**TO:** Jonathon Hathaway, Research Program Director
**FROM:** Cole Leis, Research Assistant
**DATE:** July 16, 2025
**RE:** Addressing the Role of Deepfake Technology in Foreign Interference in U.S. Elections

## Executive Summary

Due to significant gaps in artificial intelligence (AI) policy in the U.S., it is too easy for foreign adversaries to use deepfake technology to spread election disinformation and therefore interfere in U.S. elections. The U.S. must act to preserve election integrity, prevent the public's interests from being undermined, and maintain public trust in democratic institutions. To counter foreign adversaries' use of deepfakes to interfere in elections, policymakers should consider transparency and disclosure mandates, prohibitions on certain kinds of deceptive AI content, foreign influence threat report requirements for social media platforms, investment in AI detection capabilities, media literacy promotion through educational initiatives, collaboration with foreign partners, and additional research into foreign adversaries' use of generative AI.

## Foreign Interference in U.S. Elections, Disinformation, and Artificial Intelligence

Foreign interference in U.S. elections has become an increasingly prevalent issue in recent years. Although federal law prohibits foreign nationals from spending in U.S. elections, foreign actors nevertheless spent large amounts on attempts to meddle in U.S. elections in 2016 and 2018, using digital advertising and social media to promote particular candidates and sow discord.[i] Foreign interference has become more substantial in volume over time, with adversarial operations in 2024 exceeding operations in both 2016 and 2020. Interference primarily comes from Russia, China, and Iran. In 2024, Russia spent $10 million to manipulate far-right media in the U.S., and it worked to disrupt the integrity of elections in swing states like Arizona, Georgia, and Pennsylvania through its "Doppelganger" network, through which it distributed staged videos and false stories numbering in the tens of thousands. Meanwhile, China targeted candidates with anti-China sentiments in down-ballot races, employing generative AI and nonexistent American personas across over fifty platforms.[ii] Foreign interference will likely only continue to expand moving forward.

Election interference frequently comes in the form of disinformation, "intentionally false information spread with the purpose of deceiving its recipients."[iii] Disinformation can be differentiated from misinformation, or "false information that is spread without the intention to deceive its recipients."[iv] Growing numbers of social media platforms and websites exacerbate the issue of disinformation, which poses a threat to important U.S. institutions including elections. When foreign adversaries use disinformation to influence electoral outcomes, there is a risk that subsequent action, especially from officials who benefitted from the interference electorally, will contribute to foreign adversaries' interests or undermine the interests of the U.S. and its allies, whether intentionally or unintentionally. When the public is deceived, it may mistakenly act — or pressure policymakers to act — against its own interests in ways that have dangerous implications for health, safety, or even national security.[v]

Disinformation can come in the form of almost any type of communication, with news, doctored photos, and manipulated videos all having the potential to spread disinformation. As technology advances, it has become increasingly cheap, quick, and easy to create seemingly legitimate disinformation. Foreign actors frequently use heavy-handed bots and fake accounts to distribute disinformation, but once regular people in the U.S. have been tricked, the threat starts to come from "within" as people who mistakenly believe the information to be true share it with others. By co-opting recipients of disinformation to further spread false information, foreign adversaries can distribute their disinformation via more credible sources with better networks. This progression from one source to the next amplifies the reach — and danger — of foreign disinformation considerably.[vi]

A large portion of the growth of foreign interference in U.S. elections can be explained by the proliferation of AI, which has vastly expanded adversaries' ability to create and spread disinformation. The advent of AI has magnified concerns surrounding election integrity worldwide, with AI already having transformed the elections of at least 50 countries. Prior to Canada's election in April 2025, an AI-made image depicting prime minister candidate Mark Carney together with the controversial figure Jeffrey Epstein surfaced on X. In Poland, AI-generated social media posts from Russia falsely informed Poles that terrorist activities could result in the cancellation of Poland's May 2025 election. A Russian influence operation involving AI disrupted the first round of voting in Romania's 2024 presidential election to such an extent that another vote had to be held, and in March 2025, an AI-created video purported to show President Donald Trump endorsing a Romanian candidate. As AI grows more sophisticated, AI-generated content becomes harder to distinguish from genuine content, and disinformation becomes harder to differentiate from accurate information.[vii] As a result, deliberative democracy, which typically depends in principle on the idea that "the epistemic function of a deliberative system is to produce preferences, opinions, and decisions that are appropriately informed by facts and logic and are the outcome of substantive and meaningful consideration of relevant reasons," comes under threat, and electoral integrity in particular comes into question.[viii]

AI-made disinformation is especially dangerous for at least two major reasons. First, AI has the ability to test and improve its strategies and tactics far quicker than humans by observing how people react to and engage with content and then adjusting its methods accordingly. Second, AI-created disinformation can be tailored to specific audiences so that it is more convincing. Currently, efforts to personalize AI-designed disinformation are conducted by humans, but AI will eventually gain the ability to analyze people's online presence to determine their psychological traits, which will in turn enable AI to create content that appeals to people's dispositions and preferences, ultimately influencing them in a political setting. Russia, for example, distributed tailored, AI-generated disinformation in the U.S. as the 2024 presidential election approached. China has frequently disseminated AI-made propaganda on social media platforms, sometimes targeting conservatives with posts meant to prompt disaffection with the American government.[ix] As AI becomes better equipped to revise its methods in real time and target specific audiences with its messaging, the threat that AI poses will continue to grow.

The largest social media platforms, such as Facebook, X, TikTok, and YouTube, have policies addressing the misuse of AI, and they have sometimes acted in cases relevant to elections. However, researchers argue that such platforms are controlled by companies with a vested interest

in ensuring that users continue to engage with the platform, and AI misuse often produces content that draws users' attention. Enforcement of companies' AI misuse policies therefore falls short. For example, although Meta requires AI content to be flagged as such on its platforms, little AI content actually had disclaimers placed on it in India's 2024 elections, during which fake videos of deceased politicians emerged. Although TikTok claims that it removed over 7,300 posts that were at odds with its policies in the two weeks prior to the second round of voting in Romania's election, the European Union is currently investigating whether TikTok sufficiently restricted disinformation pertaining to the Romanian election (along with election campaigns in Croatia and Ireland).[x] Though social media platforms' AI misuse policies are perhaps a step in the right direction, the level of actual enforcement apparently leaves much to be desired. This is the case for corporate AI developers as well; while OpenAI prohibits political uses of its tools and employed AI to automatically prevent a quarter-million attempts to create images of American political candidates in 2024, the company's enforcement of its ban on political uses has nonetheless been deemed ineffective.[xi] Since companies have failed to adequately enforce AI misuse policies, government intervention may prove necessary.

**Deepfake Technology**

Deepfake technology is of particular concern when it comes to foreign interference in elections. Though definitions vary, a deepfake is generally considered to be an image, video, or audio recording that is created or altered using AI to depict a person doing or saying something that they did not actually do or say.[xii] Deepfakes are created through deep learning, a form of machine learning whereby a generative adversarial network (GAN), a neural network meant to emulate the way that human brains learn, takes input and learns to generate output comparable to the input from which it learned. Neural networks have series of nodes called hidden layers that use mathematical transformations to translate input signals (i.e., real images, videos, and audio) into output signals (i.e., lifelike fake images, videos, and audio). With more hidden layers, a neural network becomes more sophisticated. Making complex deepfakes involves two algorithms: one that learns to emulate actual media and one that learns to determine whether media is real. By iterating together, the generator and discriminator algorithms both improve to the point where output becomes easily mistakeable for genuine media.[xiii] [xiv]

To generate images or videos, a GAN system views photos or videos showing a target from a variety of angles, and in the case of video generation, the GAN analyzes the target's movement, behavior, and speech patterns.[xv] Three common approaches to deepfake videos include "face swap," "lip sync," and "puppet master." Face swap involves switching out one person's face for another's. Lip sync involves making a person's mouth move in alignment with an audio recording. Finally, puppet master involves replacing a person's entire body with another's.[xvi] When generating audio, meanwhile, the GAN clones input providing the target's voice, builds a model incorporating the target's speech patterns, and uses the model to make the target "speak" as directed. By repeatedly checking its work against the discriminator, a GAN develops increasingly realistic media.[xvii]

Deep learning advancements have made it possible for anyone to create deepfakes quickly and at little cost.[xviii] A range of evolving technologies are necessary for creating deepfakes, including GANs; convolutional neural networks, which help with recognizing faces and tracking movement; autoencoders, which impose the facial expressions and body movements they recognize onto

source videos; natural language processing algorithms, which analyze the traits of a person's speech and then create new audio based on those traits; high-performance computing, which provides the required computing power; and video editing software, which helps with end-product refinement and realism. Common tools for making deepfakes include DeepFaceLab, DeepSwap, and FaceApp, among others.[xix]

Deepfakes have already seen significant use as a tool for spreading disinformation in elections. For instance, a deepfake video of Rep. Rob Wittman circulated prior to Taiwan's January 2024 election, falsely depicting Wittman soliciting votes for a Taiwanese presidential candidate.[xx] In an effort to influence the same election, a Chinese Communist Party-linked group referred to as both Storm-1376 and "Spamouflage" distributed an AI-generated audio recording of one Taiwanese presidential candidate (who had dropped out of the race) endorsing another.[xxi] Content of this sort misleads voters, interrupting democratic processes.

Taiwan is hardly the only country whose elections have been influenced by deepfakes; foreign actors have targeted the U.S. with a variety of deepfakes that bear on elections, political cohesion, and democratic health. In August 2024, a Russian influence network shared articles with deepfaked audio of former president Barack Obama expressing dismay at the failure of the Trump assassination attempt. In AI-written articles, 171 fake local news websites presented the audio clip as genuine. The articles appeared across X, Facebook, LinkedIn, Telegram, and other platforms. In October 2024, a deepfake video spread by a Russian-aligned propaganda network purported to show a former student of vice president candidate Tim Walz accusing Walz of sexual assault.[xxii] Russian-made deepfakes of Vice President Kamala Harris depicted her making inflammatory comments, and Elon Musk was among those who circulated the fake video.[xxiii] Such videos reached tens if not hundreds of thousands of American voters, manipulating them with the intent to make particular electoral outcomes more likely.

It is important to ask, however, whether deepfakes actually impact the results of elections. In the case of the 2024 presidential election in the U.S., experts argue that deepfakes — and AI in general — did not disrupt the electoral process, but misuse of such tools still actively harms public trust in elections and will likely have far greater impacts down the line. Although major AI-assisted attacks on election infrastructure and disinformation campaigns were absent, AI-made deepfakes spreading false information about politically relevant events and candidates have already begun to blur the line between fact and fiction; worsen polarization; and reduce confidence in the institutions crucial to democracy. As AI-created content continues to proliferate and foreign adversaries like China continue to experiment with deepfake technology, these dynamics will have considerable effects on democracy, especially elections.[xxiv] [xxv] Experts note that in particular, bad actors will become better able to exploit the liar's dividend as deepfake technology evolves, leading to lower engagement in democratic processes and an increased vulnerability to manipulation from bad actors located both within the U.S. and abroad.[xxvi]

**Policy History, Challenges, and Options**

Although a number of bills have been introduced in Congress, there is currently no comprehensive federal legislation addressing AI-related issues in the United States. Deepfakes are legal unless they violate laws surrounding issues like hate speech, defamation, or child pornography, leaving

law enforcement with few avenues for action. The Take It Down Act was the first piece of federal legislation directly addressing deepfakes to get signed into law; sponsored by Sen. Ted Cruz and Rep. Maria Elvira Salazar, the bill passed in May 2025. The Take It Down Act criminalized publishing deepfake pornography, and it requires social media platforms to promptly remove such media upon notification. Otherwise, efforts to combat problems involving deepfakes through federal legislation have been unsuccessful; such efforts include the DEFIANCE Act, the DEEPFAKES Accountability Act (which notably addresses foreign interference in elections specifically), and the NO FAKES Act, among others.[xxvii] Failed legislation from the 118th Congress focused on AI use in elections includes the Protected Elections from Deceptive AI Act, the AI Transparency in Elections Act of 2024, the Candidate Voice Fraud Prohibition Act, the Securing Elections From AI Deception Act, and the AI Transparency in Elections Act of 2024.[xxviii]

Since federal efforts to handle deepfakes have been inadequate, states have attempted to mount a patchwork defense against AI's harms. By December 2023, five states had banned deepfakes meant to affect elections, seven states were considering similar legislation, and ten states had banned nonconsensual deepfake pornography.[xxix] By January 2025, eighteen states had passed legislation regulating campaign materials with "manipulated" or "deceptive" media; this trend began in 2019 with Texas. Nevertheless, these laws had led to no prosecutions as of January, indicating a lack of effectiveness.[xxx] By May, forty states had pending legislation related to deepfake use, and by July, twenty-six states had passed bills regulating political deepfake use.[xxxi] [xxxii] As of July, state-level legislation on political deepfakes takes the form of either durational prohibitions (as in the case of Minnesota and Texas) or requirements surrounding disclosure (as in the case of twenty-four other states).[xxxiii] So far, enforcement has primarily fallen to civil courts, but generally, the laws have yet to undergo thorough testing in courts.[xxxiv]

Despite increasing enthusiasm for managing deepfakes among some policymakers, other lawmakers and political actors have sought to contain attempts at policy action. Critics argue that deepfake laws threaten to prevent free speech and stifle American competitiveness, and they say the laws are essentially impotent since they are so challenging to enforce. For these reasons, some Congressional Republicans sought (but ultimately failed) to impose a ten-year moratorium on state-level AI regulation as part of the One Big Beautiful Bill Act in mid-2025. Moreover, January 2025 executive orders such as "Restoring Freedom of Speech and Ending Federal Censorship" and "Removing Barriers to American Leadership in Artificial Intelligence" aimed to remove and prevent government-imposed hurdles on AI that may hinder free speech and AI innovation. The goal of the executive orders is evidently to stifle policymakers' efforts to interfere in the affairs of American AI companies and social media platforms, but impairing policymakers' ability to combat AI issues comes with its own risks. Outside of government, conservatives have raised legal challenges against state laws that address AI use in elections in states like California, further handicapping efforts to resolve problems with political deepfakes through policy.[xxxv]

Along with AI policy, election disinformation policy is also relevant to countering foreign adversaries' use of deepfakes to interfere in U.S. elections. Both federal law and laws in almost every state ban voter intimidation, and many of these laws have historically been interpreted as banning certain forms of election disinformation. A number of states have also banned particular kinds of false election-related speech, including false statements about how to vote and who is qualified to do so.[xxxvi] Some state laws explicitly ban false statements about candidates (as in the

case of sixteen states as of late 2022) and ballot measures (as in the case of fourteen states as of late 2022), but courts have debated such laws' constitutionality intensely, with multiple federal appellate courts striking these laws down in recent years.[xxxvii] [xxxviii] Together with these laws, campaign finance disclosure laws, communications laws, consumer protection laws, media literacy laws, and privacy laws all may be helpful to policymakers when attempting to address AI-made election disinformation.[xxxix]

Outside of the legislative arena, federal entities that work to combat foreign disinformation include the Departments of State (State), Homeland Security (DHS), and Defense (DOD). These three departments monitor public and nonpublic information sources, detecting disinformation via a range of methods. State and DHS's Office of Intelligence and Analysis watch social media, and all three departments identify, publicize, and research disinformation threats while educating policymakers, the public, and allies on these threats. State's Global Engagement Center assists agencies, embassies, and foreign partners in developing tools to combat foreign disinformation abroad. DHS's Cybersecurity and Infrastructure Security Agency teaches citizens about disinformation's risks, and it works with election officials at the local and state levels to distribute educational materials on recognizing disinformation. Finally, DOD's Public Affairs office makes press releases, social media posts, and statements available to counter disinformation with genuine information. [xl] Policymakers can draw on agencies' existing efforts to combat foreign disinformation when seeking to better protect election integrity.

Aside from legal and political opposition to prior AI policy, challenges in crafting and passing future policy addressing political AI use include avoiding First Amendment lawsuits, defining AI properly, determining the circumstances under which legal restrictions should be triggered, and developing procedures for establishing liability.[xli] Difficulty also comes from the fast pace of AI development, which can overwhelm government officials, as well as the task of figuring out what to target with regulation and what to leave untouched.[xlii]

Policymakers have a wealth of options for countering foreign adversaries' use of deepfakes in election interference, each with their own advantages and disadvantages. To protect election integrity, policymakers should consider possibilities ranging from transparency mandates to voter education campaigns.[xliii] Multiple attempts have been made in Congress to establish a new federal agency for AI-related issues, and policymakers still may wish to pursue this route. Although various AI and social media moguls like Sam Altman, Brad Smith, and Mark Zuckerberg once expressed support for the creation of a federal digital regulator, support has since seemingly dwindled. A new agency could create a new licensing structure, adopt a risk-based approach to regulation that prioritizes private-sector innovation, and delegate code development in a standards-like process.[xliv] Such an agency would be able to tackle deepfake regulation head-on, helping to protect against election interference from foreign actors. However, a lack of support makes this option infeasible at the present.

Policymakers might instead mandate that social media platforms either mark AI content as such or require users to label their own AI content appropriately, increasing transparency through technologies like watermarking and blockchain.[xlv] This option would build on the growing trend of disclosure laws that has reached some states but not others. Although bans on certain kinds of deceptive AI content are harder to establish than transparency rules, they should nevertheless also

receive consideration.[xlvi] Alternatively, policymakers could require platforms to regularly publish threat reports or to inform the appropriate government entities when they learn that foreign actors are targeting them.[xlvii] Notifying citizens and public officials of disinformation threats sooner could help to both minimize the negative impact and facilitate a quicker response from government. Additionally, policymakers might invest in AI detection capabilities, working together with the private sector. Improved detection capabilities may be useful in preventing the public from mistaking political deepfakes for genuine media depicting political figures. Policymakers can also protect the public through promoting media literacy, which may involve creating or bolstering educational initiatives that make citizens more resilient to election disinformation from foreign actors. Collaborating with agencies that already do this work, including State, DHS, and DOD, may be beneficial. Collaboration might also be a useful approach for policymakers to consider in the context of partners like Taiwan; this option would entail encouraging increased information-sharing regarding disinformation threats and best practices for threat mitigation. The U.S. and its partners would be better equipped to counter foreign efforts to interfere in elections if they were to work together more closely. Finally, policymakers themselves might value from funding additional research into how foreign adversaries use generative AI to exert influence. Greater knowledge on this topic may inform future policymaking.[xlviii]

[i] Campaign Legal Center. "Combatting Foreign Interference." Campaign Legal Center. Accessed July 16, 2025. https://campaignlegal.org/democracyu/transparency/combatting-foreign-interference.

[ii] Atlantic Council. "What to Know about Foreign Meddling in the US Election." *Atlantic Council*, November 5, 2024. https://www.atlanticcouncil.org/content-series/fastthinking/what-to-know-about-foreign-meddling-in-the-us-election/.

[iii] American Security Project. "Disinformation." *American Security Project*, n.d. Accessed July 16, 2025. https://www.americansecurityproject.org/public-diplomacy-and-strategic-communication/disinformation/.

[iv] Ibid.

[v] Ibid.

[vi] Ibid.

[vii] Myers, Steven Lee, and Stuart A. Thompson. "A.I. Is Starting to Wear Down Democracy." Technology. *The New York Times*, June 26, 2025. https://www.nytimes.com/2025/06/26/technology/ai-elections-democracy.html.

[viii] Goldstein, Josh A., and Andrew Lohn. "Deepfakes, Elections, and Shrinking the Liar's Dividend." Brennan Center for Justice, January 23, 2024. https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend.

[ix] Wilbur, Douglas. "The Challenge of AI-Enhanced Cognitive Warfare: A Call to Arms for a Cognitive Defense." *Small Wars Journal*, January 22, 2025. https://smallwarsjournal.com/2025/01/22/the-challenge-of-ai-enhanced-cognitive-warfare-a-call-to-arms-for-a-cognitive-defense/.

[x] Myers, Steven Lee, and Stuart A. Thompson. "A.I. Is Starting to Wear Down Democracy." Technology. *The New York Times*, June 26, 2025. https://www.nytimes.com/2025/06/26/technology/ai-elections-democracy.html.

[xi] Schneier, Bruce, and Nathan Sanders. "The Apocalypse That Wasn't: AI Was Everywhere in 2024's Elections, but Deepfakes and Misinformation Were Only Part of the Picture." *Harvard Kennedy School: Ash Center for Democratic Governance and Innovation*, December 4, 2024. https://ash.harvard.edu/articles/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture/.

[xii] Hsu, Tiffany, Steven Lee Myers, and Sheera Frenkel. "How Russia, China and Iran Are Interfering in the Presidential Election." Technology. *The New York Times*, October 29, 2024. https://www.nytimes.com/2024/10/29/technology/election-interference-russia-china-iran.html.

[xiii] UVA Information Security. "What the Heck Is a Deepfake?" University of Virginia. Accessed July 16, 2025. https://security.virginia.edu/deepfakes.

[xiv] Yasar, Kinza, Nick Barney, and Ivy Wigmore. "What Is Deepfake Technology?" TechTarget, May 22, 2025. https://www.techtarget.com/whatis/definition/deepfake.

[xv] Ibid.

[xvi] Goldstein, Josh A., and Andrew Lohn. "Deepfakes, Elections, and Shrinking the Liar's Dividend." Brennan Center for Justice, January 23, 2024. https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend.

[xvii] Yasar, Kinza, Nick Barney, and Ivy Wigmore. "What Is Deepfake Technology?" TechTarget, May 22, 2025. https://www.techtarget.com/whatis/definition/deepfake.

[xviii] Goldstein, Josh A., and Andrew Lohn. "Deepfakes, Elections, and Shrinking the Liar's Dividend." Brennan Center for Justice, January 23, 2024. https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend.

[xix] Yasar, Kinza, Nick Barney, and Ivy Wigmore. "What Is Deepfake Technology?" TechTarget, May 22, 2025. https://www.techtarget.com/whatis/definition/deepfake.

[xx] Hsu, Tiffany, Steven Lee Myers, and Sheera Frenkel. "How Russia, China and Iran Are Interfering in the Presidential Election." Technology. *The New York Times*, October 29, 2024. https://www.nytimes.com/2024/10/29/technology/election-interference-russia-china-iran.html.

[xxi] Ewe, Koh. "China Is Using AI to Sow Disinformation and Stoke Discord Across Asia and the U.S., Microsoft Reports." TIME, April 5, 2024. https://time.com/6963787/china-influence-operations-artificial-intelligence-cyber-threats-microsoft/.

[xxii] Elliott, Vittoria. "The WIRED AI Elections Project." Tags. *WIRED*, May 30, 2024. https://www.wired.com/story/generative-ai-global-elections/.

[xxiii] Hasan, Shanze, and Abdiaziz Ahmed. "Gauging the AI Threat to Free and Fair Elections." Brennan Center for Justice, May 6, 2025. https://www.brennancenter.org/our-work/analysis-opinion/gauging-ai-threat-free-and-fair-elections.

[xxiv] Ibid.

[xxv] Ewe, Koh. "China Is Using AI to Sow Disinformation and Stoke Discord Across Asia and the U.S., Microsoft Reports." TIME, April 5, 2024. https://time.com/6963787/china-influence-operations-artificial-intelligence-cyber-threats-microsoft/.

[xxvi] Hasan, Shanze, and Abdiaziz Ahmed. "Gauging the AI Threat to Free and Fair Elections." Brennan Center for Justice, May 6, 2025. https://www.brennancenter.org/our-work/analysis-opinion/gauging-ai-threat-free-and-fair-elections.

[xxvii] Yasar, Kinza, Nick Barney, and Ivy Wigmore. "What Is Deepfake Technology?" TechTarget, May 22, 2025. https://www.techtarget.com/whatis/definition/deepfake.

[xxviii] Hooshidary, Sanam, and Adam Kuckuk. "AI in Elections: A Look at the Federal and State Legislative Landscape." NCSL, September 12, 2024. https://www.ncsl.org/elections-and-campaigns/ai-in-elections-a-look-at-the-federal-and-state-legislative-landscape#state-actions.

[xxix] Yasar, Kinza, Nick Barney, and Ivy Wigmore. "What Is Deepfake Technology?" TechTarget, May 22, 2025. https://www.techtarget.com/whatis/definition/deepfake.

[xxx] Larkin, C. J. "Regulating Election Deepfakes: A Comparison of State Laws." Tech Policy Press, January 8, 2025. https://techpolicy.press/regulating-election-deepfakes-a-comparison-of-state-laws.

[xxxi] Yasar, Kinza, Nick Barney, and Ivy Wigmore. "What Is Deepfake Technology?" TechTarget, May 22, 2025. https://www.techtarget.com/whatis/definition/deepfake.

[xxxii] NCSL. "Artificial Intelligence (AI) in Elections and Campaigns." NCSL, July 9, 2025. https://www.ncsl.org/elections-and-campaigns/artificial-intelligence-ai-in-elections-and-campaigns.

[xxxiii] Ibid.

[xxxiv] Hooshidary, Sanam, and Adam Kuckuk. "AI in Elections: A Look at the Federal and State Legislative Landscape." NCSL, September 12, 2024. https://www.ncsl.org/elections-and-campaigns/ai-in-elections-a-look-at-the-federal-and-state-legislative-landscape#state-actions.

[xxxv] Hsu, Tiffany. "Deepfake Laws Bring Prosecution and Penalties, but Also Pushback." Business. *The New York Times*, May 22, 2025. https://www.nytimes.com/2025/05/22/business/media/deepfakes-laws-free-speech.html.

[xxxvi] Common Cause. "As a Matter of Fact: The Harms Caused by Election Disinformation Report." *Common Cause*, October 28, 2021. https://www.commoncause.org/resources/as-a-matter-of-fact-the-harms-caused-by-election-disinformation-report/.

[xxxvii] Ardia, David. "First Amendment Limits on State Laws Targeting Election Misinformation, Part IV." Politics. *Reason.Com*, September 22, 2022. https://reason.com/volokh/2022/09/22/first-amendment-limits-on-state-laws-targeting-election-misinformation-part-iv/.

[xxxviii] Common Cause. "As a Matter of Fact: The Harms Caused by Election Disinformation Report." *Common Cause*, October 28, 2021. https://www.commoncause.org/resources/as-a-matter-of-fact-the-harms-caused-by-election-disinformation-report/.

[xxxix] Ibid.

[xl] U.S. Government Accountability Office. "Foreign Disinformation: Defining and Detecting Threats." GAO.Gov, September 26, 2024. https://www.gao.gov/products/gao-24-107600.

[xli] Kuckuk, Adam. "Challenges Ahead for Lawmakers Seeking to Legislate AI in Campaigns." NCSL, January 3, 2024. https://www.ncsl.org/state-legislatures-news/details/challenges-ahead-for-lawmakers-seeking-to-legislate-ai-in-campaigns.

[xlii] Wheeler, Tom. "The Three Challenges of AI Regulation." *The Brookings Institution*, June 15, 2023. https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/.

[xliii] Hasan, Shanze, and Abdiaziz Ahmed. "Gauging the AI Threat to Free and Fair Elections." Brennan Center for Justice, May 6, 2025. https://www.brennancenter.org/our-work/analysis-opinion/gauging-ai-threat-free-and-fair-elections.

[xliv] Wheeler, Tom. "The Three Challenges of AI Regulation." *The Brookings Institution*, June 15, 2023. https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/.

[xlv] Beauchamp-Mustafaga, Nathan. *Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations: Chinese Military Strategies, Capabilities, and Intent*. RAND, 2024. https://www.rand.org/pubs/testimonies/CTA3191-1.html.

[xlvi] Weiner, Daniel I., and Lawrence Norden. "Regulating AI Deepfakes and Synthetic Media in the Political Arena." Brennan Center for Justice, December 5, 2023. https://www.brennancenter.org/our-work/research-reports/regulating-ai-deepfakes-and-synthetic-media-political-arena.

[xlvii] Thibaut, Kenton. "Effective US Government Strategies to Address China's Information Influence." *Atlantic Council*, July 30, 2024. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/effective-us-government-strategies-to-address-chinas-information-influence/.

[xlviii] Beauchamp-Mustafaga, Nathan. *Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations: Chinese Military Strategies, Capabilities, and Intent*. RAND, 2024. https://www.rand.org/pubs/testimonies/CTA3191-1.html.