," National Association of Secretaries of State, July 30. 2020.

398 "NASED and NASS 2020 Election Preparations and Reminders," National Association of State Election Directors, October 30, 2020.

399 "Joint NASED and NASS 2020 Post-Election Day Statement," National Association of State Election Directors, November 4, 2020.

400 "ICYMI: NASS Elections 101 Virtual Press Brief," National Association of Secretaries of State, October 14, 2020.

401 Brian Naylor, "Former Public Officials Group To Spend $20 Million To Highlight Secure Elections," NPR, October 7, 2020.

402 Stacey Nakintu and Jonathan Harris, "New NACo data release highlights the key role of counties in elections," National Association of Counties, November 2, 2020.

403 Eryn Hurley, "U.S. Election Assistance Commission releases new resources to support local elections officials," National Association of Counties, August 19, 2020.

404 Quarcoo, 2020; "100," Civic Alliance, Accessed February 22, 2021; "Faith Leaders United," Faith and Elections, November 12, 2020; "Business, Labor and Faith Leaders Call for Patience and Trust in Election Process," U.S. Chamber of Commerce, November 3, 2020); Louis Jacobson and Amy Sherman, "Be patient on election night 2020. Counting the returns will take time.," Poynter Institute, November 1, 2020.

405 "Business, Labor and Faith Leaders Call for Patience and Trust in Election Process," United States Chamber of Commerce, November 3, 2020.

406 Louis Jacobson and Amy Sherman, "Be patient on election night 2020. Counting the returns will take time," Poynter, November 1, 2020.

407 Emily Birnbaum, "Meet the researchers and activists fighting misinformation," Protocol, November 3, 2020.

408 "The Fight Against Disinformation Requires the Right Tools," PEN America, October 27, 2020.

409 Ashley Quarcoo, "Three New Ways Civil Society Is Protecting the U.S. Election," Carnegie Endowment for International Peace, October 28, 2020.

410 Janine Zacharia and Andrew Grotto, "How to Report Responsibly on Hacks and Disinformation: 10 Guidelines and a Template for Every Newsroom," Stanford Cyber Policy Center, accessed March 1, 2021.

411 "Announcing the EIP," Election Integrity Partnership, July 27, 2020.

412 Samantha Bradshaw, et al., "Election Delegitimization: Coming to you Live," Election Integrity Partnership, November 17, 2020.

413 "Election Official Handbook: Preparing for Election Day Misinformation," Election Integrity Partnership, accessed February 16, 2021.

414 Joe Bak-Coleman, et al., "Weaponizing projections as tools of election delegitimization," Election Integrity Partnership, November 3, 2020.

415 Jack Cable and David Thiel, "Analysis of Wednesday's foreign election interference announcement," Election Integrity Partnership, October 23, 2020.

416 Ben Nimmo, "Russian Narratives on Election Fraud," Election Integrity Partnership, November 3, 2020.

417 Sheera Frenkel, "Russian internet trolls are amplifying election fraud claims, researchers say," The New York Times, November 3, 2020.

418 "Researchers Find A Top YouTube Video Of Election Results To Be A Fake," NPR, November 3, 2020.

419 Joseph Marks, "The Cybersecurity 202: Biden campaign hires first top cybersecurity official to protect against digital threats," The Washington Post, July 10, 2020.

420 Ibid.

421 "What We Do," Defending Digital Campaigns, accessed February 11, 2021.

422 Woolbright, 2020; for more information on DDC, see Section II: Private Sector, Cybersecurity and Technology Companies, "Assistance and Training."

423 The FEC's decision to allow free and discounted cybersecurity support to campaigns occurred in July 2019, before the period covered in this appendix.

424 "ISAO," US Cyberdome, accessed February 11, 2021.

425 "Advisory Board," US Cyberdome, accessed February 11, 2021.

426 Reed Richardson, "Iowa Caucus Vote Delays Over 'Quality Control' Baffles Cable News, Ignites Speculation: 'Something Is Clearly Off'," Mediate, February 3, 2020.

427 Ibid.

428 CNN, February 3, 2020,

429 Gilad Edelman, "The Media Just Passed a Test It Failed Four Years Ago," Wired, October 15, 2020.

430 Janine Zacharia and Andrew J. Grotto, "The Media Must Prepare for Another Hack-and-Leak," Lawfare, October 21, 2020.

431 Twitter suspended Sherman's account, while Haberman subsequently deleted the tweet. For more information: Zacharia and Grotto, October 21, 2020.

432 Joe Pompeo, "Connect the Dots: Marty Baron Warns Washington Post Staff About Covering Hacked Materials," Vanity Fair, September 23, 2020.

433 Zacharia and Grotto, October 21, 2020.

434 Lauren Jackson and Desiree Ibekwe, "Covering Political Hacks and Leaks Ahead of the Election," The New York Times, October 25, 2020.

435 Neil MacFarquhar, et al., "Far-Right Group That Trades in Political Violence Gets a Boost," The New York Times, September 30, 2020.

436 Ana Ceballos and Carli Teproff, "Voting intimidation emails to UF students may be scam, authorities say," Miami Herald, October 23, 2020.

437 Tess Owen and Lorenzo Franceschi-Bicchierai, ""Proud Boys' Emails Threatening Florida Voters Appear to Use Spoofed Email Address," Vice, October 20, 2020.

438 Sarah Nelson, "Law enforcement investigates 'Proud Boys' emails," The Gainsville Sun, October 20, 2020.

439 Joel Shannon, et al., "'We will come after you': Voters report personalized emails pressuring them to vote for Donald Trump," USA Today, October 21, 2020.

440 Michael M. Grynbaum, "Networks Pledge Caution for an Election Night Like No Other," The New York

Times, October 31, 2020.

441 Tiffany Hsu, "How the Major Cable Networks Covered Election Night," The New York Times, November 4, 2020.

442 Ibid.

443 Ibid.

444 Stephen Battaglio, "TV news coverage is cautious as election night turns into a weeklong epic," The Los Angeles Times, November 4, 2020; Grynbaum, 2020.

445 Joshua Benton, "So what did the 2020 election really mean, anyway? Here's a first draft of media history, from 100-plus scholars," Nieman Lab, November 16, 2020.

446 Tiffany Hsu and John Koblin, "Fox News Meets Trump's Fraud Claims With Skepticism," The New York Times, November 7, 2020.

447 Shayan Sardarizadeh, "US election 2020: Fox News, Newsmax walk back voter fraud claims after legal threat," BBC, December 22, 2020.

448 Jeremy Barr and Sarah Ellison, "Conservative media has stayed devoted to Trump's bogus claims of victory — but cracks are starting to show," The Washington Post, November 20, 2020.

449 Hsu, 2020.

450 Benton, 2020.

451 Marina Watts, "Fox News Cuts Away From Trump's Press Secretary, Says It Can't Air 'False Claims' in Good Conscience," Newsweek, November 9, 2020.

452 Melinda Haughey, et al., "Media Largely Frames Trump's Victory Declaration as False in Headlines," Election Integrity Project, November 5, 2020.