SAFEGUARDING DEMOCRACY IN ELECTIONS: ANALYZING STATE PREPAREDNESS AGAINST DELIBERATE EFFORTS TO UNDERMINE U.S. ELECTION ADMINISTRATION

by
Honor Bea Durham

Senior Honors Thesis
Presented to the Faculty of the Department of Political Science
University of Wisconsin-Madison
May 2025

Professor Barry C. Burden
Lyons Family Professor: American Politics | Political Methodology

Dr. Amy Gangl
Director of Undergraduate Studies, Political Science

Table of Contents

Introduction

"Democratic backsliding today begins at the ballot box." —*Levitsky and Ziblatt*

The inspiration for this thesis comes from the book *How Democracies Die* by political scientists Steven Levitsky and Daniel Ziblatt. Written in 2018, Levitsky and Ziblatt argue that the United States is experiencing *democratic backsliding*, which refers to a slow, long-term erosion of democracy through the weakening of various political institutions and norms. The implications of this political phenomenon extend to many parts of American government, and the weakening of norms, including institutional forbearance and the mutual toleration of political opponents, makes for more contentious and disharmonious politics.[1] Democratic backsliding results in the internal erosion of democratic practices in various levels of politics and a simultaneous shift toward authoritarian norms. Together, this can include attacking those who share different political opinions, disregarding judicial decisions, and interfering in elections that are meant to be free and fair. The latter consequence—election interference—is the focal point of this thesis. As politics becomes more competitive, it is important to protect election administration to ensure that American elections remain free and fair. Polarization in the electorate and persistently hostile rhetoric between the two major parties have made elections more contentious, increasing the perceived stakes of losing key political offices to both politicians and partisans. Some of those consequences emerged during the 2020 presidential election with unfounded electoral fraud claims and the January 6th insurrection. In a time when threats to democracy have become normalized, it is important to assess whether the American electoral system is equipped to face the dangers that could subvert the democratic process of any election.

[1] Levitsky and Ziblatt, 2018

In their article called "The Miracle and Tragedy of the 2020 U.S. Election," Persily and Stewart argue that the 2020 election was both a miracle and a tragedy because election administrators were barely able to pull off a successful election as they faced the unique challenges of the COVID-19 pandemic as well as claims about electoral fraud; both cast severe doubt among voters regarding the integrity of the electoral process.[2] This article illustrates the fragility of American elections, especially as more people distrust how elections are administered. Did the electoral system get lucky in 2020, and is it adequately prepared to face a variety of threats that may purposefully accelerate democratic backsliding and the weakening of democratic guardrails in the future? The answer to those questions remains to be seen, and these concerns will become more important if more voters start to doubt election outcomes and practices.

Time is of the essence to protect our electoral system. We have already seen attempts to thwart our political system after the 2020 election and during the 2021 insurrection, so now is the time to ensure that each state's election administration system is ready to handle a variety of threats that may interfere in the electoral process. Because states run their own elections, it is imperative to assess whether they are each independently capable of protecting themselves against a variety of attempts to interfere in their administration. As trust in elections wanes and threats grow increasingly severe, this question must be answered quickly to identify weaknesses and patterns in preparedness across all 50 states. In my senior thesis, I explore how current election laws and general practices prepare the United States to resist threats to the electoral process and democracy itself. Since the states have considerable autonomy in election administration, I focus on how states are similar in their preparedness levels and which states are the most and least prepared.

---

[2] Persily and Stewart III, 2021

Review of Threats and Relevant Literature

General Overview

Election administration can be disrupted by many intentional actions, or "threats." These threats range in scope and severity, from a few missing paper ballots to the assassination of a candidate. Because the word "threat" is broad and can take on many meanings, the term will have a specific definition in the context of this paper.

Threat: **An intentional, human-made action taken to deliberately interfere with the process of running free and fair democratic elections.**

There are a few aspects of this definition that are important to focus on. First, the threat must be done purposefully and originate from a human action. This means that events such as natural disasters, power outages, and pandemics will not be considered in this paper. While such emergencies have the potential to disrupt the way an election is carried out, threats must deliberately attempt to alter the course of the process. This second part of the definition must be highlighted. Threats are the intentional attempts to interfere with election administration. This can include attempts to deceive voters about where to vote, intimidation of election officials, or even widespread, baseless claims about voter fraud that could lead to delays in the certification process. This specification means that factors including disinformation about a political candidate and/or an assassination attempt will not be considered here because these actions are not necessarily taken to directly interfere with an election being carried out. They have the power to influence vote choice but will not subvert the process itself. These are important concepts to keep in mind as the selected threats to future U.S. elections are discussed.

In this paper, the following threats will be considered:

1. Election officials refusing to certify election results
2. Disinformation about the electoral process (two categories: disinformation about election administration/how the voting process is carried out and disinformation about election fraud/"stolen elections")
3. Voter intimidation
4. Intimidation of election officials and poll workers
5. Foreign interference that attempts to sway vote choice and count
6. Candidates refusing to concede elections
7. Cybersecurity and hacking concerns

These are not the only circumstances that would result in election interference, but they are the most relevant to democratic backsliding and appear most often in the current discussion on this subject. These threats clearly undermine elections from being considered free and fair, and they are intentional actions whose perpetrators seek to interfere with how elections are administered. There is also considerable overlap between certain, if not all, threats. For example, foreign interference could involve another country distributing misleading information on social media about the voter registration process. Each section of this review will focus on an individual threat and its history in American elections.

Officials Refusing to Certify Elections

The idea of election officials refusing to certify election results might have seemed unthinkable before 2020, but now it is a legitimate concern for future elections. Trust in the electoral system is at a concerningly low point for Republicans and Republican-leaning Americans. According to the Pew Research Center, only 11% of this group say that they trust the

federal government almost always or most of the time.[3] This disconnect has consequences at many levels of American politics. Still, one of the more significant outcomes is that election officials may choose not to certify election results due to their lack of faith in how elections are run. Widespread concerns about election certification did not exist before 2020. The process was seen as a ceremonial affirmation of the election results and was free of widespread controversy. The politicization of this post-election ritual and the widespread doubts about election administration have normalized concerns from election officials refusing to certify the results of American elections. To understand what happened in the attempts to delay certification in 2020 and 2022, it is important to comprehend how the process works as a whole for national elections.

The certification procedure begins on Election Day, when election officials and poll workers start to organize and count all electronically read votes.Vote totals include all votes cast in person and all mailed ballots cast before, during, or after Election Day. Once this electronic tabulation is completed, the first step of certification can begin. This period is known as the "canvass" when local election officials verify all electronically read vote tallies and add ballots that could not be included in the electronic count (including provisional ballots). The next step is to "certify" the results by confirming that the review of the vote counts is finished and accurate to the best of the officials' ability. The certification process ends here for local races, but there are a few additional steps for both state and national races. Local officials pass the results to officials who then run an independent, statewide canvass, review the results from each local jurisdiction, and formally certify the winners.[4] After this canvass, the certification procedure is over.

[3] Bell, 2024
[4] Miller Karalunas, 2024

An important concept to clarify is that it is not the role of election officials to investigate voter fraud complaints or even to refuse to certify the results. Certification duty is meant to be mostly ceremonial and straightforward, and there is a specific time frame within which the process must be completed.[5] Challenges to the election results relating to fraud or similar concerns are left to particular state-designated processes that will investigate, so the election certification process is not meant to be a forum for looking into the validity of fraud claims.[6] Many voters are unaware of this distinction, which can distort how Americans see the certification process and the role of the election officials in charge of certification.

The trend of election officials refusing to certify election results has grown more common during the 2020s despite these officials lacking the power to truly investigate voter fraud claims. A well-known example of this occurred during the 2020 election in Wayne County, Mich. Two Republican members of the Wayne County certification board decided not to certify the election due to "unexplained discrepancies in precincts between the recorded number of persons who cast ballots and the number of ballots counted."[7] This meant that the board was in a 2–2 deadlock and could not certify the election results. These so-called discrepancies mostly amounted to three or fewer votes, yet the officials were praised by the Michigan Chair of the Republican Party and former President Trump. Later that evening, the two members who refused to certify the results finally joined the Democratic members of the board to complete the certification.[8] This new phenomenon continued during the 2022 midterm elections, as some local officials in New Mexico, Nevada, Arizona, North Carolina, and Pennsylvania voted against certifying results. While all results were eventually certified, the ability of local election officials to disrupt state

[5] National Conference of State Legislatures, 2025
[6] Miller Karalunas, 2024
[7] McDonald, 2022
[8] ibid

and national elections has concerning implications for the future of this procedure. Moreover, it can inflame existing false claims about election fraud and election denialism because these officials are seen as experts in administering elections.[9] The consequences of certification upheaval are not seen in each state just yet, but certification disruptions have been happening more often. It also affects Americans in every state because it can amplify concerns about the security of elections in the U.S.

In response to what happened in Wayne County, Mich., voters were able to amend their state constitution to explicitly outline that election officials are obligated to certify election results, and that this role is non-discretional.[10] More states should consider enacting similar legislation to combat this threat to the electoral process and to implement legal consequences for those who refuse to do their ministerial duty in certifying an election's results.

Candidates Refusing to Concede Elections

The threat of candidates refusing to concede elections in the U.S. is another very recent threat, and it appears to be a new political strategy for primarily the Republican Party. It is a danger to election administration because it undermines public confidence in the electoral process and can interfere with the peaceful transfer of power. As American partisan politics becomes more contentious, cooperation between winning and losing candidates is essential to preserve trust in elections and the political system more broadly.

Candidates refusing to concede elections is the most contested threat in this paper. However, this phenomenon must be considered a threat to the American electoral system. Even though refusing to concede has not changed an election outcome as of 2025 and the peaceful transition of power has been protected throughout American history, breaking the norm of

[9] Bock Clark, 2023
[10] Miller Karalunas, 2024

accepting election results can cultivate widespread distrust in the electoral system and contribute to false narratives about stolen elections. If fewer people have faith in election administration, election results become that much easier to discredit in the future. This threat could also disrupt the certification process and potentially result in delays if a high-profile candidate refuses to concede. As doing so becomes an increasingly popular political strategy to incite unrest over elections, it is an important phenomenon to keep an eye on. One of the conditions for a politician to be considered a loyal democrat—small "d," as in, a politician who prioritizes maintaining democracy—is that they must accept election outcomes even if they lose.[11] If we want to protect American democracy, we will see the refusal to concede as fundamentally dangerous to election administration, and treat those who engage in this without sufficient evidence of fraud as seditionists who are attempting to undermine democracy's guardrails.

Donald Trump's refusal to concede the 2020 election, followed by the subsequent insurrection attempt by his loyalists on January 6th, 2021, is the most well known and serious example of a candidate not accepting election results in American history. His refusal to concede inspired widespread distrust of elections, the "Stop the Steal" campaign, and false voter fraud claims. His campaign took it a step further with its legal strategy to overturn the election outcome. They tried to reverse the result with recounts, lawsuits, and attempts to block individual states' certifications of election results in a strategy known as the "Kraken." The Kraken was unable to convince a single judge to rule in their favor because there was no evidence of widespread fraud that fueled Biden's victory.[12] Another part of the Trump campaign's strategy was to pressure officials to prevent the certification. There were many targets for this, including canvassing boards, election officials, Republican-controlled state

[11] Levitsky and Ziblatt, 2023
[12] McDonald, 2022

legislatures, and Congress. In general, they wanted to convince Republican decision-makers to make decisions to overturn the results. Trump also focused on state officials and legislatures, and tried to persuade some of them to reverse election outcomes by switching out the electors with ones that might vote for him. He tried this in Arizona, Michigan, Pennsylvania, and Georgia without success.[13] His refusal to accept defeat led to his supporters believing that he was the true winner of the election, despite no evidence for it at all; this lie is ongoing because Trump has still not conceded the 2020 election.

The legal and political strategies that Trump pursued after refusing to concede was harmful to American democracy itself. The events of January 6th escalated his refusal to concede into a serious threat against the electoral system and endangered the entire political system. As armed protesters infiltrated the United States Capitol, Trump and Guiliani made calls to see if they could use the violence as an excuse to delay the count.[14] Instead of immediately calling in the National Guard to protect members of Congress, Trump still held onto his lie that he won the election and tried to advance it further by using the insurrection to stop votes from being counted. Never before has a refusal to concede gone this far in American politics.

The 2020 election illustrated the dangers of refusing to concede elections because of how quickly it fired up a violent mob and threatened the lives of American politicians. Doing so is a threat to elections because it is a direct threat to democracy. The unwritten rules of politics, including publicly conceding to winning opponents, may seem trivial to some, since falsely claiming a win is not inherently breaking the law. Even so, accepting a loss protects the institutions that make the American government democratic.[15] Trump's refusal to concede did not stop Joe Biden from becoming president, but the violence and destruction of January 6th

[13] ibid
[14] ibid
[15] Levitsky and Ziblatt, 2018

demonstrated the consequences of this lie. Unfortunately, he is not the only politician who has refused to concede in recent years.

Refusing to concede elections has become more popular over the past 10 years. In 2017, Alabama judge Roy Moore refused to concede the U.S Senate election in Alabama. He lost to Democrat Doug Jones after facing sexual assault allegations during his campaign. In a video released after his loss, he did not admit his defeat and he warned that "The heart and soul of our country is at stake."[16] In 2019, Republican Governor Matt Bevin refused to concede the Kentucky gubernatorial election to his opponent, Democrat Andy Beshear, even after 100% of precincts reported the results.[17] This trend is not entirely unique to Republicans. Democrat Stacey Abrams refused to concede to Republican Brian Kemp during the 2018 Georgia gubernatorial election because of Kemp's alleged role in voter suppression.[18] Even though she acknowledged that Kemp was the winner and did not question the integrity of the election results, she still violated a democratic norm by refusing to concede to her opponent, no matter what the reason for doing so was.

The seriousness of this threat has gotten worse since Trump's refusal to concede because candidates who engage in this behavior have consistently been basing it on false voter fraud claims, mirroring Trump's big lie. In 2020, Republican candidate Loren Culp lost the Washington gubernatorial race and promoted voter fraud claims with mail-in ballots as the reason for his loss. He lost by more than 545,000 votes.[19] One of the more notorious cases of this in recent years is Kari Lake, the losing Republican candidate for Arizona governor in 2022 and in the 2024 U.S. Senate election in Arizona. In 2022, she refused to concede to Democrat Katie

[16] Holpuch, 2017
[17] Schreiner, 2019
[18] Hurt, 2020
[19] Brunner, 2020

Hobbs and inaccurately claimed that significant voter disenfranchisement happened in Maricopa County. Local election officials stated that all of the ballots in the county were counted and there were no problems with long lines, countering Lake's claims.[20] A judge also rejected Lake's request to examine the signed ballot envelopes from early votes. She had two other losing lawsuits that attempted to challenge the results of her election.[21] In 2024, she lost to Democratic Rep. Ruben Gallego. She made a video thanking her supporters but did not explicitly concede. Her campaign also said it was "hard to believe" that she lost to Gallego.[22] Another 2024 example is Eric Hovde, who lost to Democratic incumbent Tammy Baldwin in the U.S. Senate race in Wisconsin. A week after his loss, he posted a video that questioned Milwaukee's results being tallied at 4 a.m., despite this being a typical practice for national elections in Milwaukee. Similarly to Abrams in 2018, Hovde acknowledged his loss but did not concede to his opponent for two weeks after the election.[23, 24] Unfortunately, this trend is becoming more routine in politics despite the harmful implications it has for American democracy.

Disinformation about the Electoral Process

Disinformation, which is false information that is intentionally used to deceive others, can serve many purposes in politics. The spread of purposefully misleading "facts" about political leaders, activities, or institutions can have severe consequences on public knowledge of American politics. These repercussions certainly affect elections, and the scope of this threat is substantial. To that end, this paper will look at a very specific type of disinformation, which is disinformation about the electoral process itself. This may seem like a disregard for the impacts of disinformation on vote choice or trust in elections, but this scope is justified when

[20] Cooper, 2022
[21] Tang, 2023
[22] Marley, 2024
[23] ibid
[24] Bauer, 2024

reconsidering the definition of a "threat" in this paper. Misleading information about a politician running for office does not interfere with the process of administering a free and fair election. It can impact a voter's opinion, but it will not make an election illegitimate or undemocratic. However, disinformation about voting can be considered an example of undermining the electoral process. If someone purposefully shared incorrect information about a particular polling place closing early, they would be intentionally contributing to voter suppression and trying to unfairly alter the result by tricking some voters into not casting a ballot. This fits into the previously outlined definition of what constitutes a "threat."

But what about the spread of unintentional disinformation? There is no such thing. Disinformation is different from misinformation because misinformation is simply incorrect information that is spread without the intention to mislead. Disinformation is deliberate and can be considered to be a misstatement of information that is shared with intent.[25] If someone unknowingly shares incorrect information about their state's voter registration requirements, that can be classified as an accidental spread of misinformation. If the same person was aware that the information about registration requirements was incorrect, and then knowingly shared it online to an audience full of people who lived in that state, that person would be disseminating misinformation that could impact the electoral process.

Understanding the distinction between misinformation and disinformation is crucial in order to grasp the scope and implications of this threat. The unintentional spreading of misinformation still poses a significant issue to election administration, but it does not fit the definition of a "threat" as described above. The deliberate nature of disinformation is precisely why it will be focused on in this paper. The inspiration for this study of electoral threats came from concerns about democratic backsliding in the U.S., so this paper is focused more on

[25] American Psychological Association, 2022

intentional threats rather than unintentional ones. So, while intentional misinformation about elections is still extremely important, it will not be focused on in this work.

Disinformation about the electoral process can be split into two categories. The first relates to some of the examples described earlier in this section. It concerns disinformation about election administration itself and voting. This category focuses on any misleading information about where voting takes place, what voters need to bring to the polling place, how polling places are run, or any other information about the voting process and how it is carried out. The main concern about this type of disinformation is that it will affect voters' ability to cast their ballot or create unnecessary uncertainty about how votes are counted. This category primarily focuses on the spread of incorrect information about how elections are run. Therefore, it is relatively easy to disprove. The second category of disinformation is more complicated because it focuses on electoral fraud and "rigged" elections. While this category also leads to confusion about election administration, it additionally casts doubt on the integrity of the electoral process.

Category I: Disinformation about Election Administration and Voting

Disinformation about elections and voting administration can happen through the use of various strategies, and this issue can be used as evidence that Americans do not currently have a comprehensive understanding of how elections are administered. Artificial intelligence (AI) and social media are the most likely culprits for the spread of this kind of disinformation. Scammers have been using digital tools to target potential voters to share and help spread incorrect information about elections and voting. Some of these scams include fake links claiming to help with voter registration, false claims about needing to pay to register to vote, and AI deepfakes.[26] Such malevolent forces are making it more difficult than ever to discern facts from false information, and easier for disinformation campaigns to take hold. They have, and will continue,

[26] Pistone et al., 2024

to impact Americans' understanding of elections, especially future elections. The election administration system is already complicated in the U.S. because each state has its own process, and it is a decentralized system with many different rules. A typical American might vote and generally follow election news but likely will not know much about voter registration or voter identification requirements in other states.[27] So, it is easy to spread disinformation about the complexities of the election administration process, because it is difficult for the average voter to keep up with details about how elections are run. This poses an important yet tough question: How can election administration disinformation be combatted if most people being targeted by these campaigns lack a baseline understanding of how the process works? Encouraging voter education is crucial because voters must understand how elections are run to recognize disinformation attempts. Challenging the disinformation itself is also important and is becoming more difficult. Social media companies, especially X (formerly Twitter), have not been combating false information about elections as rigorously as these platforms did during the 2020 presidential election and before and after January 6th.[28] This will make it more difficult to disprove false information shared on these sites about voting and election administration, as well as claims about election fraud and "rigged" elections, which presents a considerable challenge.

Category II: Disinformation about election/voter fraud and "stolen" elections

False voter and election fraud claims are nothing new in American politics, but they are more widespread and have the potential to incite chaos during close elections. First and foremost, voter fraud is a rare phenomenon and is not a concerning threat to election administration.[29] "Voter fraud politics" refers to politicians who use voter fraud allegations as a scare tactic to

[27] Jones, 2016
[28] Fung, 2024
[29] Minete, 2010

convince the public that more restrictions on voting are needed for election administration.[30] It is a political tool used to stir up unrest instead of speaking to practical concerns that must be imminently addressed. Such claims have been amplified in the 21st century and reached a new level after the 2020 election. Before January 6th, 2021, it was unprecedented that widespread claims of election fraud led to outright political violence in the U.S.[31] Disinformation about "stolen" elections is extremely inflammatory and can interfere with the process of safe and secure elections if it leads to events like the January 6th insurrection.

There were a few cases of disinformation on social media during the 2020 election that contributed to fraud concerns, including the "ballot dumping" incident in Sonoma County, Calif. This was the widespread claim that thousands of mail-in ballots were found in a landfill dumpster in Sonoma County in September 2020. It was originally spread by a conservative influencer, Elijah Schaffer, who posted a photo of the alleged ballots in the dumpster, and the rumor spread through retweets of Schaffer's original tweet. Even though this alleged ballot dumping was impossible because ballots had not been sent out in California and were not supposed to be until October, Schaffer never admitted the claim was false and instead only vaguely implied that his original information was incorrect. He did not try to correct any misconceptions that an X user would have derived from that tweet, not even after it was discovered that the photo in question was one of ballots that had been counted years prior for a 2018 election.[32] Because the post was left uncorrected by its creator, it only follows that many people online who had seen it may not have understood that the photo was used out of context.

Another incident was "SharpieGate," which was the allegation that the Sharpie pens given to Arizona voters to fill out their ballots damaged them by bleeding through the paper. This

[30] Minete, 2010
[31] Prochaska et al., 2023
[32] Prochaska et al., 2023

disinformation campaign began on Election Day and escalated the day after. Users started using the hashtag #SharpieGate to discuss the rumor, and then a viral video spread where two women in Maricopa County claimed they saw ballots being discarded due to the Sharpie damage. The day after Election Day, many Trump supporters picked up on the story and claimed fraud, including First Son Eric Trump.[33] There were even protests outside of the Maricopa County elections department demanding a revote, despite Arizona election officials repeatedly insisting that there was no evidence of ballot damage.[34] So, despite the theory being disproved, disinformation continued to spread, resulting in direct political action by misinformed citizens.

A third and final example of a disinformation campaign during the 2020 election was about Dominion voter machines. In Antrim County, Mich., a vote reporting error incorrectly tallied Biden as having a 3000 vote lead, despite the county's conservative-leaning background. This was a simple mistake by an election worker who did not properly update the software provided by Dominion Voting Systems (DVS), causing incorrect numbers to display that were different from the actual results. The error was corrected relatively quickly, but conspiracies soon started to spread that this was a problem caused by the Dominion machines themselves. The Allied Security Operations Group (ASOG) alleged that DVS manipulated the results, but these claims have since been disproved.[35] Nonetheless, it provided a foundation for disinformation about the effectiveness and accuracy of Dominion machines. Trump himself contributed to these rumors by tweeting that Dominion deleted millions of votes for him across the country, and the only citation he provided was "data analysis."[36] DVS fought these allegations and ended up suing Fox News in a $1.6 billion defamation lawsuit. The company's legal team claimed that Fox

[33] ibid
[34] Nguyen et al., 2020
[35] Prochaska et al., 2023
[36] McNamara, 2020

News promoted inaccurate stories about electoral fraud that had significant negative consequences for Dominion.[37] The lawsuit resulted in a settlement, and Fox News agreed to pay Dominion almost $800 million instead of going to trial in 2023.[38] Similarly, another voting machine company, Smartmatic, settled a lawsuit with Newsmax in a similar defamation over fraud disinformation in 2024.[39] Despite evidence that these fraud claims were unfounded, concerns about voting machines continued to be relevant in the 2024 presidential election. GOP officials in Georgia attempted to file a lawsuit that would challenge the legality of using Dominion voting machines in the state, and they wanted to make images of voting records and ballots available for the public to see immediately after Election Day. Judge Scott McAfee rejected the lawsuit, arguing that policymakers, not courts, should look into this issue.[40] Disinformation about DVS remains relevant in discussions about American elections online, and there appears to be no evidence that satisfies those who already believe the disinformation they read online.

President Donald Trump's role in spreading disinformation about fraud in 2020 must be addressed in this discussion, starting with his attempts to discredit mail-in voting. Despite the American electoral system handling the challenge of expanded mail-in voting extremely well in 2020 according to Persily and Stewart, Trump used this change to claim election fraud. He encouraged supporters to be worried about historical levels of fraud leading up to the election and then blamed mail-in ballots for his loss.[41] His attack on mail-in ballots was his main "voter fraud" grievance, despite Republicans comprising a significant portion of voters in past elections who used mail-in ballots. However, the partisan patterns of mail-in voting flipped because

[37] Long, 2021
[38] Bauder et al., 2023
[39] Durkee, 2024
[40] Cohen, 2024
[41] Persily and Stewart III, 2021

Republicans were less likely to take COVID seriously due to Trump's rhetoric, and many Democrats chose to be more cautious. When that shift became clear, Trump turned on voting by mail, claiming it would increase crime and fraud.[42] He said that voting by mail is "horrible" and "corrupt" and that "they grab thousands of mail-in ballots and they dump it." These claims were backed by Fox News and got further traction on Twitter, as Republican elites, including the Trump campaign's Deputy Director of Communications and Florida U.S. House Representative Matt Gaetz, went on Fox News to amplify fraud allegations in early April 2020. As state governments tried to handle COVID-19 and expand their use of mail-in voting, more right-wing disinformation began to circulate about these ballots in May. In late July, Trump tweeted, "With Universal Mail-In Voting (not Absentee Voting, which is good), 2020 will be the most INACCURATE & FRAUDULENT Election in history. It will be a great embarrassment to the USA. Delay the Election until people can properly, securely and safely vote???"[43] He also claimed that Democrats were planning on sending mail-in ballots to 80 million voters and mailing them to people who did not want them during his first speech at the 2020 Republican National Convention.[44] Additionally, despite making numerous claims that voter fraud was rampant in mail-in voting, Trump had a third-party return his own election ballot through the mail.[45] This disinformation campaign was spurred on and encouraged by President Trump, contributing to widespread accusations of voter fraud through mail-in ballots, claims that are simply not supported by the 2020 election data. As the president at the time, his words about voting by mail had significant credibility for many Americans, and his endorsement of these conspiracies made those claims more believable, despite the lack of evidence that they were true.

---

[42] McDonald, 2022
[43] Benkler et al., 2020
[44] Liptak, 2020
[45] Parks, 2020

In addition to conspiracy about mail-in ballots, President Trump also started the "Big Lie" about election fraud and stolen elections. In April and May 2020, early election polls showed Biden taking the lead. Around the same time, Trump launched disinformation campaigns about election fraud, specifically stating that the only way he would lose the 2020 presidential election was if the election was stolen. This is the idea behind what's known as the "Big Lie," and such voter fraud allegations continued to be supported by Trump, both leading up to the election and then through January 8, 2021 (which is when his Twitter account was suspended).[46] Much of this rhetoric was related to mail-in ballots, but it took a turn after Election Day when he refused to concede the election. He started using the language of "stop the count," which caused Trump supporters in swing states to go to election offices and demand that they stop counting ballots. This campaign quickly morphed into a movement called #StopTheSteal. Trump and his campaign continued to support disinformation about burning ballots, claimed that there were more votes cast than there were registered voters, and shared allegations of election machine hacking.[47] While political conspiracy theories have always existed, these false accusations of election fraud likely would have been given less attention if Trump had not endorsed them through his Twitter account or in public statements. His meritless refusal to concede the 2020 election is an example of a disinformation campaign that came to represent this particular election cycle, and his spread of false information created widespread distrust in elections that still exists today.

Disinformation did not play as significant of a role in the 2024 presidential election outcome as it might have done. However, it still ran largely unchecked and unverified, especially on the social media platform, X. Elon Musk bought the platform in 2022 to "help humanity and

[46] Canon and Sherman, 2021
[47] McDonald, 2022

"protect free speech."[48] However, he has created changes to the platform that have made it easier for disinformation about elections to spread, and he has personally contributed to disinformation campaigns about elections. He has spread misinformation about illegal immigration and election fraud, fueled by a changed algorithm on X that promotes Musk's posts to more people. The warning labels that once flagged false information on Twitter have been replaced by "community notes" on X, which are not as effective in combating disinformation.[49] This has made it much harder for election officials to disprove false narratives about elections on X, primarily because it is harder for them to get as much engagement on their posts, compared to Musk-promoted posts that share disinformation to a much larger audience.[50] Election officials in battleground states have even tried to contact Musk and try to put accurate information in front of him, to no avail.[51] If voters continue to use X as a source of political news, then that presents a dangerous precedent for future elections.[52] While it did not interfere with the administration of the 2024 election or contribute to fraud allegations after the election results came in, it remains a problem that must be addressed in the next elections cycle.

Voter Intimidation

When the word "intimidation" is discussed in this paper, it refers to violent rhetoric or physical threats that are used to coerce someone into changing the way they participate in the electoral system. Voter intimidation can occur in many settings, including polling places and drop box sites. This threat has the potential to incite political violence and prevent some voters from casting a ballot out of fear for their personal safety. If voters choose not to participate in an election out of worry for their physical and mental well-being, then that directly interferes with

[48] Clayton, 2022
[49] Estes, 2024
[50] Collier, 2024
[51] Cohen et al., 2024
[52] Shearer et al., 2024

the end goal of a free and fair election. An election cannot be fair if certain voters are targeted based on their race, gender, political preferences, or any other demographic. The legacies of racial disenfranchisement and voter intimidation at the ballot box illustrates that these tactics are successful in preventing certain groups of American citizens from casting their votes, in turn diluting the voice of legitimate factions in the electorate. Widespread harassment or coercion against voters contributes to election interference efforts, and it may cause serious consequences for voting itself.

There is a significant history of voter intimidation throughout American history, and the attempts to stop African Americans from voting tend to be the most well-known and widely discussed. Black voters were given the right to vote with the Fifteenth Amendment and were able to cast a ballot for a few years during the Reconstruction period. However, even before Reconstruction came to an end in 1877, African American voters faced violent pushback, especially in the South. Organizations such as the Ku Klux Klan targeted Black Americans who attempted to vote, and the violence became widespread and difficult to control. Initially, the federal government tried to hold these offenders accountable through acts including the Enforcement Act of 1870, but many Republicans eventually lost the momentum to police this unrest in the South.[53] In general, African Americans faced the inherent danger of violent backlash if they attempted to vote until the passage of the Civil Rights Act of 1957, the Civil Rights Act of 1965, and the Voting Rights Act of 1965. Together, these acts prohibited attempts to intimidate or coerce voters.[54] While this means that voter intimidation is illegal today, it is still a legitimate threat in elections due to an increase in the number of threats being made toward election administrators.

---

[53] Keyssar, 2000
[54] Friel et al., 2022

Concerns about voter intimidation proved admissible once again as election denialism became more prevalent. In September 2020, a group of Trump supporters gathered at a polling location in Fairfax County, Vir., and chanted “four more years” in front of the entrance. They also formed a line that forced voters to walk around them to enter the polling place. While they stayed 100 feet away from the building and did not directly block access to the building, voters reported feeling “intimidated in a statement made by Gary Scott, the general registrar of Fairfax County.”[55] In Arizona during the 2022 midterms, there were more than a dozen complaints to the Arizona secretary of state about observers camped out by drop boxes watching voters drop off their ballots. They took photographs and videos of the voters as they turned in their ballots, and some of them were armed. There were poll watchers in Mesa and Phoenix, and it was part of a coordinated effort by election deniers across the country.[56] Eventually, a federal judge ordered armed members of Clean Elections USA, a group coordinating drop box monitoring, to stay at least 250 feet from the drop boxes.[57] During the primary elections for the 2024 presidential election, someone installed a camera near a drop box in Plymouth Township, Mich., that would flash when a person walked by the drop box.[58] These efforts to surveil voters can be classified as intimidation because the end goal is to make voters uncomfortable and potentially attempt to influence vote choice. Other methods that have continued to grow in popularity are intimidation tactics from poll watchers, political canvassers, and online trolls.[59] As these efforts continue to happen during recent election years, voter intimidation is a threat that should be taken seriously by election administrators.

---

[55] Corasaniti, 2020
[56] Leingang, 2022
[57] Tang, 2022
[58] Mauger, 2024
[59] Sweren-Becker and Singh, 2024

Intimidation of Election Officials and Poll Workers

Intimidating poll workers and election officials can also disrupt the electoral process by making it more difficult to administer safe and secure elections, both in terms of preventing potential violence and recruiting more workers to run elections. To understand what kinds of threats these officials and poll workers may face, it is important to know the various roles that election officials take on. On the state level of election administration, most states have an elected chief election official, and usually, this role is fulfilled by the secretary of state. Some states allow the legislature, state board, or election commission to select the chief election official. If a state does not have a chief election official, they may split the responsibility for election administration between the secretary of state and an election commission. On the local level, elections are usually run at the county level and by a single individual or an election commission.[60] While elections are administered differently in every state, election officials and poll workers are always on the front line of the electoral process. It is essential to the voting process that these workers are protected from outside intimidation or coercion efforts. If they do not feel safe working in their jobs and voters notice security problems, it will reduce both enthusiasm to work in election administration and trust in the security of American elections. Therefore, threats to both poll workers and election administrators on the local and state levels must be studied and taken seriously to continue having properly run elections.

For poll workers, the most pressing threat is violence at polling places. As threats against election officials surge, there is more concern about protecting poll workers and local election administrators from harm. Some states have enacted legislation since 2020 to prohibit carrying a gun at a polling place, and at least six states have proposed new policies in 2024 to enact this or strengthen existing laws. Many of these acts have been created as a precaution as political

[60] National Conference of State Legislatures, 2023

violence has become more normalized.[61] This legislation helps prevent potential violence at polling places, and it also helps reduce some methods of voter intimidation. While voter suppression attempts are more likely to occur than violent outbursts at the polls, being overly vigilant will likely make poll workers and voters feel safer participating in the electoral process.

Threats to election officials have become increasingly grave. In September 2024, Deputy Attorney General Lisa Monaco revealed that election officials have received unprecedented threats on both the state and local levels. She also declared that the Department of Justice (DOJ) was trying its best to identify those behind the threats to prosecute them.[62] These threats often occur online or over the phone, and they target election administrators on all levels. Colorado Secretary of State Jena Griswold has reported receiving hundreds of threats on her life across her social media accounts, email, and fringe social networks since the 2020 presidential election.[63] Tina Barton, the former clerk for elections in Rochester Hills, Mich., received a profanity-laden voicemail threatening her and her family's lives a week after the 2020 election.[64] Lisa Deeley, a local election chief in Philadelphia, received so many threats on social media that she had to be accompanied by a security detail everywhere she went for weeks after the election.[65] Thousands of election officials have reported receiving similar threats since the 2020 election, and it has led to the DOJ creating a task force in 2021 to try to protect election workers and offer support.[66] Despite this effort to take these threats more seriously and potentially prosecute those who do (though more often than not, this does not happen because of First Amendment protections), election administrators continue to face concerning levels of harassment and menacing threats.

---

[61] Rodriguez et al., 2024
[62] Gibson et al., 2024
[63] Zakrzewski, 2022
[64] Sullivan, 2024
[65] Johnson et al., 2022
[66] Sullivan, 2024

This new phenomenon of widespread intimidation of election officials has had serious consequences for election administration. According to a survey conducted by the Brennan Center in early 2024, 38% of local election officials have experienced threats or harassment from doing their jobs.[67] The Bipartisan Policy Center discovered that areas with more than 250,000 residents have higher percentages of local election officials reporting harassment and abuse compared to less-populated districts. They also have found that there has been a 38% increase in turnover from 2004 to 2022, illustrating a slow but upward trend.[68] This pattern should not be overlooked. This new phenomenon of widespread, violent threats is an added layer of stress for election administrators. Local election officials now wearily carry out their duties with a new fear for their personal safety as some administrations receive daily threats online or over the phone.[69] For example, the top election official in a swing county in Nevada decided to take a stress leave of absence two months before the 2024 presidential election, and this county has been constantly under scrutiny from conspiracy theorists since 2020.[70] If election officials continue to be put under this strain, the increasing turnover rates will not decrease and it will be harder to recruit qualified professionals to take on these jobs. This will make it more difficult to carry out the electoral process. It will also make it more vulnerable and easy to undermine. Therefore, the well-being and safety of local election officials must be prioritized.

Foreign Interference

The United States is no stranger to both interfering in other countries' elections and experiencing intrusions of its own. In this review, the term “foreign interference” will refer to intentional acts made by another country to infiltrate the American election process in a way that

[67] Edlin et al., 2024
[68] Ferrer et al. 2024
[69] Garrett, 2024
[70] Sonner et al., 2024

could impact vote choice or thwart election administration. This is a threat that has been mostly dismissed for most of American history, despite the U.S. contributing to many election interference attempts in other countries, especially during the Cold War.[71] American presidents intervened in other states' elections without fear because they believed that no one would be able to target the U.S.s in a similar operation. This attitude and feeling of security all changed in 2016 when Russia launched a strong anti-Hillary Clinton movement that would change the way voters saw their candidates and, more importantly, the integrity of the electoral system. This section will discuss the history of foreign actors attempting to intervene in American elections, with a special focus on Russia. It will also focus on the 2024 presidential election cycle.

Pre-2000s Examples of Foreign Interference in American Elections

There is no substantial history of foreign election interference in the U.S.before the Cold War, so there are only two notable events to mention. The first took place during the 1796 election when France attempted to thwart the re-election campaign of George Washington. When Washington chose not to run again, they attempted to sabotage the campaign of John Adams through overt intervention. A decree was sent by Pierre Adet, the French ambassador to the U.S., which removed the neutral status that American ships were given during the Napoleonic Wars. This was aimed to restrict American trade. Their efforts to prevent Adams from becoming president were unsuccessful, as Adams won the election. The second event occurred during the 1940 election, and it was an effort by the Nazis, who aimed to stop Franklin Roosevelt from winning a third term. Hitler was concerned that Roosevelt would bring the U.S. into World War II, so the Nazis started a secret operation inside the U.S. against Roosevelt. They bribed an American newspaper to publish a 1939 memorandum featuring American and Polish government officials that depicted Roosevelt as a "war-monger" five days before the election. This became a

[71] Suri, 2024

front-page story, and it countered Roosevelt's promise that he would avoid war if possible. However, Roosevelt won his re-election, so the attempt was unsuccessful.[72] These attempts may seem insignificant in their impacts on election outcomes, but that is exactly why they must be included in the larger history of foreign election interference. Because the intervening states' efforts did not achieve their desired outcomes, American officials in Obama's administration were not prepared to face the effectiveness of foreign interference in 2016. This is important to keep in mind alongside the Soviet Union's attempts to sway election results.

The Soviet Union worked to interfere in American elections from 1960 to 1984, albeit unsuccessfully, for the most part. As described by historian David Shimer, these efforts were the most apparent in 1960, 1968, 1976, and 1984.[73] In 1960, Soviet leader Nikita Khrushchev wanted Nixon to lose the election so he reached out to Adlai Stevenson, the Democratic nominee for president in 1952 and 1956. Stevenson had said he would not run again, but Khrushchev wanted to change his mind. He sent Moscow's ambassador to the U.S. to meet with Stevenson, and the ambassador gave Stevenson a letter that offered assistance from the Soviet Union to win the presidency. Stevenson refused and explicitly stated that he did not want to participate in foreign interference attempts.[74] In 1968, the Soviet Union wanted to undermine Nixon again, despite Khrushchev no longer being in power. Similarly to 1960, Andrei Gromyko, the Soviet foreign minister, told Anatoly Dobrynin, the Soviet ambassador to the U.S., to help Democratic Party nominee Hubert Humphrey with whatever he needed. Once Humphrey caught onto this, he firmly declined the offer.[75] While Nixon prevailed in 1968 and won the presidential election, it was not due to Soviet election interference efforts because Humphrey was not interested in

[72] Levin, 2021
[73] Shimer, 2020
[74] ibid
[75] ibid

receiving foreign assistance. In 1976, the KGB was unsupportive of both Democratic and Republican candidates. They became afraid of Ronald Reagan during the Republican primary because he was very anti-Soviet, so Soviet officials were wary of him. Despite this, there is no evidence they did anything to thwart his electoral prospects. Soviet officials were more proactive with Henry "Scoop" Jackson, a Democratic senator from Washington who was known for being outspoken against the Soviet Union. KGB officers noted that he kept his personal life private, and investigated his sex life hoping that they would find that he was homosexual. They also searched all matters of his personal life in pursuit of information to blackmail him with.[76] The officers found no evidence that Jackson was gay, so they created the evidence themselves with a forged FBI document from 1940 that claimed that Jackson was homosexual. They sent it to the *Chicago Tribute*, the *Los Angeles Times*, and Jimmy Carter's campaign headquarters. However, this did not get much traction from the newspapers, and Jackson later dropped out for other reasons.[77] In 1984, Soviet officials targeted Reagan with a letter-writing campaign that ultimately was not successful, especially because the U.S. government caught on.[78] Shimer argues that these attempts were not particularly successful because the Soviet Union had to rely on third-party actors, such as the media and politicians, to allow their interference efforts to be successful.[79] This was no longer the case leading up to the 2016 presidential election, primarily because of the creation of social media networks.

2016 Foreign Interference

Russia intervened in the 2016 American presidential election through three main methods. The first was through hacking DNC emails and distributing them by posting them

[76] ibid
[77] Shimer, 2020
[78] ibid
[79] ibid

online or sending them to WikiLeaks.[80] There were also successful attempts to breach the voter registration system in several states. These first two methods will be discussed further in detail in the section on cybersecurity and hacking. The third method was widespread social media propaganda to which many social media users were exposed. These influence campaigns and their impact on vote choice is the focus of this section's discussion of 2016 interference. Its impacts on vote choice and trust in elections cannot be understated. The Obama administration, especially U.S. Secretary of Homeland Security Jeh Johnson, was terrified of widespread Russian hacks on Election Day after Russia's successful email hacks. However, nothing happened. There were no cyberattacks, no stolen files, and no evidence of attempts to change the vote count. However, the Obama administration's focus on Russia possibly trying to affect the election results through changing actual votes distracted from Russia's disinformation campaign that infiltrated popular social media sites.[81] They did not realize the threat of Russian propaganda on social media until the election was over, and by then it was too late to correct.

Russia's plan to influence public opinion about Democratic nominee Hillary Clinton and general feelings about election integrity was implemented on a wide scale and was extremely successful in targeting millions of Americans. Russian President Vladimir Putin and his influence operations started focusing on the Republican Party during Obama's presidency. Both Putin and the Republicans despised then-Secretary of State Hillary Clinton. Putin disliked her because she criticized him for his attempts to dictate Ukrainian politics, and the Republicans saw her as a political threat who could succeed Obama. Many Republicans who would work on Trump's presidential campaign, including Paul Manifort, Roger Stone, and Michael Flynn, were given compromising materials on Clinton by Russia and assisted with spreading that

[80] ibid
[81] ibid

information. Putin also created a network of hackers and internet trolls to cause chaos for Clinton's campaign efforts on social media. This group was called the Internet Research Agency (IRA).[82] Millions of people unknowingly saw Russian propaganda that was depicted as news about Clinton during her 2016 presidential campaign. Russians behind this disinformation often posed as American users so Americans would not realize the information was coming from foreign actors. They made the accounts and posts seem like they belonged to actual Americans and engaged people with normal posts and ads. Members of the IRA tracked which elements of the content engaged viewers and collected detailed reports to continue their work. They used advertisements to reach specific kinds of voters and targeted voters by location. They also encouraged divisions between different races and religions, especially African Americans and Jewish Americans.[83] This micro-targeting of specific groups in the American electorate further exacerbated racial tensions, and one of the ways Russia tried to influence the outcome of the 2016 election was by inflaming these historical divisions.[84] Above all, they weaponized fear and fed into conspiracy theories, including the idea that Clinton and Obama wanted to steal the 2016 election.[85] They sowed doubts, encouraged conspiracy theories, and empowered divisions within the electorate to achieve a tense political environment contributing to questions about election integrity and the security of American elections. These factors would have made it perfect for Trump to challenge his defeat and create chaos in the American political system.

This Russian disinformation campaign was likely operating on the assumption that Clinton would win the presidency and Trump would use the conspiracies spread by the Russians to cast doubt on the election results. However, as we all know, that did not happen. Trump was

[82] Suri, 2024
[83] Shimer, 2020
[84] Johnson, 2019
[85] Shimer, 2020

able to clinch an electoral victory through very tight margins in a handful of battleground states, to the surprise of many Americans. After this unexpected victory, the Russians stopped the disinformation about voter fraud since their preferred candidate had won. Despite avoiding widespread public disorder about election integrity, this outcome still had consequences for the electoral system. Trump was aware that Russia was helping him as the election drew closer and formed a friendly relationship with Putin once he became president. Alarmingly, he displayed a lack of concern about election integrity and did not personally take steps to make elections more secure in the U.S.[86] So, there were no real repercussions for Russia from Trump that would prevent this outcome from happening again.

Despite Trump not taking action directly against Russia, the American national government did intervene and try to punish Russia for its role in interference. In December 2016, the Obama administration announced sanctions on Russia, specifically Russia's military intelligence agency, the GRU, and removed 35 suspected Russian intelligence operatives from the U.S.[87] In 2018, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) used the Countering America's Adversaries Through Sanctions Act (CAATSA) and Executive Order (E.O.) 13694 to create sanctions against the IRA for its cyber interference.[88] These sanctions targeted 24 entities and individuals for their role in attempting to interfere in the 2016 election and the cyber attacks they were behind, including the GRU.[89] The Senate also investigated Russia's role in the cyber attacks. The Senate Intelligence Committee released a report in 2018 that discovered that African Americans were specifically targeted by Russia's disinformation campaign in an attempt to suppress turnout among Democratic voters.[90] Another

[86] Shimer, 2020
[87] Sanger, 2016
[88] U.S. Dept of Treasury, 2018
[89] Schor et al., 2018
[90] Shane and Frenkel, 2018

report by the same committee in 2020 affirmed that the initial assessment of Russian interference in the January 2017 U.S. intelligence assessment was indeed correct and nonpartisan.[91] Russia's interference attempts did not go unnoticed by the American national government, but the punishments against Russia might have been more effective if Trump endorsed them instead of showing support for Putin and Russia.[92] It also might have discouraged Russia from trying to interfere similarly during the 2020 presidential election if he was more willing to take action.

2020 Foreign Interference

Foreign attempts to interfere in the 2020 presidential election were less impactful than in 2016, but they came from a larger number of states. Russia, China, and Iran all aspired to contribute to existing political chaos in 2020, and Russia was behind the most serious attempts to interfere in the election.[93, 94] Unlike 2016 interference attempts, none of these states attempted to interfere with any technical component of the voting process itself. Instead, they further focused on the spread of false information that aimed to change Americans' perceptions of the two candidates. Russian state-owned media outlets, such as *RT* and *Sputnik News*, promoted Trump and Senator Bernie Sanders and their campaigns. They supported Sanders because they thought he was more interested in foreign isolation compared to other anti-Trump candidates, they wanted to split Democratic support, and because Sanders is a left-wing populist. These media sources bashed other Democratic candidates running against Trump, and they published stories that questioned the validity of the election results coming out of the primaries, especially the Iowa Caucus' app glitch. Kremlin media spread information about the violence during the Black Lives Matter movement to try to play off the divisions that took over American political thought.

---

[91] Dilanian, 2020
[92] BBC, 2018
[93] Government Agencies and Private Companies Undertake Actions to Limit the Impact of Foreign Influence and Interference in the 2020 U.S. Election, 2021
[94] Watts and Chernaskey, 2021

Russia also contributed to questions about the validity of the 2020 election results and published stories about illegal votes and glitches.[95] After the election, the Office of National Intelligence assessed that Putin and other Russian government organizations tried to conduct influence operations to negatively impact Biden and the Democrats while supporting Trump. This was done through undermining public trust in elections and attempting to heighten existing socio-political divisions. They did not try to hack into election infrastructure, unlike in 2016.[96] Many of these attempts to sow doubt in the electoral process were done on Twitter (now X) through the use of "trolls" (fake accounts spreading hyperpartisan ideas) and "superconnectors" (highly connected accounts that aimed to spread information quickly).[97] Russia intended to create chaos on online networks to undermine overall confidence in American democracy, just like they did in 2016.

Iran's state-owned *PressTV* promoted negative coverage of Trump and criticized Trump's foreign policy stances from his first term. It also criticized Biden as part of the "corrupt" Democratic Party. Through their rebuke of the Democratic Party, they also portrayed Sanders as a victim of Democratic Party leadership.[98] The Office of National Intelligence also found that Iran tried to launch its own influence campaign to hurt Trump's campaign by undermining confidence in elections and institutions and creating divisions within the electorate. However, they did not directly promote Trump's rivals. The Office of National Intelligence also suggested that Supreme Leader Li Khamenei likely authorized Iran's influence campaign and Iran increased cyber influence efforts against the U.S. from previous elections.[99] Additionally, they tried to infiltrate voting information and registration systems for 11 states, and they were

[95] Watts and Chernaskey, 2021
[96] Foreign Threats to the 2020 US Federal Elections, 2021
[97] Marcellino et al., 2020
[98] Watts and Chernaskey, 2021
[99] Foreign Threats to the 2020 US Federal Elections, 2021

successful in one state.[100] While Iran did not have an interference plan as coordinated as the Russians' plan, it cannot be considered insignificant.

The U.S. government was much more prepared to handle foreign interference in 2020 than it was in 2016. The U.S. Cyber Command used a more proactive and aggressive strategy in the weeks leading up to Election Day, and attacks on election infrastructure never happened.[101,102] The Office of the Director of National Intelligence (ODNI) also issued a warning about potential election-related operations, specifically with China, Iran, and Russia in July 2020. Additionally, there were some warnings identifying Russia as the most dangerous adversary, with then-FBI Director Christopher Wray publicly stating in September 2020 that they had seen attempts by the Russians to influence the election by promoting information attacking Biden. The U.S. government also issued sanctions against Russian and Iranian actors involved in interference. One sanction was applied to Ukrainian Parliament member Andrii Derkach, who had been working with the Russians to spread disinformation about American politicians, and another was applied to Iranian government-linked entities who sent emails to voters in Alaska and Florida claiming to be the Proud Boys.[103] Cyber Command and Microsoft also worked together to combat TrickBot, a Russian network of computers that had the potential to put ransomware in election systems. Cyber Command was able to free many of the hijacked computers from TrickBot's control.[104] In general, social media companies were much more willing to report cases of disinformation and publicized their efforts to prevent foreign influence from spreading.[105] So, the government was much more prepared and proactive in dealing with foreign interference in

---

[100] U.S. Attorney Announces Charges Against Two Iranian Nationals For Cyber-Enabled Disinformation And Threat Campaign Designed To Interfere With The 2020 U.S. Presidential Election, 2021
[101] Watts and Chernaskey, 2021
[102] Cohen and Herb, 2021
[103] Government Agencies and Private Companies Undertake Actions to Limit the Impact of Foreign Influence and Interference in the 2020 U.S. Election, 2021
[104] ibid
[105] ibid

the 2020 election, and foreign actors were not as successful in influencing perceptions about American politicians in 2020 as they had been in 2016.

2024 Foreign Interference

In 2024, foreign interference attempts were similar to 2020. China, Iran, and Russia all contributed to the spread of disinformation across social media sites leading up to the election. However, the disinformation threat was worse because the tactics used were more sophisticated and AI has made it much easier to spread it. Russia continued to spread disinformation to support Trump, and Iran used it to support Kamala Harris.[106] In particular, Iran created fake news websites to spread information and target conservative voters in Georgia and Arab Americans in Michigan, demonstrating a deep understanding of the groups that Harris needed to win over.[107] The use of AI has made it much easier for foreign states to distribute disinformation. For example, China spread audio, members, and voter polls that were manipulated by AI, including a deepfake video showing a Republican congressman from Virginia that incorrectly depicted the politician canvassing for a Taiwanese presidential candidate.[108] Russia also targeted American swing states during the election by creating false content to sway voters toward Trump. They did not hack anything, but they continued to target Americans by creating content that appeared to come from authentic Americans.[109] U.S. intelligence agencies also discovered that Russian actors spread content trying to promote false narratives about election fraud.[110] Russia was responsible for a number of manipulative videos that spread across social media leading up to the election, including a false depiction of ballots being destroyed in Pennsylvania and false allegations showing noncitizens voting in large numbers at polls in Georgia.[111] In response to Russia's

[106] Frenkel et al., 2024
[107] ibid
[108] ibid
[109] Nakashima, 2024
[110] Cassidy and Swenson, 2024
[111] Jingnan, 2024

widespread campaign to promote disinformation online, the U.S. sanctioned Russian state media and announced plans to try and make these attempts less impactful for the election.[112] A final takeaway about 2024 foreign disinformation is that it is becoming harder to identify disinformation because social media companies either have no policies in place to correct disinformation or have relaxed them since 2020.[113] Foreign disinformation did not contribute to any issues with carrying out the 2024 election, but its advanced tactics and use of artificial intelligence illustrate potential problems for future elections because these methods are becoming extremely difficult to detect and correct.

One of the most concerning parts of 2024 foreign interference happened on Election Day. Hoax bomb threats were sent by Russian email addresses to polling places in several states.[114] These emails targeted polling places in Georgia, Pennsylvania, Michigan, Wisconsin, and the Navajo Nation in Arizona.[115] In some areas, these threats delayed voting and the counting of the ballots.[116] While this type of foreign interference did not cause a major disruption, that does not mean it will not be able to in the future. This attempt to create chaos on Election Day could have had serious consequences for election administration if election officials were not prepared to handle it. It is important to ensure that they continue to be ready to defend the electoral system against similar threats in the future.

Cybersecurity and Hacking Concerns

Maintaining cybersecurity and defending electoral administration from hackers is a new threat to the American electoral system, but it is one of the most important to consider. The main concerns include the hacking of voting machines and the hacking of voter registration systems.

---

[112] Cabral, 2024
[113] Frenkel et al., 2024
[114] FBI Statement on Bomb Threats to Polling Locations, 2024
[115] Jingnan, 2024
[116] Luhby et al., 2024

The 2016 presidential election highlighted the growing importance of cybersecurity and defense against hacking attempts in American elections. In mid-June 2016, it was discovered that two Russian hacking groups, sponsored by the Russian state, had hacked into the DNC's network as well as an anonymous entity called Guccifer 2.0 to upload stolen DNC documents online. Just before the 2016 Democratic National Convention, the GRU sent stolen DNC information to WikiLeaks, which began posting DNC emails online. This became a major story in American media because it highlighted a bias within Democratic Party leaders that favored Clinton getting the nomination over Sanders.[117] The GRU was also behind successful hacks into the voter registration bases for Arizona and Illinois, and they were able to access records for millions of voters with their personal information, including Social Security numbers. They did not manipulate voter data, but they showed that they could.[118] Obama officials knew that Russia would not be able to alter enough voters to swing the election, despite some state voter registration lists being insecure, but they could do enough damage that people would question whether the election was valid.[119] Additionally, Russia targeted the election systems in all 50 states, hinting at the United States' vulnerability to handle cyberattacks in future elections.[120] This posed a serious issue for election administration and started a more important conversation about vulnerabilities in the electoral system. Concerns about voting machines and voter registration systems have been the most prominent election cybersecurity issues in recent years.

After Russia's 2016 attacks, concerns about the security of voter registration systems were warranted. However, research from the Center for Election Innovation & Research (CEIR) has concluded that voter registration databases, or VRDBs, have become much more secure

[117] Shimer, 2020
[118] Shimer, 2020
[119] ibid
[120] Sanger and Edmondson, 2019

since then. They have been surveying states about VRDBs every few years and released reports in 2018, 2020, and 2022.[121] Their 2018 report concluded that while some aspects of VRDB security had improved, like the implementation of regular audit systems and database backups, there was still significant work to be done. They also noted that states showed a real commitment to cybersecurity and were taking the steps needed to prevent the 2016 cyber attacks from happening again.[122] In the 2020 report, CEIR found that more of the surveyed states were using multi-factor authentication to make sure only authorized users were able to access these databases, which they wanted to see more of in the future. They also argued that VRDB security had gotten better since the previous report, especially because cyber threat detection had gotten better. They recommended that states regularly back up their VRDBs and test backups frequently.[123] The 2022 report detailed more of the same, and it demonstrated that states have maintained the improvements that they have implemented since 2020 to protect VRDBs. More progress was made with multi-factor authentication, and states were even better at detecting potential cyberattacks. Overall, they concluded that there is still room for improvement, but that they felt confident in VRDB security measures across the U.S.[124] While there are still improvements that can be made to protect American voter registration systems, it is in a much better place than it was in 2016, and states are much more prepared to fend off cyberattacks on VRDBs from both foreign and domestic aggressors.

To fully comprehend the concern about voting machines being vulnerable to hacking, it is important to have a basic understanding of the modern history of voting machines. The two most popular systems that are used today are direct recording electronic devices (DREs) and optical

[121] Securing Voter Registration Databases: 2024 Survey Preliminary Results, 2024
[122] Becker et al., 2018
[123] Becker et al., 2020
[124] Sullivan et al., 2023

scanners. DREs were created in the 1970s and as screen technologies were made more common, there was a shift into making them fully digital with no paper trail.[125] Voters simply tap the screen to make their selection.[126] As this technology was adopted by many voting districts, there was more resistance to its implementation. Opponents argued that it would be difficult to tell if the machines were tampered with and that they could be more error-prone than other systems.[127] To address this, many DREs now have a Voter Verified Paper Audit Trail (VVPAT), which can be used to confirm a voter's selections and provide a paper trail to help verify results.[128] Optical scanners are machines that take physical ballots and tabulate the results. They accept two kinds of ballots. One version has ovals that a voter can fill in to mark their choice, and the other version has a discontinuous arrow that a voter completes.[129] This form of voting leaves a paper trail because voters fill out a physical ballot that they feed to the machine. These two types of voting technologies are the most popular machines used in polling places today, but there are significant questions about their security in present-day elections.

The 2000 election was a turning point in the voter machine history, and punch cards caused problems and widespread controversy. Because Florida was the state that was going to determine the outcome of the election, it received significant attention for its confusing ballot design and issues with punch card ballots. This ballot had two columns for candidates with a middle column of squares that needed to be punched through. The punched-through square that lined up with a candidate's name was called a "chad." This proved to be a problem for election workers because some chads were not punched all the way through, and these chads were called "hanging chads." Election workers then had to guess who the voter wanted to choose because it

[125] Stewart III, 2011
[126] Thomas, 2023
[127] Stewart III, 2011
[128] Thomas, 2023
[129] Stewart III, 2011

was unclear whether they wanted the candidate corresponding to the hanging chad or whether marking the hanging chad candidate was an accident.[130] While this was one of the many controversies surrounding the 2020 election, it changed the way many people saw punch cards and made their use more controversial.

The Help America Vote Act of 2002 (HAVA) created new standards for voting machines. First, it created the U.S. Election Administration Commission (EAC), which creates voting system standards and guidelines. It also gave states funding to replace punch card machines with DREs or optical scanners.[131] HAVA promised states $3.9 billion to help buy this new equipment and to run elections on a few conditions, including not spending the money on punch card or lever machines.[132] However, the implementation of this act led to further problems for election security, specifically with DREs. The main problems with DREs today are outdated machines and malware concerns combined with some machines still lacking a paper trail.

Outdated voting machines can pose a significant risk to the American voting system. Today's machines are not meant to last for numerous election cycles, and they tend to work for 10 to 20 years, likely closer to 10.[133] This means they need to be replaced and updated relatively frequently. If new machines are not purchased, there will be potential problems with system failures and crashes which can lead to votes being lost, potential hacking, and a loss in public confidence. Additionally, election officials might not have the resources available to buy new and expensive voting machines, which makes the issue even more alarming.[134] Outdated voting systems remain an issue today, but there has been significant progress towards replacing old systems. In 2022, 24 states still had machines that were over ten years old as their main voting

[130] Thomas, 2023
[131] Thomas, 2023
[132] Zetter, 2018
[133] Norden and Famighetti, 2015
[134] ibid

equipment.[135] This poses a significant risk to vote counting and storage and should be taken seriously. The consequences of this predicament only grow more dire as public confidence in election integrity decreases.

A concern about DREs that is more directly connected with cybersecurity is the threat of malware hacking on these voting machines. In 2007, studies that California and Ohio sponsored found evidence that DREs had security flaws and that it was possible for malware to be installed on them that could potentially record votes incorrectly or miscount them.[136] This potential for hacking remains a pressing concern today, and multiple computer scientists have warned of the dangers of electronic voting machines. David A. Eckhardt, a professor of computer science at Carnegie Mellon University, was asked to examine the voting systems used in Venango County, Pa. There had been issues with these machines flipping votes to other candidates, which was a significant issue because these machines had no backup paper trail. While Eckhardt determined that the issue was a simple glitch, they discovered that remote-access software had been installed on the voting machines. This software is typically used to control computers remotely or over an internal network, so this was alarming to discover on voting machines because they are meant to be fully disconnected from the internet and from other machines that are online. While the software was not being used by a hacker and by an "authorized county contractor," it still raises questions for election security.[137] Installing this remote access software and modems on voting systems that carry out the voting process is an important security issue. While these machines transmit results to county election offices using modems and phone lines, not the Internet, it can still be a security risk because cellular modems use radio signals to send data to routers that

[135] Baker et al., 2022
[136] Ottoboni and Stark, 2019
[137] The Myth of the Hacker-Proof Voting Machine, 2018

belong to mobile carriers, and these routers are connected to the Internet.[138] This means that hackers could potentially intercept results or hack into voting machines and install malware or alter results. Election officials and the EAC often defend DREs and optical scanners by saying that they are hack-proof because they are not connected to the Internet, but this is simply untrue. Experts in computer science and cybersecurity remain worried about voter machine hacking, despite elections officials dismissing these concerns.

At the University of Michigan, computer scientist J. Alex Halderman ran a mock election asking students to choose between the University of Michigan and its arch-rival The Ohio State University using a DRE. When the results showed an Ohio State victory, he revealed to students that he was able to install malware on the voting machine through elementary coding techniques.[139] He used this simulation to advocate for paper ballots or paper trails for all DREs so audits could be run. This reasoning is why VVPATs were implemented in more DREs. However, VVPATs could still be compromised because the printer could malfunction and VVPATs are difficult to audit because the paper is easily damaged.[140] It is not a completely reliable way to audit results, which is why shifting back to paper ballots is the safest way to handle cybersecurity concerns with voting machines. DREs without paper trails should be discontinued immediately and all DREs should have a way to run post-election audits to verify results.

Risk-limiting audits are the best way to verify election results that come from voting machines, and they require voting machines with paper trails. These audits have gained more traction as election security becomes more important.[141] Risk-limiting audits are incremental and are meant to give statistical confidence that election results are correct. This means that if the

[138] ibid
[139] How I Hacked an Election, 2018
[140] Ottoboni and Stark, 2019
[141] Risk-Limiting Audits, 2024

margin of an election is wide, not as many ballots will be reviewed. If it is more narrow, more ballots will be looked over.[142] Most states do not have risk-limiting audits in place, but they are an efficient way to review election results and provide more confidence in results. Because hacking and cybersecurity concerns have become a pressing issue, implementing cost and time efficient audit systems is a great way to restore confidence in election results. This is why DREs without paper trails must continue to be phased out and replaced by DREs with VVPATs. Voting machines that polling places use must be kept up to date with risks to election security, or else problems with hacking and cybersecurity will become even more amplified.

[142] Risk Limiting Audits, 2024

Methodology

To evaluate U.S. states' preparedness to face the threats covered in the literature review, a sample of 12 states was selected and investigated thoroughly, divided into three groups: Republican-leaning states, Democratic-leaning states, and swing states. Within each partisan group of states, there was also a consideration of regional diversity, size diversity, and the strength of the state's partisan label. In other words, I wanted each group to include states from different parts of the country, states of differing sizes, and states that vary in the robustness of their partisan leaning. To determine swing states, I selected four out of the seven swing states in the 2024 presidential election. I also focused on regional diversity in this grouping, since there were not many options for swing states. For Democratic-leaning and Republican-leaning states, I used the Cook Partisan Voting Index, choosing states that shared the same partisan leaning but are different in region, size, and how partisan they were according to the PVI.[143] Keeping such criteria in mind, the following table depicts the 12 chosen states within their partisan groups that were studied for this analysis.

RED STATES	BLUE STATES	SWING STATES
Montana	California	Arizona
Tennessee	Maryland	North Carolina
Texas	Minnesota	Pennsylvania
West Virginia	Vermont	Wisconsin

General Procedure for Preparedness Evaluations

Each state was researched and evaluated based on how prepared it was to face each of the threats outlined in this thesis. The first step in this process was to identify indicators that assessed

[143] 2022 Cook PVI: State Map and List

how prepared states were to respond to each threat. Each threat had at least two indicators. The next step was to combine all indicator scores to produce a composite "threat grade." Each state received one threat grade for every threat. Finally, I ran K-Means clustering on the threat grades, and states were placed into "preparedness groups" by the algorithm. The results from this test were graphed onto a map of the U.S. to easily visualize the state groupings.

A crucial distinction should be made here before continuing with the results of this methodology. When I started researching the indicators, I wondered if each state had the power to fully defend itself against all of the cited threats. In other words, is it reasonable to expect that state action (paired with federal assistance) is fully effective in preventing those threats from happening? The answer to this question is no for most of the threats I have discussed in this paper. Since states cannot be fully defensible against all threats outlined here, it reasonably follows that this analysis should be a comparative analysis. This means that the preparedness groupings are relative, and they focus on realistic ways that a state can improve its response to these threats, and how states score compared to other states. This is why K-Means is an effective method to group the states. This clustering method is comparative since it places states in clusters based on how their scores compare to other states' threat scores.

My focus on comparative rankings is why I also decided to exclude two threats from this analysis. While candidates refusing to concede and disinformation about election fraud are two very important threats to election administration, states can do relatively little to police or prevent these threats. In regards to candidates refusing to concede, one could argue that courts can throw out frivolous lawsuits and sanction the lawyers, but that does not always punish the candidates themselves, the ones who are most responsible for this threat. Most of the damage from refusing to concede occurs from voters questioning the validity of election results and

distrusting election administration, which is not remedied by punishing frivolous lawsuits. So, I decided to exclude this threat from my comparative analysis. I also removed disinformation about election fraud (category two of disinformation) because there is little that can be done about this due to free speech concerns. So, the threats that will be included in this procedure are election officials refusing to certify results, voter intimidation, election official intimidation, disinformation about the voting process or the way elections are run, foreign interference, and hacking.

I also want to define two important terms before moving on to the results. When I refer to indicators, I am referencing the list of criteria that a state has to meet to receive a good grade on a threat. Each criterion is one indicator, and indicators will determine the overall threat grade that a state receives for a certain threat. The term “threat grade” refers to the general score that a state receives for a certain threat. Higher scores indicate that a state is doing a good job in defending itself against the threat.

Results

Threat Indicators

The first step of the methodology was to collect and score indicators for each threat and state. Table 3 lists all the indicators used to evaluate each threat and how grades were assigned. Grades ranged from 0 to 3. All sources that determined the answers to each indicator for each threat and state can be found in Appendix C.

Election Officials Refusing to Certify

Table 1a. *Indicators to Evaluate State Preparedness for Election Officials Refusing to Certify*

Indicators	Threat Grade Rubric
1. Can the state implement a writ of mandamus to compel an official to certify an election? 2. Can the state enforce a writ of mandamus? 3. Does the state have an equivalent of FRCP 70 in state law? 4. Does the state have a specific law that gives state officials the ability to directly intervene and complete the certification process?	**3**: The state can implement a writ of mandamus to compel an official to complete their certification duty, has an equivalent of FRCP 70 in state law, and has a law/statute that gives state officials the ability to directly intervene and complete the certification process.
	2: The state can implement a writ of mandamus to compel an official to complete its certification duty and has an equivalent of FRCP 70 in state law.
	1: The state can implement a writ of mandamus to compel an official to complete its certification duty and has some mechanism for enforcing the writ of mandamus that is not a direct implementation of FRCP 70 in state law.
	0: The state cannot implement and/or enforce a writ of mandamus.

For election officials refusing to certify, there are a few clear actions that a state can take, as outlined by the Brennan Center for Justice. Their report on guardrails to election certification processes outlined that states can issue writs of mandamus to specifically compel election officials to certify election results, and some states even have laws that explicitly allow state officials to complete certification if a local official refuses. The report also mentioned that many states have a state equivalent of Rule 70 of the Federal Rules of Civil Procedure, which compels officials to comply with a writ of mandamus. If they don't have this rule implemented on the state level, courts also can direct other officials to certify results.[144] However, Rule 70 is the most effective way to enforce a writ of mandamus, and states who do have this law are better protected against the threat of an official refusing to certify.[145] Based on the Brennan Center's report, a state is also more equipped to counter this threat if they have an explicit law that allows state officials to complete certification if there's an issue. These conclusions made the grading relatively intuitive as each state's grade was based on their readiness to face the threat of election officials refusing to certify results.

[144] Election Certification Processes and Guardrails, 2024
[145] Muller, 2023

Voter Intimidation

Table 1b. *Indicators to Evaluate State Preparedness for Voter Intimidation*

Indicators	Threat Grade Rubric
1. Does the state have its own version of the Voting Rights Act? 2. Does the state have legislation that makes voter intimidation illegal at polling places? 3. Does the state have legislation that makes voter intimidation illegal at drop off sites/ballot boxes? 4. Does the state have a rule against having weapons at the polling place? 5. Does the state have restrictions on who can be in the polling place at a time? 6. Does the state have some kind of security or check for poll watchers that prohibits them from interfering with voters? Do they have a code of conduct? 7. Does the state have explicit restrictions on electioneering outside the polling place that interferes with voters?	Each state was awarded a score from 0 to 3 for each indicator. If the state had the indicator, it received a score of 3 for it. If it didn't, it received a 0. For some indicators, some partial credit was given (see Appendix A for full scoring results). Indicators were treated equally in all cases. The average score across all indicators was calculated for each state and rounded to the nearest whole number. This value became the grade

Indicators for voter intimidation were compiled and evaluated using the Law Enforcement Quick Reference Guides from the Committee for Safe and Secure Elections, databases from the National Conference of State Legislatures, and information on protecting voters from intimidation from the Campaign Legal Center.[146,147,148,149,150] These sources compiled

[146] Law Enforcement Quick Reference Guides, Committee for Safe and Secure Elections
[147] Poll Watchers and Challengers, 2024
[148] Electioneering Prohibitions Near Polling Places, 2024
[149] Table 9: Ballot Drop Box Laws, 2025
[150] Protecting Voters from Intimidation, Campaign Legal Center

existing state laws that aim to prevent voter intimidation. Indicators were all weighed equally and ranged from 0 to 3. Partial credit was awarded in certain cases for four out of the seven indicators if a state had some aspect of the indicator but not enough to mark it as a 3. Each state received an average score based on its indicator scores, which were then rounded to the nearest whole number. I chose to round the average scores because these indicators were scored with my subjective judgement and rounding allowed me to assign grades while avoiding false precision. This rounded value became the threat grade for each state.

Election Official Intimidation

Table 1c. *Indicators to Evaluate State Preparedness for Election Official Intimidation*

Indicators	Threat Grade Rubric
1. Does the state have legislation that makes election official intimidation illegal at polling places and online/in personal settings? 2. Does the state count poll workers as protected election workers? 3. Does the state have a rule against having weapons at the polling place? 4. Does the state allow election workers to keep their personal information, including addresses, confidential? 5. Does the state have some kind of security or check for poll watchers that prohibits them from interfering with election officials? Code of conduct? 6. Does the state criminalize doxxing election officials' personal information online?	Each state was awarded a score from 0 to 3 for each indicator. If the state had the indicator, it received a score of 3 for it. If it didn't, it received a 0. For some indicators, some partial credit was given (see Appendix B for full scoring results). Indicators were treated equally in all cases. The average score across all indicators was calculated for each state and rounded to the nearest whole number. This value became the grade.

For election official intimidation, indicators were collected and scored using the Law Enforcement Quick Reference Guides from the Committee for Safe and Secure Elections and

databases from the National Conference of State Legislatures.[151,152,153] These sources compiled existing state laws that aim to prevent election official intimidation. Indicators were all weighed equally and ranged from 0 to 3. Partial credit was awarded in certain cases for four out of the six indicators if a state had some aspect of the indicator but not enough to mark it as a 3. Each state received an average score based on its indicator scores, which were then rounded to the nearest whole number. I chose to round the average scores because these indicators were scored with my subjective judgement and rounding allowed me to assign grades while avoiding false precision. This rounded value became the threat grade for each state.

Disinformation (Category 1)

Table 1d. *Indicators to Evaluate State Preparedness for Disinformation (Category 1)*

Indicators	Threat Grade Rubric
1. Does the state have a law regulating the use of AI-generated, misleading content about elections? 2. Does the state have a general law prohibiting giving voters **any** kind of false information about how elections are run?	**3**: Both indicators are met & AI law applies to general election information, not just a law against deepfakes.
	2: Both indicators are met and AI law only applies to deepfakes.
	1: Only one indicator is met.
	0: Zero indicators are met.

Disinformation (Category 1) was simpler than some of the other threats because there were only two indicators. The Brennan Center, the Movement Advancement Project, and Public Citizen were helpful in tracking legislation on AI laws and laws about false election

[151] Law Enforcement Quick Reference Guides, Committee for Safe and Secure Elections
[152] Poll Watchers and Challengers, 2024
[153] State Laws Providing Protection for Election Officials and Staff, 2024

administration.[154,155,156] All sources and legislation were double-checked to ensure that the information was accurate and up-to-date. A 3 was awarded to states that had both indicators met and AI laws which did not just apply to deepfakes. Other grades were assigned based on which components of the criteria a state was missing.

Foreign Interference

Table 1e. *Indicators to Evaluate State Preparedness for Foreign Interference*

Indicators	Threat Grade Rubric
1. Does the state have a law regulating the use of AI/deepfakes? 2. Does the state have laws prohibiting tampering with its voter registration system? 3. Does the state prohibit spending by foreign-influenced corporations? 4. Does the state prohibit foreign spending on state and local ballot measures?	**3**: All indicators are met.
	2: Three out of the four indicators are met.
	1: Two out of the four indicators are met.
	0: Zero to one of the four indicators are met.

Foreign interference indicators were collected using the Brennan Center, Public Citizen, and the Campaign Legal Center.[157,158,159] The grading scale was simply based on how many of the four indicators each threat met.

[154] Norden et al., 2024
[155] Protections Against Election Disinformation, 2025
[156] Tracker: State Legislation on Deepfakes in Elections, 2025
[157] Ibid.
[158] Norden et al., 2024
[159] Combatting Foreign Interference, Campaign Legal Center

Cybersecurity Concerns/Hacking

Table 1f. *Indicators to Evaluate State Preparedness for Cybersecurity Concerns/Hacking*

Indicators	Threat Grade Rubric
1. Does the state have laws against tampering with voting machines? 2. Does the state have laws against tampering with voter registration databases? 3. Does the state have a voting system where a majority of its districts use paper ballots with BMDs/DREs with VVPAT? 4. Does the state have zero jurisdictions that are using equipment that is over a decade old?	**3**: All indicators are met.
	2: Three out of the four indicators are met.
	1: Two out of the four indicators are met.
	0: Zero to one of the four indicators are met.

The grading scale used for foreign interference was the same one used for cybersecurity concerns and hacking. The information for those indicators came from information about state laws on government websites, Verified Voting, and the Brennan Center.[160,161] The grading scale for this threat was also based on the number of indicators that each state met.

[160] Election Day Equipment — November 2024, Verified Voting
[161] Edlin et al., 2024

Grades

Using these indicators and grading metrics, the threat scores were calculated for each threat and state. They can be viewed in Table 2.

Table 2. *Threat Grades with Unweighted Indicators*

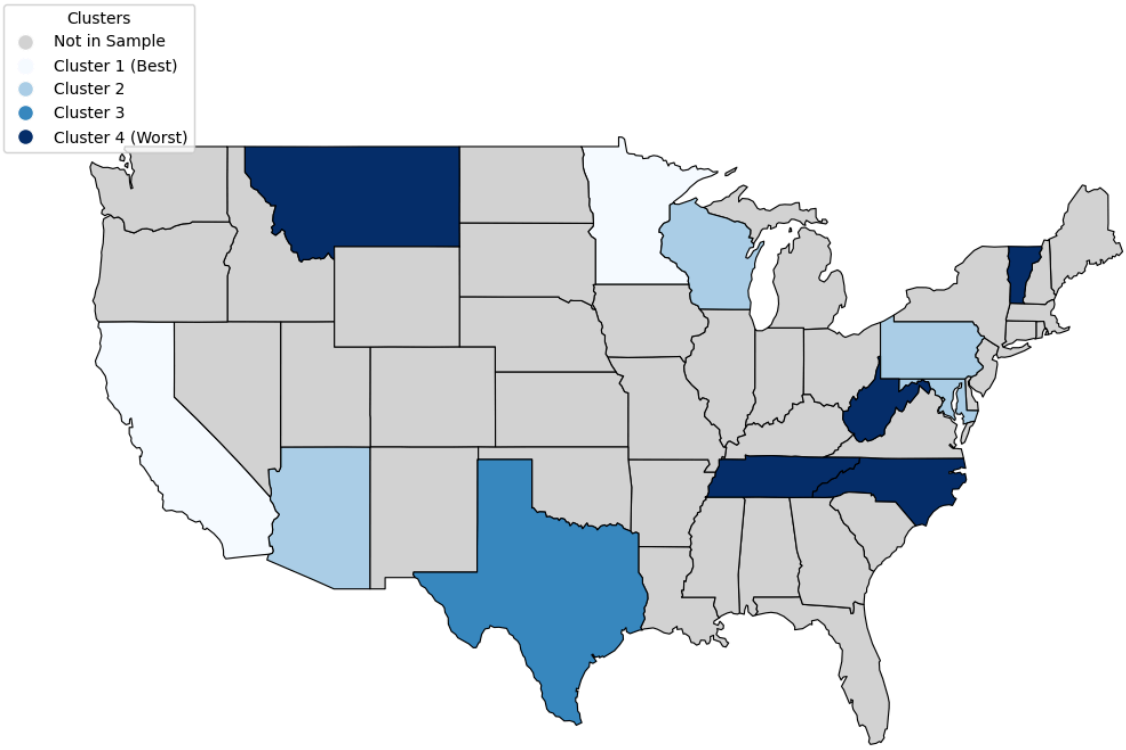
State	Election Officials Refusing to Certify	Voter Intimidation	Election Official Intimidation	Disinformation Category 1	Foreign Interference	Cybersecurity threats / Hacking
TN	2	2	1	1	0	1
TX	1	2	1	2	1	1
WV	2	1	1	0	0	2
MT	2	2	1	1	0	2
MN	2	3	2	2	2	2
CA	1	2	2	3	2	3
MD	1	2	2	1	1	3
VT	2	2	1	0	0	1
WI	1	2	1	1	1	2
AZ	2	2	2	1	1	2
NC	3	2	1	0	0	1
PA	1	2	1	1	0	3
Average Threat Grade Per Threat	**1.67**	**2**	**1.33**	**1.08**	**0.67**	**1.92**

K-Means

After the grades were scored for each indicator and state, I ran K-Means clustering on the results to group states into clusters with similar levels of preparedness. Using k = 4 (four

outputted clusters), I ran K-Means clustering a thousand times. I ran the procedure multiple times because K-Means can output completely different results each time it runs, so I wanted to ensure that each state was assigned to its most consistent cluster. Each time the algorithm ran, it placed each state into a cluster, and then the clusters were ranked by the average position of their cluster's center. The logic behind this is that clusters of states with stronger threat grades will also have higher centroid values. Each time K-Means ran, it also saved a complete list of cluster ranks for each state. Once K-Means finished running a thousand times, each state's mode rank was saved as their overall ranking. This means that a state's cluster was based on the ranking they received most often after all of the K-Means trials. Figure 1 highlights the results of this methodology.

Figure 1. *Mode Ranked Clusters for Each State Using Unweighted Indicators and K-Means*



Weighting the Indicators

After running this initial K-Means test, I introduced another procedure that I believed would result in more valid results. In the first attempt with this methodology, I gave equal weight to all indicators within each threat. However, I came to believe that this decision was flawed because certain indicators should be more influential on an overall threat grade, so they should not all be considered equal. After looking over my indicators for each threat, I decided to change the indicator weights for three threats: voter intimidation, election official intimidation, and cybersecurity concerns. Voter intimidation and election official intimidation had many indicators to consider, and some of them appeared to be much more impactful in preventing the threat than others. For cybersecurity concerns, one indicator stood out to me as being necessary for a state to have to have a grade of 2 or higher. So, I recalculated the threat grades for these threats and re-ran the K-Means clustering procedure.

Table 3a. *Using Weighted Indicators to Evaluate State Preparedness for Voter Intimidation*

State	Unweighted Indicators Grade	Weighted Indicators Grade
TN	2	2
TX	2	2
WV	1	2
MT	2	2
MN	3	3
CA	2	2
MD	2	2
VT	2	2
WI	2	1

AZ	2	3
NC	2	2
PA	2	2

In the unweighted version of voter intimidation, each indicator was scored from 0 to 3, the indicators were averaged, and that score was rounded to the nearest whole number for each state. These values can be seen in the second column of Table 3a. In the weighted indicator version of this analysis, I counted certain indicators twice. The indicators that I weighed more were: 1.) whether the state had specific anti-voter intimidation legislation, 2.) whether the state banned weapons at their polling places, and 3.) whether the state had restrictions on who could be at the polling place. I chose these indicators because I reasoned that they would be the most helpful in protecting voters at polling places since these indicators represent legislation that most directly minimizes the potential physical harm that can be inflicted on voters trying to cast their ballots. When I calculated the average score across all indicators, I simply counted the scores for these columns twice and continued with the same procedure used in the unweighted version. The new scores can be found in the third column of Table 3a. Only three scores changed from the unweighted version to the weighted version. West Virginia and Arizona scored higher, and Wisconsin scored lower.

Table 3b. *Using Weighted Indicators to Evaluate State Preparedness for Election Official Intimidation*

State	Unweighted Indicators Grade	Weighted Indicators Grade
TN	1	1
TX	1	1
WV	1	1
MT	1	1
MN	2	2
CA	2	2
MD	2	2
VT	1	1
WI	1	1
AZ	2	2
NC	1	1
PA	1	1

In the unweighted version of election official intimidation, each indicator was scored from 0 to 3, the indicators were averaged, and that score was rounded to the nearest whole number for each state. These values can be seen in the second column of Table 3b. In the weighted indicator version of this analysis, I counted certain indicators twice. The indicators I weighed more were: 1.) whether the state had an explicit ban on election official intimidation that applied to polling places and in public/online settings, 2.) whether the state banned weapons at their polling places, and 3.) whether the state allowed election workers to keep their information confidential. I chose these indicators because they most directly minimized the

chances of election officials being harmed at polling places or in their day-to-day lives. When I calculated the average score across all indicators, I simply counted the scores for these columns twice and continued with the same procedure used in the unweighted version. The scores can be found in the third column of Table 3b. None of the scores changed from the unweighted procedure to the weighted procedure.

Table 3c. *Weighted Indicators and Grading Criteria for Cybersecurity Concerns/Hacking*

Indicators	Grading Scale
1. Does the state have laws against tampering with voting machines? 2. Does the state have laws against tampering with voter registration databases? 3. Does the state have a voting system where a majority of its districts use paper ballots with BMDs/DREs with VVPAT? 4. Does the state have zero jurisdictions that are using equipment that is over a decade old?	**3**: All indicators are met.
	2: Indicator three is met, and two other indicators are met.
	1: Indicators three and/or four are met, and at least one other indicator is met.
	0: Zero to one indicators are met.

Table 3d. *Using Weighted Indicators to Evaluate State Preparedness for Cybersecurity Concerns/Hacking*

State	Unweighted Indicators Grade	Weighted Indicators Grade
TN	1	0
TX	1	0
WV	2	1
MT	2	2
MN	2	2
CA	3	3
MD	3	3
VT	1	1
WI	2	2
AZ	2	2
NC	1	1
PA	3	3

The weighted indicators version for cybersecurity concerns/hacking was different from the other weighted versions. Since I had fewer indicators, the process of weighing was much simpler. My four indicators for this threat were: 1.) whether the state had laws against tampering with voting machines; 2.) whether the state had laws against tampering with voter registration databases; 3.) whether the state had a voting system where a majority of its districts used paper ballots with BMDs/DREs with VVPAT; and 4.) whether the state had zero jurisdictions that were using equipment that is more than a decade old. After carefully considering all of those indicators, I reasoned that the third and fourth indicators were the most important because of the relative vulnerability of voting machines, and that the third was arguably the most impactful way

to protect voter machines because it would offer a way to verify election results through paper trails. The newly weighted grading mechanism based on this can be seen in Table 3c, and the scores can be found in the third column of Table 3d. Three scores changed between the unweighted indicators version and the weighted indicators version, and all the scores that changed were for Republican states. These states' grades went down, indicating that their preparedness to handle cybersecurity concerns and hacking declined when protections for voting machines were considered the most important.

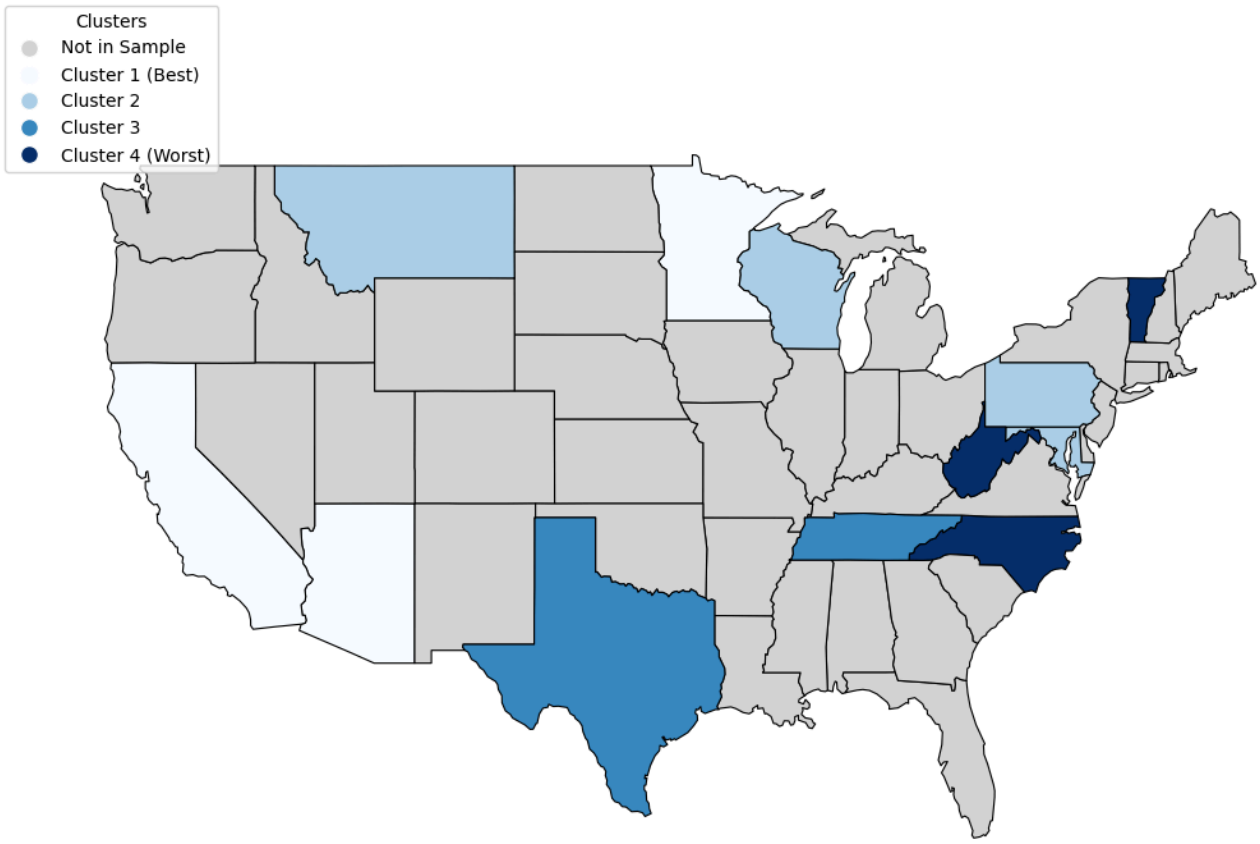
K-Means with Weighted Indicators

Table 4. *Threat Grades with Weighted Indicators*

State	Election Officials Refusing to Certify	Voter Intimidation	Election Official Intimidation	Disinfo Category 1	Foreign Interference	Cybersecurity threats / Hacking
TN	2	2	1	1	0	0
TX	1	2	1	2	1	0
WV	2	2	1	0	0	1
MT	2	2	1	1	0	2
MN	2	3	2	2	2	2
CA	1	2	2	3	2	3
MD	1	2	2	1	1	3
VT	2	2	1	0	0	1
WI	1	1	1	1	1	2
AZ	2	3	2	1	1	2
NC	3	2	1	0	0	1
PA	1	2	1	1	0	3

The threat grades based on weighted indicators can be found in Table 4. These values were then used to run K-Means clustering with k = 4. The procedure for K-Means was the same as the unweighted indicators version, and the results are shown in Figure 2.

Figure 2. *Mode Ranked Clusters for Each State Using Weighted Indicators and K-Means*



Discussion

General Clustering Results and Key Takeaways

The two different sets of K-Means clustering results were generally similar, though three states switched groups. This can be seen in Table 5 and Figure 3. Tennessee, Montana, and Arizona all placed into higher clusters compared to the initial ranking, and Montana was able to move up two cluster ranks. Every other state received the same cluster ranking, and no state moved down in their cluster ranking. These results show that when I weighed certain indicators more for voter intimidation, election official intimidation, and cybersecurity threats, Tennessee, Montana, and Arizona had stronger performances because they scored well on at least some of those indicators. Overall, the clusters stayed very similar and weighing certain indicators more improved some states' overall preparedness cluster.

Table 5: *Preparedness Clusters and Average Threat Grades for Each State*

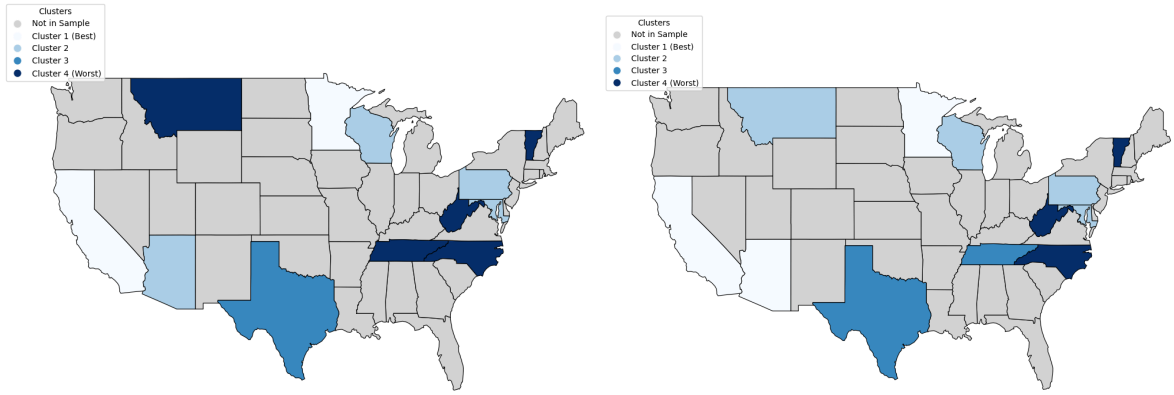
State	Mode K-Means Cluster (Unweighted Indicators)	Mode K-Means Cluster (Weighted Indicators)	Average Threat Score (Unweighted Indicators)	Average Threat Score (Weighted Indicators)
TN	Cluster 4	Cluster 3	1.17	1
TX	Cluster 3	Cluster 3	1.33	1.17
WV	Cluster 4	Cluster 4	1	1
MT	Cluster 4	Cluster 2	1.33	1.33
MN	Cluster 1	Cluster 1	2.17	2.17
CA	Cluster 1	Cluster 1	2.17	2.17
MD	Cluster 2	Cluster 2	1.67	1.67
VT	Cluster 4	Cluster 4	1	1
WI	Cluster 2	Cluster 2	1.33	1.17

AZ	Cluster 2	Cluster 1	1.67	1.83
NC	Cluster 4	Cluster 4	1.17	1.17
PA	Cluster 2	Cluster 2	1.33	1.33

Table 6: *Differences in Average Threat Grades for Threats Whose Indicators Were Weighed*

Threat	Average Threat Grade Across All U.S. States (Unweighted Indicators)	Average Threat Grade Across All U.S. States (Weighted Indicators)
Voter Intimidation	2	2.08
Election Official Intimidation	1.33	1.33
Cybersecurity concerns/Hacking	1.92	1.67

Figure 3. *Figures 1 and 2 Placed Together for Comparison (Figure 1 on the top)*



The three states that are considered the most prepared by this measure are Minnesota, Arizona, and California. Minnesota and California were placed in Cluster 1 in both renditions of the K-Means clustering, indicating that these two are the most prepared out of the 12 states in the sample. Arizona was in Cluster 2 initially and moved into Cluster 1 after the weighting, so it appears to be slightly less prepared than Minnesota and California but overall is still comparable

to those states. It likely was boosted to Cluster 1 after receiving a higher score for voter intimidation in the weighted version. All three of these states did very well and should be considered the most prepared states in the sample.

The states that were consistently in the middle for preparedness were Wisconsin, Pennsylvania, Maryland, Montana, Texas, and Tennessee. These states were grouped in either Cluster 2 or 3 for both K-Means procedures (with Montana as an exception), indicating these states did not score high enough to be considered in the top cluster for preparedness but they performed better than the states at the bottom. Wisconsin, Pennsylvania, and Maryland were in Cluster 2 both times, and Texas was in Cluster 3 both times. Tennessee was able to move into Cluster 3 in the weighted version after being in Cluster 4 initially.

Montana is an interesting case because it was able to move up two cluster ranks from Cluster 4 to Cluster 2. This was initially puzzling because Montana's threat grades did not change at all from the unweighted version to the weighted version. Furthermore, when Pennsylvania and Montana are compared, they have the same average threat grade both times (1.33), yet Pennsylvania was consistently in Cluster 2 and Montana was in Cluster 4 for the first round. However, after looking at the average threat scores per state in Table 5 and the average scores for each threat across all states in Table 6, there is a plausible explanation for this phenomenon. It is important to remember that this is a comparative analysis, so even though Montana's threat grades did not change, its clustering would be affected by other states' grades changing. The simplest explanation for why Montana's cluster rank changed so significantly is that it was boosted by having a grade of 2 for cybersecurity preparedness both times. In Table 8, it can be observed that the average threat grade across all states for cybersecurity concerns/hacking dropped significantly from unweighted to weighted indicators. This means that

states generally did not score as well when the indicators were weighted, and this means that Montana earning a higher score would be a boost for its overall cluster rating. This is likely why Montana was able to move up two cluster ranks. Since Pennsylvania scored a 3 for this threat both times, this likely kept it out of Cluster 4 for the initial clustering and provides a reason why it did not experience the same "jump" that Montana did. Overall, states scored lower across all threats in the weighted version compared to the unweighted version, and this may be why Arizona and Tennessee experienced smaller boosts to their preparedness cluster as well. If a state has a higher score compared to most other states for one of the threats with weighted indicators, then that is a significant advantage in K-Means clustering.

The remaining states were in the bottom cluster for preparedness for both sets of K-Means results, and these states were North Carolina, West Virginia, and Vermont. In comparison to the other states, these states were not as prepared and did not score as well in the threat grades. Based on the clusters and the average threat grades per state in Table 7, the final preparedness ranking of the states is as follows:

1. Minnesota and California
2. Arizona
3. Maryland
4. Pennsylvania
5. Wisconsin
6. Montana
7. Texas
8. Tennessee
9. North Carolina
10. West Virginia and Vermont

The clear pattern that emerges from the K-Means is that Democratic-leaning states and swing states are more prepared than Republican-leaning states to face intentional threats to election administration. The top six most prepared states in the sample were all

Democratic-leaning or swing states, and all four of the Republican states were in the bottom half of the ranked states. These results demonstrate a partisan trend in what kinds of states are the most prepared and the ones that are the least prepared. Democratic-leaning states were the most prepared out of all the other partisan groups. Both states in the top ranking for preparedness were Democratic-leaning, and overall they had the best average ranking (3.75) compared to swing states (5) and Republican-leaning states (7.75). Swing states performed relatively well, which was generally expected. Since swing states have more contentious elections, they likely have to handle more occurrences of these threats and therefore have a stronger infrastructure in place to handle them. Republican states had the weakest performance in this measure, indicating that they have fewer measures in place to prepare them for election administration threats compared to the other groups of states.

Limitations and Future Work

One key limitation of this study was that I simply did not have the time to collect data on all 50 states in the time frame I had to write this senior thesis. While a 12-state sample was enough to see a partisan pattern in the results, it is difficult to assess whether this trend extends to all of the U.S. In the future, I would like to revisit this study and collect data on all 50 states to see if I observe the same pattern and how the results change.

Another limitation of this work is that there are some threats where a state cannot fully protect itself. I mentioned this before in the methodology section as justification for leaving out two of the threats that were discussed in the literature review: candidates refusing to concede and disinformation (category 2). It was also the reason why this analysis was comparative and focused on how states scored compared to each other, rather than assessing states based on how prepared they would be to stop these threats in a perfect world. These threats that are difficult to police have one thing in common: the Internet. States do not have a lot of control over what is said and done in online spaces, and this is increasingly becoming an issue for election administration as trust in elections dwindles and disinformation runs rampant. Americans have the ability to refuse to concede an election and spread false information online, and there is not much a state can do to stop that. Foreign countries are also capable of doing this, which is an aspect of foreign interference that a state can only do so much to prevent. If states were able to fully defend themselves against every threat and all threats could be included in the analysis, then these final results would be much more compelling in demonstrating which states are actually the most prepared to defend themselves and protect their election administration.

In the future, I would also like to add more indicators to each threat to cover more ways that these threats can occur and how states can stop them. Time constraints also played a role

here and stopped me from exploring more indicators, so I hope to revisit this project and research other indicators that might be relevant to this analysis. It would also be nice to try out different methodologies other than K-Means to see how different states are grouped. Finally, I would also like to experiment with feature analysis to see which indicators and threats are the most important to the overall preparedness score after researching all 50 states.

Conclusion

In this study, I identified eight threats to election administration, described their scope and past occurrences, collected indicators that were used to create threat grades to assess preparedness, and ran K-Means clustering on a sample of 12 states to look for patterns in the states that were the most and least prepared to handle these threats. While I had to exclude two of my threats from my methodology and results, I still discovered a partisan pattern in my results. My results indicate that the Republican states in my sample are generally less prepared than Democratic and swing states. Since swing states have had more competitive elections and more exposure to the impacts of these threats, I conclude that this is an important reason why these states are more prepared. It is unclear why Democratic-leaning states performed the best, though my work demonstrates that these states have invested more in protecting their systems of election administration and generally received higher threat grades compared to other states. Future work should explore the causal mechanisms behind this partisan phenomenon.

This work is increasingly relevant and important as the U.S. experiences significant democratic backsliding. Elections and their administration are an important safeguard that protects American democracy, and they are set to become even more contentious as traditional norms of institutional forbearance and mutual toleration erode. These threats have the ability to upend our elections and threaten the democratic principles that govern our political system. While it may seem reassuring that swing states are generally in the best position to counter many of these threats, it is crucial for each state to have strong protection mechanisms because they could potentially have contested elections in the future. Every state's electoral process must have the necessary resources and enacted legislation to handle these potential problems that could

prevent a fair election from being carried out. It is crucial that states are able to defend themselves against these intentional acts for the health of American elections and democracy.

References

1. American Psychological Association. “Misinformation and Disinformation,” July 2022. https://www.apa.org/topics/journalism-facts/misinformation-disinformation.
2. Baker, Turquoise, Lawrence Norden, Warren Stewart, and Megan Maier. “Voting Machines at Risk in 2022.” The Brennan Center, March 1, 2022. https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-2022.
3. Bauder, David, Randall Chase, and Geoff Mulvihill. “Fox, Dominion Reach $787M Settlement over Election Claims.” *The Associated Press*, April 18, 2023. https://apnews.com/article/fox-news-dominion-lawsuit-trial-trump-2020-0ac71f75acfacc52ea80b3e747fb0afe.
4. Bauer, Scott. “Wisconsin Republican Eric Hovde Concedes Defeat to Democrat Tammy Baldwin in US Senate Race.” *The Associated Press*, November 18, 2024. https://apnews.com/article/wisconsin-senate-hovde-baldwin-recount-0af5107044b5fa2c24fe99e6d7ab5271.
5. *BBC*. “Trump Sides with Russia against FBI at Helsinki Summit.” July 16, 2018. https://www.bbc.com/news/world-europe-44852812.
6. Becker, David. “2020 Voter Registration Database Security Report: A Report from the Center for Election Innovation & Research.” The Center for Election Innovation & Research, August 2020.
7. Becker, David, Jacob Kipp, Jack R. Williams, and Jenny Lovell. “Voter Registration Database Security: A Research Report from the Center for Election Innovation & Research.” The Center for Election Innovation & Research, September 2018.
8. Bell, Peter. “Public Trust in Government: 1958-2024.” Pew Research Center, June 24, 2024. https://www.pewresearch.org/politics/2024/06/24/public-trust-in-government-1958-2024/.
9. Benkler, Yochai, Casey Tilton, Bruce Etling, Hal Roberts, Justin Clark, Robert Faris, Jonas Kaiser, and Carolyn Schmitt. “Mail-In Voter Fraud: Anatomy of a Disinformation Campaign.” *The Berkman Klein Center for Internet & Society at Harvard University*, October 8, 2020.
10. Bentele, Keith, and Erin O’Brien. “Jim Crow 2.0? Why States Consider and Adopt Restrictive Voter Access Policies.” *Perspectives on Politics* 11 (2013): 1088–1116. https://doi.org/10.1017/s1537592713002843.
11. Bock Clark, Doug. “Some Election Officials Refused to Certify Results. Few Were Held Accountable.” *ProPublica*, March 9, 2023. https://www.propublica.org/article/election-officials-refused-certify-results-few-held-accountable.
12. Brennan Center for Justice. “How States Can Prevent Election Subversion in 2024 and beyond | Brennan Center for Justice,” March 28, 2024. https://www.brennancenter.org/our-work/policy-solutions/how-states-can-prevent-election-subversion-2024-and-beyond.
13. Brunner, Jim. “Loren Culp, Refusing to Concede Washington Gubernatorial Race, Turns on Top Republicans.” *The Seattle Times*, November 21, 2020. https://www.seattletimes.com/seattle-news/politics/loren-culp-refusing-to-concede-washington-gubernatorial-race-turns-on-top-republicans/.

14. Cabral, Sam. “US Accuses Russia of 2024 Election Interference.” *BBC*, September 4, 2024. https://www.bbc.com/news/articles/c8rx28v1vpro.
15. Campaign Legal Center. “Combatting Foreign Interference,” 2025. https://campaignlegal.org/democracyu/transparency/combatting-foreign-interference.
16. Campaign Legal Center. “Protecting Voters from Intimidation,” n.d. https://campaignlegal.org/democracyu/inclusion/protecting-voters-intimidation.
17. Canon, David, and Owen Sherman. “Debunking the ‘Big Lie’: Election Administration in the 2020 Presidential Election.” *Presidential Studies Quarterly* 51, no. 3 (May 15, 2021): 546–81. https://doi.org/10.1111/psq.12721.
18. Cassidy, Christina A., and Ali Swenson. “Federal Agencies Say Russia and Iran Are Ramping up Influence Campaigns Targeting US Voters.” *The Associated Press*, November 5, 2024. https://apnews.com/article/election-misinformation-presidential-race-russia-iran-ab8ed2baadbb02364a4becff6d38f4f5.
19. Clayton, James. “Elon Musk Claims He’s Buying Twitter to ‘Help Humanity.’” *BBC*, October 27, 2022. https://www.bbc.com/news/business-63408384.
20. Codrington III, Wilfred. “Can Members of the Electoral College Choose Who They Vote For?” Brennan Center for Justice, 2020.
21. Cohen, Zachary. “Georgia Judge Rejects Lawsuit from GOP Officials Raising Concerns about Voting Machines.” *CNN*, October 4, 2024. https://www.cnn.com/2024/10/04/politics/georgia-judge-rejects-lawsuit-gop-officials-dominion/index.html.
22. Cohen, Zachary, and Jeremy Herb. “Intelligence Report Contradicts Claims by Trump and His Team on China Election Interference.” *CNN*, March 17, 2021. https://www.cnn.com/2021/03/17/politics/us-intel-report-trump-china-election-interference-claims/index.html.
23. Cohen, Zachary, Sean Lyngaas, and Sara Murray. “Election Officials Are Outmatched by Elon Musk’s Misinformation Machine.” *CNN*, October 31, 2024. https://www.cnn.com/2024/10/31/politics/election-officials-outmatched-elon-musk-misinformation/index.html.
24. Collier, Kevin. “Musk’s Election Falsehoods Travel Hundreds of Times Further on X than Fact-Checks from Officials.” *NBC News*, October 25, 2024. https://www.nbcnews.com/tech/misinformation/musk-election-misinformation-x-officials-twitter-voting-rcna176938.
25. Columbia Law. “To Combat Election Subversion in 2024, Look to State Constitutions,” 2024. https://www.law.columbia.edu/news/archive/combat-election-subversion-2024-look-state-constitutions.
26. Committee for Safe and Secure Elections. “Law Enforcement Quick Reference Guides,” n.d. https://safeelections.org/referenceguides/.
27. Cooper, Jonathan J. “Lake Refuses to Concede in Arizona Governor’s Race She Lost.” *The Associated Press*, November 17, 2022. https://apnews.com/article/2022-midterm-elections-arizona-phoenix-government-and-politics-bcea98345ee81ec1b8fa6a5364bc296f.
28. Corasaniti, Nick. “Trump Supporters Disrupt Early Voting in Virginia.” *Fairfax County Times*, September 21, 2000.

https://www.fairfaxtimes.com/articles/trump-supporters-disrupt-early-voting-in-virginia/article_be07dda0-fc55-11ea-b8ab-4b39670e4fe8.html.

29. Corasaniti, Nick, Karen Yourish, and Keith Collins. "How Trump's 2020 Election Lies Have Gripped State Legislatures." *The New York Times*, May 22, 2022. https://www.nytimes.com/interactive/2022/05/22/us/politics/state-legislators-election-denial.html.
30. Dilanian, Ken. "Bipartisan Senate Report Says 2017 Intel Assessment about Russian Interference and Trump Was Accurate." *NBC News*, April 21, 2020. https://www.nbcnews.com/politics/national-security/bipartisan-senate-report-says-2017-intel-assessment-about-russian-interference-n1188696.
31. Durkee, Alison. "Smartmatic Settles With Newsmax: Here's Where It And Dominion's Other Lawsuits Stand." *Forbes*, September 26, 2024. https://www.forbes.com/sites/alisondurkee/2024/09/26/smartmatic-goes-to-trial-against-newsmax-today-heres-where-it-and-dominions-other-lawsuits-stand/.
32. Edlin, Ruby, Megan Maier, and Warren Stewart. "Costs for Replacing Voting Equipment in 2024." The Brennan Center, February 7, 2024. https://www.brennancenter.org/our-work/analysis-opinion/costs-replacing-voting-equipment-2024.
33. Edlin, Ruby, and Lawrence Norden. "Poll of Election Officials Finds Concerns about Safety, Political Interference." Brennan Center for Justice, 2024. https://www.brennancenter.org/our-work/analysis-opinion/poll-election-officials-finds-concerns-about-safety-political.
34. Eichensehr, Kristen E., ed. "Government Agencies and Private Companies Undertake Actions to Limit the Impact of Foreign Influence and Interference in the 2020 U.S. Election." *Cambridge University Press* 115, no. 2 (April 19, 2021): 309–17. https://doi.org/10.1017/ajil.2021.10.
35. "Election Certification Processes and Guardrails." The Brennan Center, September 18, 2024. https://www.brennancenter.org/our-work/research-reports/election-certification-processes-and-guardrails.
36. Estes, Adam Clark. "We're All Living inside Elon Musk's Misinformation Machine Now." *Vox*, November 7, 2024. https://www.vox.com/technology/383336/trump-election-elon-musk-misinformation.
37. "FBI Statement on Bomb Threats to Polling Locations," November 5, 2024. https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations.
38. Ferrer, Joshua, Daniel Thompson, and Rachel Orey. "Election Official Turnover Rates from 2000-2024," 2024. https://bipartisanpolicy.org/report/election-official-turnover-rates-from-2000-2024/.
39. "Foreign Threats to the 2020 US Federal Elections." Office of National Intelligence, March 10, 2021. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.
40. Frenkel, Sheera, Tiffany Hsu, and Steven Lee Myers. "How Russia, China and Iran Are Interfering in the Presidential Election." *The New York Times*, October 29, 2024. https://www.nytimes.com/2024/10/29/technology/election-interference-russia-china-iran.html.
41. Friel, Katie, and Jasleen Singh. "Voter Intimidation and Election Worker Intimidation Resource Guide." Brennan Center for Justice, 2022. https://www.brennancenter.org/our-work/research-reports/voter-intimidation-and-election-worker-intimidation-resource-guide.

42. Fung, Brian. “How Republicans Pushed Social Media Companies to Stop Fighting Election Misinformation.” *CNN*, October 21, 2024. https://www.cnn.com/2024/10/21/politics/election-social-media-misinformation-republicans/index.html.
43. Garrett, Major. “Election Officials Say Threats Are Escalating Ahead of 2024 Vote: ‘A Heightened State of Anxiety’.” *CBS News*, September 10, 2024. https://www.cbsnews.com/amp/news/2024-election-worker-threats/.
44. Gibson, Brittany, and John Sakellariadis. “Public Officials, Election Workers Are Facing ‘Unprecedented’ Wave of Threats, Monaco Says - Live Updates - POLITICO.” *Politico*, September 17, 2024. https://www.politico.com/live-updates/2024/09/17/politico-ai-and-tech-summit/unprecedented-threats-violence-election-workers-monaco-00179591.
45. Hasen, Richard. “Identifying and Minimizing the Risk of Election Subversion and Stolen Elections in the Contemporary United States.” *Harvard Law Review Forum* 135 (2022). https://doi.org/10.2139/ssrn.3926381.
46. Hicks, William, Seth McKee, and Daniel Smith. “A Bipartisan Election Reform? Explaining Support for Online Voter Registration in the American States.” *American Politics Research* 44 (2016): 1008–36. https://doi.org/10.1177/1532673x16661818.
47. Holpuch, Amanda. “Roy Moore Issues Fiery Video Refusing to Concede: ‘Immorality Sweeps over Our Land.’” *The Guardian*, December 14, 2017. https://www.theguardian.com/us-news/2017/dec/14/roy-moore-issues-fiery-video-refusing-to-concede-immorality-sweeps-over-our-land.
48. *How I Hacked an Election*. The New York Times: University of Michigan, 2018. https://www.youtube.com/watch?v=w8eujrTyRRE.
49. Hurt, Emma. “Trump Hasn’t Conceded Georgia. Neither Did Stacey Abrams. What Changed?” *NPR*, November 18, 2020. https://www.npr.org/2020/11/18/935734198/trump-hasnt-conceded-georgia-neither-did-stacey-abrams-what-changed.
50. Jingnan, Huo. “Foreign Influence Efforts Reached a Fever Pitch during the 2024 Elections.” *NPR*, November 12, 2024. https://www.npr.org/2024/11/09/nx-s1-5181965/2024-election-foreign-influence-russia-china-iran.
51. Johnson, Darin E.W. “Russian Election Interference and Race-Baiting.” *Columbia Journal of Race and Law* 9, no. 2 (2019): 191–264.
52. Johnson, Kevin, and David Jackson. “Election Workers Fear Trouble, Boost Security as Vengeful Threats Persist after Trump Loss.” *USA TODAY*, October 9, 2022. https://www.usatoday.com/story/news/politics/2022/10/09/midterm-elections-2022-poll-workers-fears/10460917002/.
53. Jones, Bradley. “Many Americans Unaware of Their States’ Voter ID Laws.” Pew Research Center, October 24, 2016. https://www.pewresearch.org/short-reads/2016/10/24/many-americans-unaware-of-their-states-voter-id-laws/.
54. Keyssar, Alexander. “Know-Nothings, Radicals, and Redeemers.” In *The Right to Vote: The Contested History of Democracy in the United States*. Basic Books, 2000.

55. Klepper, David, and Eric Tucker. “Iranian Hackers Tried but Failed to Interest Biden’s Campaign in Stolen Trump Info, FBI Says.” *The Associated Press*, September 18, 2024. https://apnews.com/article/iran-fbi-election-interference-dni-ae96f57f438772dac08e076be7aa4904.
56. Leingang, Rachel. “‘We’re Watching You’: Incidents of Voter Intimidation Rise as Midterm Elections Near.” *The Guardian*, November 4, 2022. https://www.theguardian.com/us-news/2022/nov/04/voter-intimidation-midterm-elections-arizona.
57. Levin, Dov H. “Should We Worry about Partisan Electoral Interventions? The Nature, History, and Known Effects of Foreign Interference in Elections.” In *Defending Democracies: Combating Foreign Election Interference in a Digital Age*. Oxford University Press, 2021.
58. Levitsky, Steven, and Daniel Ziblatt. *How Democracies Die*. Crown, 2018.
59. ———. *Tyranny of the Minority*. Crown, 2023.
60. Liptak, Kevin. “Trump Uses Dark Message to Kick off RNC despite Aides’ Claims of Optimism.” *CNN*, August 24, 2020. https://www.cnn.com/2020/08/24/politics/trump-nomination-rnc/index.html.
61. Long, Colleen. “Dominion Voting Sues Fox for $1.6B over 2020 Election Claims.” *The Associated Press*, March 26, 2021. https://apnews.com/article/joe-biden-donald-trump-media-lawsuits-elections-912eea8e168f95d51dec02da78ac2760.
62. Luhby, Tami, Eric Levenson, and Jeremy Herb. “Voting Nationwide Has Been Mostly Orderly, despite Non-Credible Bomb Threats from Russian Origin.” *CNN*, November 5, 2024. https://www.cnn.com/2024/11/05/politics/voting-security-election-day/index.html.
63. Marcellino, William, Christian Johnson, Marek N. Posard, and Todd C. Helmus. “Foreign Interference in the 2020 Election.” RAND Corporation, October 8, 2020.
64. Marley, Patrick, Colby Itkowitz, and Yvonne Winget Sanchez. “Two Republicans Who Lost Senate Races Refuse to Concede.” *The Washington Post*, November 14, 2024. https://www.washingtonpost.com/politics/2024/11/14/concession-eric-hovde-kari-lake/.
65. Mauger, Craig. “Police Investigating Flashing Light System Installed at Michigan Ballot Drop Box.” *The Detroit News*, March 5, 2024. https://www.detroitnews.com/story/news/politics/2024/03/05/plymouth-township-michigan-flashing-light-system-set-up-at-ballot-drop-box-voter-intimidation/72857469007/.
66. McCartney, Alyssa. “The President Who Cried Voter Fraud: A Recurring Theme of Baseless Allegations.” *UMass Law Review* 17, no. 1 (January 2022). https://scholarship.law.umassd.edu/umlr/vol17/iss1/3/.
67. McDonald, Michael. *From Pandemic to Insurrection*. De Gruyter, 2022.
68. McNamara, Audrey. “Trump Spreads Baseless Claim about Dominion Voting Systems after Losing Election.” *CBS News*, November 13, 2020. https://www.cbsnews.com/news/trump-dominion-voting-systems-false-accusation/.
69. Miller Karalunas, Lauren. “How State and Local Election Certification Works.” State Court Report, July 30, 2024. https://statecourtreport.org/our-work/analysis-opinion/how-state-and-local-election-certification-works.
70. Minnete, Lorraine. *The Myth of Voter Fraud*. Cornell University Press, 2010.
71. Movement Advancement Project. “Protections Against Election Disinformation,” 2025. https://www.lgbtmap.org/democracy-maps/protections_against_election_disinformation.

72. Muller, Derek T. “Election Subversion and the Writ of Mandamus.” *William & Mary Law Review* 65, no. 2 (2023).
73. Nakashima, Ellen. “Russia’s Election Influence Efforts Show Sophistication, Officials Say.” *The Washington Post*, September 7, 2024. https://www.washingtonpost.com/national-security/2024/09/07/russia-election-covert-disinformation-doj/.
74. National Archives. “About the Electors.” Government, August 27, 2019. https://www.archives.gov/electoral-college/electors#selection.
75. National Conference of State Legislatures. “Election Administration at State and Local Levels,” December 22, 2023. https://www.ncsl.org/elections-and-campaigns/election-administration-at-state-and-local-levels.
76. National Conference of State Legislatures. “Election Certification Deadlines,” January 20, 2025. https://www.ncsl.org/elections-and-campaigns/election-certification-deadlines.
77. National Conference of State Legislatures. “Electioneering Prohibitions Near Polling Places,” September 12, 2024. https://www.ncsl.org/elections-and-campaigns/electioneering-prohibitions.
78. National Conference of State Legislatures. “Poll Watchers and Challengers,” October 9, 2024. https://www.ncsl.org/elections-and-campaigns/poll-watchers-and-challengers.
79. National Conference of State Legislatures. “Risk-Limiting Audits,” September 6, 2024. https://www.ncsl.org/elections-and-campaigns/risk-limiting-audits.
80. National Conference of State Legislatures. “State Laws Providing Protection for Election Officials and Staff,” October 18, 2024. https://www.ncsl.org/elections-and-campaigns/state-laws-providing-protection-for-election-officials-and-staff.
81. National Conference of State Legislatures. “Table 9: Ballot Drop Box Laws,” January 13, 2025. https://www.ncsl.org/elections-and-campaigns/table-9-ballot-drop-box-laws.
82. Nguyen, Tina, and Mark Scott. “How ‘SharpieGate’ Went from Online Chatter to Trumpworld Strategy in Arizona.” *Politico*, November 5, 2020. https://www.politico.com/news/2020/11/05/sharpie-ballots-trump-strategy-arizona-434372.
83. Norden, Lawrence, and Christopher Famighetti. “America’s Voting Machines at Risk.” Brennan Center for Justice, 2015.
84. Norden, Lawrence, Niyati Narang, and Laura J. Protzmann. “States Take the Lead in Regulating AI in Elections — Within Limits.” The Brennan Center, August 7, 2024. https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits.
85. Ottoboni, Kellie, and Philip B. Stark. “Election Integrity and Electronic Voting Machines in 2018 Georgia, USA.” *E-Vote-ID 2019 Proceedings*, July 24, 2019.
86. Parks, Miles. “Trump, While Attacking Mail Voting, Casts Mail Ballot Again.” *NPR*, August 19, 2020. https://www.npr.org/2020/08/19/903886567/trump-while-attacking-mail-voting-casts-mail-ballot-again.
87. Persily, Nathaniel, and Charles Stewart III. “The Miracle and Tragedy of the 2020 U.S. Election.” *Journal of Democracy* 32, no. 2 (April 2021): 159–78.
88. Pistone, Ann, and Jason Knowles. “AI Deepfakes, Voting Misinformation, Fake Fundraisers and Other 2024 Election Scams Ramp Up.” *ABC7 Chicago*, October 14, 2024. https://abc7chicago.com/post/ai-deepfakes-voting-misinformation-fake-fundraisers-other-2024-election-scams-ramp-day-nears/15429430/.

89. Prochaska, Stephen, Kayla Duskin, Zarine Kharazian, Carly Minow, Stephanie Blucker, Sylvie Venuto, Jevin West, and Kate Starbird. “Mobilizing Manufactured Reality: How Participatory Disinformation Shaped Deep Stories to Catalyze Action during the 2020 U.S. Presidential Election.” *Proceedings of the ACM on Human-Computer Interaction* 7 (April 16, 2023): 1–39. https://doi.org/10.1145/3579616.
90. Public Citizen. “Tracker: State Legislation on Deepfakes in Elections,” 2025. https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/.
91. Rodriguez, Barbara, and Jennifer Gerson. “More States Move to Restrict Guns at Polling Sites to Protect Workers, Voters from Threats.” *PBS News*, April 7, 2024. https://www.pbs.org/newshour/politics/more-states-move-to-restrict-guns-at-polling-sites-to-protect-workers-voters-from-threats.
92. Rogers, Kaleigh. “Republicans Are Ramping up Election Fraud Claims Ahead of November.” *ABC News*, May 29, 2024. https://abcnews.go.com/538/republicans-ramping-election-fraud-claims-ahead-november/story?id=110640715.
93. Sanger, David E. “Obama Strikes Back at Russia for Election Hacking.” *The New York Times*, December 29, 2016. https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.
94. Sanger, David E., and Catie Edmondson. “Russia Targeted Election Systems in All 50 States, Report Finds.” *The New York Times*, July 25, 2019. https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html.
95. Schor, Elana, Andrew Restuccia, and Cory Bennett. “US Imposes New Sanctions on Russian Entities over 2016 Election Meddling.” *Politico*, March 15, 2018. https://www.politico.eu/article/donald-trump-russia-us-imposes-new-sanctions-on-over-2016-election-meddling/.
96. Schreiner, Bruce. “Beshear Claims Victory in Kentucky but Bevin Refuses to Concede.” *PBS*, November 6, 2019. https://www.pbs.org/newshour/politics/beshear-claims-victory-in-kentucky-but-bevin-refuses-to-concede.
97. Shane, Scott, and Sheera Frenkel. “Russian 2016 Influence Operation Targeted African-Americans on Social Media.” *The New York Times*, December 17, 2018. https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html.
98. Sharma, Karishma, Emilio Ferrara, and Yan Liu. “Characterizing Online Engagement with Disinformation and Conspiracies in the 2020 U.S. Presidential Election.” *Proceedings of the International AAAI Conference on Web and Social Media* 16 (2022). https://doi.org/10.1609/icwsm.v16i1.19345.
99. Shearer, Elisa, Sarah Naseer, Jacob Liedke, and Katerina Eva Matsa. “How Americans Get News on TikTok, X, Facebook and Instagram.” Pew Research Center, June 12, 2024. https://www.pewresearch.org/journalism/2024/06/12/how-americans-get-news-on-tiktok-x-facebook-and-instagram/.
100. Shimer, David. *Rigged: America, Russia, and One Hundred Years of Covert Electoral Interference*. Alfred A. Knopf, 2020.
101. Sonner, Scott, Rio Yamat, and Nicholas Riccardi. “Top Election Official in Nevada County That Is Key to the Presidential Race Takes Stress Leave.” *The Associated Press*, September 2024. https://apnews.com/article/nevada-2024-election-clerk-washoe-county-voting-eb7842bd5b80e86418c50a4e3673980e.

102. Stewart III, Charles. "Voting Technologies." *Annual Review of Political Science* 14 (2011): 353–78.
103. Sullivan, Eileen. "Election Workers Face Flood of Threats, but Charges Are Few." *The New York Times*, April 13, 2024. https://www.nytimes.com/2024/04/13/us/politics/election-workers-threats.html.
104. Sullivan, Kristin, Kyle Upchurch, Kyle Yoder, April Tan, Stefan Martinez-Ruiz, and Kira Flemke. "2022 Voter Registration Database Security Report." The Center for Election Innovation & Research, January 2023.
105. Suri, Jeremi. "The History of Foreign Election Interference and an Alternative Future." In *Our Nation at Risk: Election Integrity as a National Security Issue*. New York University Press, 2024.
106. Sweren-Becker, Eliza, and Jasleen Singh. "Guide to Laws Against Intimidation of Voters and Election Workers." Brennan Center for Justice, June 18, 2024. https://www.brennancenter.org/our-work/research-reports/guide-laws-against-intimidation-voters-and-election-workers.
107. Tang, Terry. "Judge Orders Armed Group Away from Arizona Ballot Drop Boxes." *The Associated Press*, November 2, 2022. https://apnews.com/article/2022-midterm-elections-arizona-phoenix-5353cfd0774727e6dd03bdbf48c12211 .
108. ———. "Kari Lake Loses Suit to See Ballot Envelopes in 3rd Trial Tied to Arizona Election Defeat." *The Associated Press*, November 30, 2023. https://apnews.com/article/kari-lake-voting-ballot-envelopes-trial-b6ee658a0d20922e7a15bf9e2a62f394.
109. The Center for Election Innovation & Research. "Securing Voter Registration Databases: 2024 Survey Preliminary Results," September 2024. https://electioninnovation.org/research/2024-vrdb-security-pre-election-snapshot/.
110. The Cook Political Report. "2022 Cook PVI: State Map and List," n.d. https://www.cookpolitical.com/cook-pvi/2022-partisan-voting-index/state-map-and-list.
111. Thomas, Morgan. "Election Technology Through the Years." The Council of State Governments, November 8, 2023. https://www.csg.org/2023/11/08/election-technology-through-the-years/.
112. United States Attorney's Office Southern District of New York. "U.S. Attorney Announces Charges Against Two Iranian Nationals For Cyber-Enabled Disinformation And Threat Campaign Designed To Interfere With The 2020 U.S. Presidential Election," November 18, 2021. https://www.justice.gov/usao-sdny/pr/us-attorney-announces-charges-against-two-iranian-nationals-cyber-enabled.
113. U.S. Department of the Treasury. "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks." Government, March 15, 2018. https://home.treasury.gov/news/press-releases/sm0312.
114. Verified Voting. "Election Day Equipment — November 2024," 2024. https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2024.
115. Watts, Clint, and Rachel Chernaskey. "Foreign Influence in the 2020 U.S. Presidential Election: More Actors, But Less Effective." *Orbis* 65, no. 2 (2021). https://doi.org/10.1016/j.orbis.2021.03.008.
116. Zakrzewski, Cat. "Election Workers Brace for a Torrent of Threats: "I KNOW WHERE YOU SLEEP"." *The Washington Post*, November 8, 2022. https://www.washingtonpost.com/technology/2022/11/08/election-workers-online-threats/.

117. Zetter, Kim. “The Crisis of Election Security.” *The New York Times*, September 26, 2018. https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html.
118. ———. “The Myth of the Hacker-Proof Voting Machine.” *The New York Times*, February 21, 2018. https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html.

Appendix A. *Voter Intimidation Indicator Scores*

Indicator	VRA	Specific anti VI legislation	Drop off sites/ballot boxes (1 pt if they don't exist, 2 pt if there's a ban on electioneering but not specific intimidation)	Weapons at polling place (2 pt if just firearms, 1.5 pt if just school grounds, 1 pt if just schools and firearms)	Restrictions on who can be at polling place	Poll Watcher Behavior Restrictions on VI (1.5 if code of conduct exists but nothing explicit about not communicating to voters)	Electioneering Outside polling place (1.5 if just about general campaigning)
TN	0	3	1	1.5	3	3	3
TX	0	3	1	3	3	3	1.5
WV	0	3	1	1.5	3	0	0
MT	0	3	1	1.5	0	3	3
MN	3	3	2	1.5	3	3	3
CA	3	3	3	2	0	3	3
MD	0	3	2	2	0	3	1.5
VT	0	3	2	2	0	1.5	3
WI	0	3	2	1	0	3	1.5
AZ	0	3	2	3	3	3	3
NC	0	3	1	1	0	3	3
PA	0	3	2	1.5	3	0	3

Appendix B. *Election Official Intimidation Indicator Scores*

Indicator	EOI explicit ban applicable to polling places and online/personal settings (2 pts if only one is covered, 1 pt if just election meetings covered)	Poll Workers = protected election workers (1.5 pts if not said explicitly)	Weapons at polling place (2 pts if just firearms, 1.5 pts if just school grounds, 1 pt if just schools and firearms)	Election workers allowed to keep info confidential	Poll Watcher Behavior Restrictions on EOI (1.5 pts if code of conduct exists but nothing explicit about not interfering with election officials)	Criminalizing doxxing
TN	2	0	1.5	0	3	0
TX	1	0	3	0	3	0
WV	3	1.5	1.5	0	0	0
MT	2	0	1.5	0	1.5	0
MN	3	1.5	1.5	0	1.5	3
CA	3	3	2	3	3	0
MD	3	1.5	2	0	3	0
VT	3	0	2	0	3	0
WI	0	0	1	0	3	0
AZ	2	0	3	3	3	3
NC	2	1.5	1	0	3	0
PA	3	0	1.5	0	0	0

Appendix C. *Indicator Sources*

Sources for Election Officials Refusing to Certify Indicators

1. "Arizona Election Certification Processes and Guardrails." Brennan Center for Justice, September 18, 2024. https://www.brennancenter.org/our-work/research-reports/arizona-election-certification-processes-and-guardrails.
2. casetext. "Ariz. R. Civ. P. 70," n.d. https://casetext.com/rule/arizona-court-rules/rules-of-civil-procedure-for-the-superior-courts-of-arizona/provisional-and-final-remedies-special-proceedings/rule-70-enforcing-a-judgment-for-a-specific-act#:~:text=Rule%2070%20%2D%20Enforcing%20a%20Judgment%20for%20a%20Specific%20Act%20(a,Act%3B%20Ordering%20Another%20to%20Act.
3. casetext. "Cal. Code Civ. Proc. § 1097," n.d. https://casetext.com/statute/california-codes/california-code-of-civil-procedure/part-3-of-special-proceedings-of-a-civil-nature/title-1-of-writs-of-review-mandate-and-prohibition/chapter-2-writ-of-mandate/section-1097-refusal-or-neglect-to-obey-peremptory-mandate.
4. casetext. "Tex. R. Civ. P. 308," n.d. https://casetext.com/rule/texas-court-rules/texas-rules-of-civil-procedure/part-ii-rules-of-practice-in-district-and-county-courts/section-11-trial-of-causes/judgments/rule-308-court-shall-enforce-its-decrees#:~:text=The%20court%20shall%20cause%20its,for%20the%20seizure%20and%20delivery.
5. casetext. "Vt. R. Civ. P. 70," n.d. https://casetext.com/rule/vermont-court-rules/vermont-rules-of-civil-procedure/viii-provisional-and-final-remedies-and-special-proceedings/rule-70-judgment-for-specific-acts-vesting-title.
6. "Election Certification Processes and Guardrails." The Brennan Center, September 18, 2024. https://www.brennancenter.org/our-work/research-reports/election-certification-processes-and-guardrails.
7. FindLaw. "California Code, Code of Civil Procedure - CCP § 128," n.d. https://codes.findlaw.com/ca/code-of-civil-procedure/ccp-sect-128/.
8. FindLaw. "California Code, Code of Civil Procedure - CCP § 717.010," n.d. https://codes.findlaw.com/ca/code-of-civil-procedure/ccp-sect-717-010/.
9. Maryland Courts. "Maryland Rule 2-648," n.d. https://www.mdcourts.gov/sites/default/files/import/rules/rodocs/152ro.pdf.
10. Minnesota Legislature. "Rule 70.Judgment for Specific Acts; Vesting Title," n.d. https://www.revisor.mn.gov/court_rules/cp/id/70/.
11. Montana State Legislature. "Rule 70. Enforcing A Judgment For A Specific Act," n.d. https://archive.legmt.gov/bills/mca/title_0250/chapter_0200/part_0080/section_0700/0250-0200-0080-0700.html.
12. Muller, Derek T. "Election Subversion and the Writ of Mandamus." *William & Mary Law Review* 65, no. 2 (2023).
13. "North Carolina Election Certification Processes and Guardrails." Brennan Center for Justice, September 18, 2024. https://www.brennancenter.org/our-work/research-reports/north-carolina-election-certification-processes-and-guardrails.
14. North Carolina General Assembly. "N.C. Gen. Stat. § 163–182.5(c) - Canvassing Votes." Government, n.d. https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_163/GS_163-182.5.pdf.
15. North Carolina General Assembly. "Rule 70. Judgment for Specific Acts; Vesting Title," n.d. https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_1A/GS_1A-1,_Rule_70.pdf.

16. “Pennsylvania Election Certification Processes and Guardrails.” Brennan Center for Justice, September 18, 2024. https://www.brennancenter.org/our-work/research-reports/pennsylvania-election-certification-processes-and-guardrails.
17. Tennessee Courts. “Rule 70: Judgment For Specific Acts; Vesting Title,” https://www.tncourts.gov/rules/rules-civil-procedure/70.
18. West Virginia Legislature. “RULES OF CIVIL PROCEDURE,” n.d. https://www.wvlegislature.gov/wvcode/magrules_htm/rules%20of%20civil%20procedure.htm.
19. “Wisconsin Election Certification Processes and Guardrails.” Brennan Center for Justice, September 18, 2024. https://www.brennancenter.org/our-work/research-reports/wisconsin-election-certification-processes-and-guardrails.
20. Wisconsin State Legislature. “Wis. Stat. §§ 785.01(1), 785.02,” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/785/02.

Sources for Voter Intimidation Indicators

1. Arizona State Legislature. “13-3102. Misconduct Involving Weapons; Defenses; Classification; Definitions,” n.d. https://www.azleg.gov/ars/13/03102.htm.
2. Arizona State Legislature. “16-1006. Changing Vote of Elector by Corrupt Means or Inducement; Classification,” n.d. https://www.azleg.gov/ars/16/01006.htm.
3. Arizona State Legislature. “16-1008. Election Officer Changing Vote of Elector by Menace or Reward; Classification,” n.d. https://www.azleg.gov/ars/16/01008.htm.
4. Arizona State Legislature. “16-1013. Coercion or Intimidation of Elector; Classification,” n.d. https://www.azleg.gov/ars/16/01013.htm.
5. Arizona State Legislature. “16-1018. Additional Unlawful Acts by Persons with Respect to Voting; Classification,” n.d. https://www.azleg.gov/ars/16/01018.htm.
6. Brennan Center for Justice. “Texas: Protections Against Intimidation of Voters and Election Workers,” October 25, 2024. https://www.brennancenter.org/our-work/research-reports/texas-protections-against-intimidation-voters-and-election-workers.
7. California Legislature. “AB-2642 Elections: Intimidation / PEACE Act,” n.d. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2642.
8. California Legislature. “Voting Rights Act - California Legislative Information,” n.d. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB182.
9. Campaign Legal Center. “PROTECTING ARIZONANS FROM VOTER INTIMIDATION,” 2024. https://campaignlegal.org/sites/default/files/2024-03/Protecting%20Arizonans%20from%20Voter%20Intimidation_1.pdf.
10. Campaign Legal Center. “PROTECTING PENNSYLVANIANS FROM VOTER INTIMIDATION,” 2024. https://campaignlegal.org/sites/default/files/2024-03/Protecting%20Pennsylvanians%20from%20Voter%20Intimidation_0.pdf.
11. Campaign Legal Center. “PROTECTING WISCONSINITES FROM VOTER INTIMIDATION,” 2024. https://campaignlegal.org/sites/default/files/2024-03/IntimidationMemo-WI-r2%20%281%29.pdf.
12. casetext. “25 Pa. Stat. § 3060,” n.d. https://casetext.com/statute/pennsylvania-statutes/statutes-unconsolidated/title-25-ps-elections-electoral-districts/chapter-14-election-code/article-xii-preparation-for-and-conduct-of-primaries-and-elections/section-3060-regulations-in-force-at-polling-places.
13. casetext. “Cal. Elec. Code § 18540,” n.d. https://casetext.com/statute/california-codes/california-elections-code/division-18-penal-provisions/chapter-

6-corruption-of-the-voting-process/article-3-intimidation-of-voters/section-18540-unlawful-threat-to-induce-or-compel-person-to-vote-or-refrain-from-voting.

14. Committee for Safe and Secure Elections. "ARIZONA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-AZ-Pocket-Guide-2024.pdf.
15. Committee for Safe and Secure Elections. "CALIFORNIA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-CA-Pocket-Guide-2024.pdf.
16. Committee for Safe and Secure Elections. "MARYLAND 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-MD-Pocket-Guide-2024.pdf.
17. Committee for Safe and Secure Elections. "MINNESOTA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-MN-Pocket-Guide-2024.pdf.
18. Committee for Safe and Secure Elections. "MONTANA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-MT-Pocket-Guide-2024.pdf.
19. Committee for Safe and Secure Elections. "NORTH CAROLINA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-NC-Pocket-Guide-2024.pdf.
20. Committee for Safe and Secure Elections. "PENNSYLVANIA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-PA-Pocket-Guide-2024.pdf.
21. Committee for Safe and Secure Elections. "TENNESSEE 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-TN-Pocket-Guide-2024-.pdf.
22. Committee for Safe and Secure Elections. "TEXAS 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-TX-Pocket-Guide-2024.pdf.
23. Committee for Safe and Secure Elections. "VERMONT 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-VT-Pocket-Guide-2024.pdf.
24. Committee for Safe and Secure Elections. "WEST VIRGINIA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE," 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-WV-Pocket-Guide-2024.pdf.
25. Committee for Safe and Secure Elections. "Wis. Stat. § 7.37," n.d. https://docs.legis.wisconsin.gov/statutes/statutes/7/i/37.
26. Maryland General Assembly. "2023 Regular Session - Senate Bill 1 Chapter," n.d. https://mgaleg.maryland.gov/2023RS/chapters_noln/Ch_680_sb0001E.pdf.
27. Maryland State Board of Elections. "2024 Voter Intimidation Guidance Memo," 2024. https://elections.maryland.gov/press_room/documents/2024%20Voter%20Intimidation%20Guidance%20Memo.pdf.
28. Minnesota Legislature. "HF 4772," n.d. https://www.revisor.mn.gov/bills/bill.php?b=house&f=hf4772&ssn=0&y=2024.
29. Minnesota Legislature. "Sec. 211B.07 MN Statutes," n.d. https://www.revisor.mn.gov/statutes/cite/211B.07.
30. Minnesota Legislature. "Sec. 211B.075 MN Statutes," n.d. https://www.revisor.mn.gov/statutes/cite/211B.075.
31. National Conference of State Legislatures. "Electioneering Prohibitions Near Polling Places," September 12, 2024. https://www.ncsl.org/elections-and-campaigns/electioneering-prohibitions.

32. National Conference of State Legislatures. “Poll Watchers and Challengers,” October 9, 2024. https://www.ncsl.org/elections-and-campaigns/poll-watchers-and-challengers.
33. National Conference of State Legislatures. “Table 9: Ballot Drop Box Laws,” January 13, 2025. https://www.ncsl.org/elections-and-campaigns/table-9-ballot-drop-box-laws.
34. West Virginia Code. “§3-1-37. Restrictions on Presence and Conduct at Polls.,” n.d. https://code.wvlegislature.gov/3-1-37/.
35. Wisconsin State Legislature. “Wis. Stat. § 7.41,” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/7/i/41.
36. Wisconsin State Legislature. “Wis. Stat. § 12.09,” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/12/09.
37. Wisconsin State Legislature. “Wis. Stat. §12.13(3)(x),” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/12/13/3/x.
38. Wisconsin State Legislature. “Wis. Stat, 948.605,” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/948/605#:~:text=Wisconsin%20Legislature%3A%20948.605&text=(a)%20A%20child%20obtains%20the,to%20himself%2C%20herself%20or%20another.
39. Wisconsin State Legislature. “Wis. Stat. Ann. § 12.03,” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/12/03#:~:text=427.-,12.03%20Campaigning%20restricted.,be%20cast%20at%20those%20locations.
40. Wisconsin State Legislature. “Wis. Stat. Ann. § 12.035,” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/12#:~:text=12.035%20Posting%20and%20distribution%20of,12.05%20False%20representations%20affecting%20elections.
41. Wisconsin State Legislature. “Wis. Stat. Ann. § 941.235,” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/941/iii/235#:~:text=To%20%E2%80%9Cgo%20armed%E2%80%9D%20does%20not,Keith%2C%20175%20Wis.

Sources for Election Official Intimidation Indicators

1. Arizona State Legislature. “13-2401. Personal Information on the Internet; Exception; Classification; Definitions,” n.d. https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/13/02401.htm.
2. Arizona State Legislature. “13-3102. Misconduct Involving Weapons; Defenses; Classification; Definitions,” n.d. https://www.azleg.gov/ars/13/03102.htm.
3. Arizona State Legislature. “16-1004. Interference with or Corruption of Election Officer; Interference with Voting Equipment; Violation; Classification,” n.d. https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/16/01004.htm.
4. California Legislature Information. “Cal. Elec Code § 2166.8,” n.d. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=ELEC&division=2.&title=&part=&chapter=2.&article=4.
5. casetext. “Cal. Elec. Code § 18502,” n.d. https://casetext.com/statute/california-codes/california-elections-code/division-18-penal-provisions/chapter-6-corruption-of-the-voting-process/article-1-general-provisions/section-18502-unlawful-interference-with-canvass-or-election.
6. Committee for Safe and Secure Elections. “ARIZONA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-AZ-Pocket-Guide-2024.pdf.
7. Committee for Safe and Secure Elections. “CALIFORNIA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-CA-Pocket-Guide-2024.pdf.

8. Committee for Safe and Secure Elections. “MARYLAND 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-MD-Pocket-Guide-2024.pdf.
9. Committee for Safe and Secure Elections. “MINNESOTA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-MN-Pocket-Guide-2024.pdf.
10. Committee for Safe and Secure Elections. “MONTANA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-MT-Pocket-Guide-2024.pdf.
11. Committee for Safe and Secure Elections. “NORTH CAROLINA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-NC-Pocket-Guide-2024.pdf.
12. Committee for Safe and Secure Elections. “PENNSYLVANIA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-PA-Pocket-Guide-2024.pdf.
13. Committee for Safe and Secure Elections. “TENNESSEE 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-TN-Pocket-Guide-2024-.pdf.
14. Committee for Safe and Secure Elections. “TEXAS 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-TX-Pocket-Guide-2024.pdf.
15. Committee for Safe and Secure Elections. “VERMONT 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-VT-Pocket-Guide-2024.pdf.
16. Committee for Safe and Secure Elections. “WEST VIRGINIA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-WV-Pocket-Guide-2024.pdf.
17. Committee for Safe and Secure Elections. “WISCONSIN 2025 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” n.d. https://safeelections.org/wp-content/uploads/2024/08/CSSE-WI-Pocket-Guide-2024.pdf.
18. LexisNexis. “Md. Election Law Code Ann. § 16-205,” n.d. https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=bad80271-c6cf-4ff6-b571-416f35ca269b&nodeid=AANAAQAACAAF&nodepath=%2FROOT%2FAAN%2FAANAAQ%2FAANAAQAAC%2FAANAAQAACAAF&level=4&haschildren=&populated=false&title=%C2%A7+16-205.+Interfering+with+election+officials.&config=014EJAA2ZmE1OTU3OC0xMGRjLTRlNTctOTQ3Zi0wMDE2MWFhYzAwN2MKAFBvZENhdGFsb2e9wg3LFiffInanDd3V39aA&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A63SM-VVV1-DYB7-W3XS-00008-00&ecomp=6gf5kkk&prid=4f91c385-d81f-4813-84b4-7aaecb4176d8.
19. LexisNexis. “Tenn. Code Ann. § 2-19-101,” 2025. https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=f98a4c07-8b29-48e7-8f33-444da42acd87&nodeid=AACAATAABAAB&nodepath=%2fROOT%2fAAC%2fAACAAT%2fAACAATAAB%2fAACAATAABAAB&level=4&haschildren=&populated=false&title=2-19-101.+Interfering+with+nominating+meeting+or+election.&config=025054JABlOTJjNmIyNi0wYjI0LTRjZGEtYWE5ZC0zNGFhOWNhMjFlNDgKAFBvZENhdGFsb2cDFQ14bX2GfyBTaI9WcPX5&pddocfullpath=%2fshared%2fdocument%2fstatutes-legislation%2furn%3acontentItem%3a4X8J-6910-R03J-J28H-00008-00&ecomp=6gf5kkk&prid=ed08c8f0-8dde-41d6-ac03-4774240498e2.
20. Minnesota Legislature. “Sec. 211B.076 MN Statutes,” n.d. https://www.revisor.mn.gov/statutes/cite/211B.076.

21. Montana State Legislature. “Interference With Election Officials Or Election Workers,” n.d. https://archive.legmt.gov/bills/mca/title_0130/chapter_0350/part_0020/section_0030/0130-0350-0020-0030.html.
22. National Conference of State Legislatures. “Poll Watchers and Challengers,” October 9, 2024. https://www.ncsl.org/elections-and-campaigns/poll-watchers-and-challengers.
23. National Conference of State Legislatures. “State Laws Providing Protection for Election Officials and Staff,” January 13, 2025. https://www.ncsl.org/elections-and-campaigns/state-laws-providing-protection-for-election-officials-and-staff.
24. North Carolina General Assembly. “§ 163-274. Certain Acts Declared Misdemeanors,” n.d. https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_163/GS_163-274.pdf.
25. North Carolina General Assembly. “§ 163-275. Certain Acts Declared Felonies,” n.d. https://www.ncleg.gov/EnactedLegislation/Statutes/HTML/BySection/Chapter_163/GS_163-275.html.
26. Vermont General Assembly. “The Vermont Statutes Online,” n.d. https://legislature.vermont.gov/statutes/section/13/039/01702.
27. West Virginia Code. “§3-9-10. Disorder at Polls; Prevention; Failure to Assist in Preventing Disorder; Penalties,” n.d. https://code.wvlegislature.gov/3-9-10/.
28. Westlaw. “§ 16-904. Threat to Harm an Election Official,” n.d. https://govt.westlaw.com/mdc/Document/N268806F0F74F11EE82B0C699FBD8E33A?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default).

Sources for Disinformation Category 1 Indicators

1. Arizona State Legislature. “2023 Assembly BILL 664,” n.d. https://azleg.gov/legtext/56leg/2R/bills/SB1359S.pdf.
2. Arizona State Legislature. “HB 2394,” n.d. https://www.azleg.gov/legtext/56leg/2r/bills/hb2394p.htm.
3. casetext. “Tex. Elec. Code § 276.013,” n.d. https://casetext.com/statute/texas-codes/election-code/title-16-miscellaneous-provisions/chapter-276-miscellaneous-offenses-and-other-provisions/section-276013-election-fraud.
4. Committee for Safe and Secure Elections. “MINNESOTA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-MN-Pocket-Guide-2024.pdf.
5. FindLaw. “California Code, Elections Code - ELEC § 18543,” 2023. https://codes.findlaw.com/ca/elections-code/elec-sect-18543.html.
6. FindLaw. “Maryland Code, Election Law § 16-101,” 2021. https://codes.findlaw.com/md/election-law/md-code-elec-law-sect-16-101.html.
7. Governor Gavin Newsom. “Governor Newsom Signs Bills to Combat Deepfake Election Content,” September 17, 2024. https://www.gov.ca.gov/2024/09/17/governor-newsom-signs-bills-to-combat-deepfake-election-content/.
8. Justia. “2021 Tennessee Code Title 2 - Elections Chapter 19 - Prohibited Practices Part 1 - Prohibited Practices Generally § 2-19-133. False or Misleading Information Regarding Voting,” n.d. https://law.justia.com/codes/tennessee/2021/title-2/chapter-19/part-1/section-2-19-133/.
9. Minnesota Legislature. “HF 1370 3rd Engrossment - 93rd Legislature (2023 - 2024),” n.d. https://www.revisor.mn.gov/bills/text.php?number=HF1370&type=bill&version=3&session=ls93&session_year=2023&session_number=0.
10. Minnesota Legislature. “HF 4772 1st Engrossment - 93rd Legislature (2023 - 2024),” n.d. https://www.revisor.mn.gov/bills/text.php?number=HF4772&type=bill&version=1&session=ls93&session_year=2024&session_number=0.

11. Minnesota Legislature. “Sec. 204C.035 MN Statutes,” n.d. https://www.revisor.mn.gov/statutes/cite/204C.035.
12. Montana State Legislature. “Incorrect Election Procedures Information,” n.d. https://archive.legmt.gov/bills/mca/title_0130/chapter_0350/part_0020/section_0350/0130-0350-0020-0350.html.
13. Movement Advancement Project. “Protections Against Election Disinformation,” 2025. https://www.lgbtmap.org/democracy-maps/protections_against_election_disinformation.
14. Norden, Lawrence, Niyati Narang, and Laura J. Protzmann. “States Take the Lead in Regulating AI in Elections — Within Limits.” Brennan Center for Justice, August 7, 2024. https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits.
15. Public Citizen. “Tracker: State Legislation on Deepfakes in Elections,” 2025. https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/.
16. Texas Legislature Online. “SB 751,” n.d. https://capitol.texas.gov/BillLookup/History.aspx?LegSess=86R&Bill=SB751.
17. Wisconsin State Legislature. “2023 Assembly BILL 664,” n.d. https://docs.legis.wisconsin.gov/2023/related/proposals/ab664.

Sources for Foreign Interference Indicators

1. Arizona State Legislature. “13-2316. Computer Tampering; Venue; Forfeiture; Classification,” n.d. https://www.azleg.gov/ars/13/02316.htm.
2. Ballotpedia. “Laws Governing Foreign Spending in Ballot Measure Campaigns,” 2025. https://ballotpedia.org/Laws_governing_foreign_spending_in_ballot_measure_campaigns.
3. California Legislative Information. “California Code, PEN 502.,” n.d. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=502.&lawCode=PEN.
4. Campaign Legal Center. “Combatting Foreign Interference,” 2025. https://campaignlegal.org/democracyu/transparency/combatting-foreign-interference.
5. Committee for Safe and Secure Elections. “TENNESSEE 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-TN-Pocket-Guide-2024-.pdf.
6. FindLaw. “California Code, Government Code - GOV § 85320,” 2023. https://codes.findlaw.com/ca/government-code/gov-sect-85320.html#:~:text=(a)%20A%20foreign%20government%20or,of%20a%20candidate%20to%20state.
7. FindLaw. “Maryland Code, Criminal Law § 7-302,” 2021. https://codes.findlaw.com/md/criminal-law/md-code-crim-law-sect-7-302/#:~:text=(a)(1)%20In%20this,computer%20system%2C%20or%20computer%20network.
8. FindLaw. “Maryland Code, Election Law § 13-236.1,” 2021. https://codes.findlaw.com/md/election-law/md-code-elec-law-sect-13-236-1.html.
9. FindLaw. “West Virginia Code Chapter 61. Crimes and Their Punishment § 61-3C-6. Unauthorized Possession of Computer Data or Programs,” 2024. https://codes.findlaw.com/wv/chapter-61-crimes-and-their-punishment/wv-code-sect-61-3c-6.html.
10. Minnesota Legislature. “6th Engrossment - 93rd Legislature (2023 - 2024),” n.d. https://www.revisor.mn.gov/bills/text.php?number=HF3&type=bill&version=6&session=ls93&session_year=2023&session_number=0.
11. Minnesota Legislature. “Sec. 609.891 MN Statutes,” n.d. https://www.revisor.mn.gov/statutes/cite/609.891#:~:text=609.891%20UNAUTHORIZED%20COMPUTER%20ACCESS.&text=A%20person%20is%20guilty%20of,security%20system%20or%20electronic%20terminal.

12. Montana State Legislature. “Tampering With Public Records Or Information,” n.d. https://archive.legmt.gov/bills/mca/title_0450/chapter_0070/part_0020/section_0080/0450-0070-0020-0080.html#:~:text=45%2D7%2D208.,public%20records%20or%20information%2C%20MCA.
13. Norden, Lawrence, Niyati Narang, and Laura J. Protzmann. “States Take the Lead in Regulating AI in Elections — Within Limits.” Brennan Center for Justice, August 7, 2024. https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits.
14. North Carolina General Assembly. “Chapter 14 - Article 60,” n.d. https://www.ncleg.net/enactedlegislation/statutes/html/byarticle/chapter_14/article_60.html.
15. Pennsylvania General Assembly. “Title 18 - PA General Assembly,” n.d. https://www.legis.state.pa.us/cfdocs/legis/LI/consCheck.cfm?txtType=HTM&ttl=18&div=0&chpt=76&sctn=11&subsctn=0.
16. Public Citizen. “Tracker: State Legislation on Deepfakes in Elections,” 2025. https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/.
17. Texas Constitution and Statutes. “PENAL CODE CHAPTER 33. COMPUTER CRIMES,” n.d. https://statutes.capitol.texas.gov/docs/pe/htm/pe.33.htm#:~:text=33.02.,effective%20consent%20of%20the%20owner.&text=(2)%20the%20computer%2C%20computer,or%20a%20critical%20infrastructure%20facility.
18. Wisconsin State Legislature. “943.70 Computer Crimes,” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/943/iii/70.

Sources for Cybersecurity concerns/Hacking Indicators

1. Arizona State Legislature. “13-2316. Computer Tampering; Venue; Forfeiture; Classification,” n.d. https://www.azleg.gov/ars/13/02316.htm.
2. California Legislative Information. “California Code, PEN 502.,” n.d. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=502.&lawCode=PEN.
3. Committee for Safe and Secure Elections. “ARIZONA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-AZ-Pocket-Guide-2024.pdf.
4. Committee for Safe and Secure Elections. “CALIFORNIA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-CA-Pocket-Guide-2024.pdf.
5. Committee for Safe and Secure Elections. “MARYLAND 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-MD-Pocket-Guide-2024.pdf.
6. Committee for Safe and Secure Elections. “MINNESOTA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-MN-Pocket-Guide-2024.pdf.
7. Committee for Safe and Secure Elections. “PENNSYLVANIA 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-PA-Pocket-Guide-2024.pdf.
8. Committee for Safe and Secure Elections. “TENNESSEE 2024 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” 2024. https://safeelections.org/wp-content/uploads/2024/08/CSSE-TN-Pocket-Guide-2024-.pdf.
9. Committee for Safe and Secure Elections. “WISCONSIN 2025 LAW ENFORCEMENT QUICK REFERENCE GUIDE,” n.d. https://safeelections.org/wp-content/uploads/2024/08/CSSE-WI-Pocket-Guide-2024.pdf.

10. Edlin, Ruby, Megan Maier, and Warren Stewart. “Costs for Replacing Voting Equipment in 2024.” Brennan Center for Justice, February 7, 2024. https://www.brennancenter.org/our-work/analysis-opinion/costs-replacing-voting-equipment-2024.
11. FindLaw. “Maryland Code, Criminal Law § 7-302,” 2021. https://codes.findlaw.com/md/criminal-law/md-code-crim-law-sect-7-302/#:~:text=(a)(1)%20In%20this,computer%20system%2C%20or%20computer%20network.
12. FindLaw. “West Virginia Code Chapter 61. Crimes and Their Punishment § 61-3C-6. Unauthorized Possession of Computer Data or Programs,” 2024. https://codes.findlaw.com/wv/chapter-61-crimes-and-their-punishment/wv-code-sect-61-3c-6.html.
13. Minnesota Legislature. “Sec. 609.891 MN Statutes,” n.d. https://www.revisor.mn.gov/statutes/cite/609.891#:~:text=609.891%20UNAUTHORIZED%20COMPUTER%20ACCESS.&text=A%20person%20is%20guilty%20of,security%20system%20or%20electronic%20terminal.
14. Montana State Legislature. “Tampering With Election Records And Information,” n.d. https://archive.legmt.gov/bills/mca/title_0130/chapter_0350/part_0020/section_0050/0130-0350-0020-0050.html.
15. Montana State Legislature. “Tampering With Public Records Or Information,” n.d. https://archive.legmt.gov/bills/mca/title_0450/chapter_0070/part_0020/section_0080/0450-0070-0020-0080.html#:~:text=45%2D7%2D208.,public%20records%20or%20information%2C%20MCA.
16. National Conference of State Legislatures. “State Statutes Prohibiting Tampering with Voting Systems,” March 20, 2024. https://www.ncsl.org/elections-and-campaigns/state-statutes-prohibiting-tampering-with-voting-systems.
17. North Carolina General Assembly. “Chapter 14 - Article 60,” n.d. https://www.ncleg.net/enactedlegislation/statutes/html/byarticle/chapter_14/article_60.html.
18. Pennsylvania General Assembly. “Title 18 - PA General Assembly,” n.d. https://www.legis.state.pa.us/cfdocs/legis/LI/consCheck.cfm?txtType=HTM&ttl=18&div=0&chpt=76&sctn=11&subsctn=0.
19. Texas Constitution and Statutes. “PENAL CODE CHAPTER 33. COMPUTER CRIMES,” n.d. https://statutes.capitol.texas.gov/docs/pe/htm/pe.33.htm#:~:text=33.02.,effective%20consent%20of%20the%20owner.&text=(2)%20the%20computer%2C%20computer,or%20a%20critical%20infrastructure%20facility.
20. Verified Voting. “Election Day Equipment — November 2024,” 2024. https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2024.
21. West Virginia Code. “§3-4A-33,” n.d. https://code.wvlegislature.gov/3-4A-33/.
22. Wisconsin State Legislature. “943.70 Computer Crimes,” n.d. https://docs.legis.wisconsin.gov/statutes/statutes/943/iii/70.