2

Hacking Elections

Contemporary Developments in Historical Perspective

Andrew Grotto and Ashray Narayan

Nowhere in the text of the U.S. Constitution is there an explicit reference to an affirmative right to vote. And yet, the Constitution and its amendments contain numerous provisions relating to the *integrity* of elections – what counts as a valid or legitimate electoral process. For the Framers of the Constitution, election integrity was fundamentally about ensuring that, if elections were held, only qualified persons could vote. As state legislatures and especially the Congress incrementally ruled out voting discrimination on the basis of whether a person owned land, was Black or another minority, was female, or was over eighteen years of age, those whose political fortunes were adversely affected by the expanding electorate have exploited features and bugs in the elections architecture of American democracy to uphold their own vision of election integrity – and in the process, disenfranchise eligible voters and influence election outcomes. Their tools have included poll taxes, literacy tests, identification requirements, residency conditions, disenfranchisement for certain criminal convictions, and a range of other measures.

The argument we advance in this contribution is that the twenty-first-century challenge of safeguarding elections from cyber threats must be understood as part of this history, and not solely as a niche engineering or information security problem. Especially since the 2016 presidential election, which brought cybersecurity risks to elections into the mainstream, political discourse about the magnitude of these risks and how best to mitigate them has become wrapped up in ideological conflict about who the threat actors are and what they aim to accomplish. It is against this backdrop of intensifying ideological conflict about the integrity and legitimacy of democratic procedures that efforts in 2016 and its aftermath to address cyber risks have occurred.

In information security, a hacker is someone who uses their skills and knowledge of digital systems to solve problems or achieve desired outcomes, even if it means subverting those systems by exploiting a vulnerability to undermine the confidentiality, integrity, or availability of the system or its information. Confidentiality ensures that systems and information are accessible only to authorized individuals or entities; it involves protecting systems and information from unauthorized access or disclosure. Integrity focuses on maintaining the accuracy, completeness, and trustworthiness of a system or information. It ensures that data remain unaltered, complete, and reliable. Availability ensures that systems and information are accessible and usable when needed. It involves protecting against disruptions, outages, or denial of service attacks that may render systems or data inaccessible.

Hackers may don a metaphorical white, black, or gray hat, depending on whether their actions and goals are rightful, wrongful, or somewhere in between. Rightful actions consist of compliance with legal and ethical norms concerning hacking and use of information technologies; a rightful motivation is identifying and responsibly showcasing vulnerabilities so that they can be fixed ("patched"). Wrongful actions and motivations consist of illegal or unethical conduct or goals. Gray hat hackers may employ illegal or unethical means to achieve rightful ends, or otherwise straddle a line between good and bad.

We port this concept over to election integrity and its preoccupation with hackers of a different kind: political hackers who use their skills and knowledge of law, psychology, and democratic procedures to subvert those procedures in pursuit of their political interests. Political hackers could be white, black, or gray hatted. Civil rights activists of the 1950s and 1960s like John Lewis are prototypical white hat hackers.

We begin with a review of American electoral history through 2016, with a focus on conceptions of election integrity and perceived threats to integrity. We then review developments that occurred between the 2016 and the 2020 presidential election cycles – an especially sensitive period for both election integrity generally and cybersecurity of elections specifically – with a focus on efforts to enhance the resilience of election infrastructure against cyber threats. As we shall see, the debate about the resilience of election infrastructure against cyber threats is at risk of becoming polarized along familiar themes from the history of American elections, with progressives viewing the principal threats as a combination of voter suppression by Republicans and their ideological allies and conservatives viewing voter fraud – people voting who are not eligible to vote – as the principal threat.

CONSTITUTIONAL FOUNDATIONS OF THE ELECTORAL PROCESS

Elections are abundant in American democracy and are held for certain federal, state, and local government offices. The constitution gives Congress the power to regulate how elections are held for these offices and specifies the qualifications and procedures for elections for the legislative and executive branches. It does not, however, dictate to the states which offices at the state and local levels are to be filled by elected or appointed officials.

The constitution was negotiated over four months in 1787 and ratified by the states in 1789. Among the fifty-five delegates that the states had sent to negotiate on their behalf in 1787, there was cynicism about the compatibility of universal suffrage – the idea that all free adults, which at the time usually meant free White men could vote[1] – with their vision of a constitutional order that safeguarded the individual rights of propertied White men against populist forces that could be manipulated by malign actors. Most of the Framers, as these delegates came to be known, preferred to eliminate the vulnerability by restricting voting privileges to White property owners. James Madison expressed apprehension about the potential influence of populist appeals on the less affluent classes and argued that limiting voting to the wealthy was essential for preserving Republican liberty and election integrity. Similarly, Gouverneur Morris, the author of the preamble to the constitution, voiced the belief that the ignorant and dependent could not be trusted to act in the public interest, drawing a comparison to children (Klarman, 2016).

Benjamin Franklin was among the dissenters; he argued against constitutional restrictions on the franchise based on wealth (Klarman, 2016). He highlighted the significant contributions of the commoners in the fight for American independence and pointed out that the decisions of the wealthy were susceptible to external influences as well. In the end, Franklin's view prevailed, with its rhetorical weight backed by the mathematics of ratification: Voting practices in many states had already extended suffrage beyond landowners, and expecting these voters to approve a constitution that would then strip them of their right to vote seemed wholly unrealistic. The Framers therefore left the responsibility of determining voting rights to the individual states. However, they devised a system wherein state legislators, rather than the voting public, would select US senators and the president. This was intended to serve as a safeguard against potential disruptions caused by populist elements within the electorate.

Hacking the 15th Amendment

The 15th Amendment, ratified in 1870 as the last of the Reconstruction Amendments,[2] prohibited states and the federal government from denying or limiting a citizen's right to vote "on account of race, color, or previous condition of servitude." The Reconstruction Amendments did not stop states from making it difficult or impossible for Black Americans to vote, however. The states' hack was to erect a host of barriers to voting that were keyed to vulnerabilities experienced disproportionately by Black Americans, as opposed to blatant race-based bans on voting: poll taxes that exploited the poverty of most Black Americans at the time, literacy tests to exploit the legacy of brutal repression of literacy among enslaved people and the limited educational opportunities of their progeny, and organized

[1] The New Jersey Constitution, adopted on July 2, 1776, uses the gender-neutral pronoun "they" and doesn't include racial categories in its election law.

[2] The 13th Amendment outlawed slavery and the 14th Amendment gave citizenship to all persons "born or naturalized in the United States," including formerly enslaved people, and provided all citizens with "equal protection under the laws."

violence by non-state actors (such as the Ku Klux Klan) to deter Black participation in elections, among other measures. Especially in the American South, so-called grandfather clauses restricted voting to those whose grandfathers had voted, which had the effect of disenfranchising generations of Black Americans with grandfathers who had been enslaved and ineligible to vote.

The Supreme Court ruled in 1915 that grandfather clauses were unconstitutional. The Court reasoned "the grandfather clauses in the Maryland and Oklahoma constitutions to be repugnant to the Fifteenth Amendment and therefore null and void."[3] In 1920, voters extended the right to vote to women with the 19th Amendment, which "prohibits the United States and its states from denying the right to vote to citizens of the United States on the basis of sex." This followed the establishment in 1913 of direct popular election of senators upon ratification of the 17th Amendment.

The poll tax exploited a vulnerability that was pervasive in the American South through much of the twentieth century and cut across racial lines: poverty. In 1959, 56.2 percent of Black Americans and other people of color lived below the poverty line. This proportion of persons below the poverty line eventually declined to 13 percent in 1968, but the poverty rate among Blacks and other people of color remained about three times the rate among White Americans (U.S. Department of Commerce, 1969). As of 1966, eleven states in the American South had poll taxes. Americans outlawed the practice for federal elections in 1964 with the 24th Amendment, but five states – Alabama, Arkansas, Mississippi, Texas, and Virginia – retained poll taxes for state elections (Lebetter Jr., 1995). In *Harper v. Va. Board of Elections*, the Supreme Court invalidated the practice for states, on the basis that "once the franchise is granted to the electorate, lines may not be drawn which are inconsistent with the Equal Protection Clause of the Fourteenth Amendment." The Court held that "a State violates the Equal Protection Clause of the Fourteenth Amendment whenever it makes the affluence of the voter or payment of any fee an electoral standard," because "voter qualifications have no relation to wealth nor to paying or not paying this or any other tax" and thus have no rational basis other than to discriminate against poor people.[4]

The 26th Amendment, ratified in 1971 amid social turmoil in the United States over the Vietnam war and US reliance on a conscript military, lowered the voting age to eighteen, giving Americans eligible for the military draft the right to vote in state and federal elections – and thus have a say in national policy on the deployment of US armed forces (Baum, Cea, & Cohen, 2021).

This collection of constitutional requirements and accompanying Supreme Court case law establishes the constitutional floor for voting rights in the United

[3] *Guinn v. United States*, 238 U.S. 347 (Supreme Court of the United States, June 21, 1915).

[4] *Harper v. Virginia Board of Elections*, 383 U.S. 663 (Supreme Court of the United States, March 24, 1966).

States. The constitution otherwise defers to state and federal legislators on most ballot decisions, saying that the “times, places and manner” of elections are state matters unless Congress sets nationwide standards. This entails that the selection, implementation, and oversight of elections and polling-related infrastructure (e.g., voting machines) are also left to the states, which, in turn, often leave many aspects of election administration to local (often county) governments.

Electoral Infrastructure Basics

Election infrastructure in the United States rests on this constitutional foundation and is usefully broken down into several discrete components: partisan campaign infrastructure and interest groups; voter registration; ballot casting; and ballot counting and certification of election results. Each of these components is subject to different state and federal laws, as well as having different cybersecurity and other risk attributes pertaining to the vulnerability of election infrastructure.

Partisan Campaign Infrastructure, Interest Groups, and the Media

Partisan campaign organizations generally determine how their political party nominates candidates to compete in the general election for a given office. Candidates’ campaign organizations provide the management infrastructure and support for their candidates to run for office. Core campaign functions such as fundraising, advertising, and get-out-the-vote initiatives are the responsibility of what might be termed the partisan elements of election infrastructure. These partisan elements are subject to a variety of state and federal laws relating to such matters as fundraising, advertising, coordination and contact with outside interest groups engaged in electioneering activities, and voter registration drives. Interest groups, political action committees (PACs), and other nonpartisan organizations such as think tanks may seek to influence public opinion, candidates’ policy preferences, and election outcomes by endorsing candidates, issuing position papers, producing policy research, advertising, and otherwise engaging in the political process; they too operate in a distinct legal context. Objective, fact-based media is essential to ensuring that voters have access to timely and accurate information about candidates, issues, election processes, and election outcomes. The First Amendment’s heightened protections for political speech are a core element of the constitutional foundation for partisan campaign infrastructure and interest groups.

Voter Registration and Identity

Persons eligible to vote must register to cast a ballot and have their vote counted toward determining the winner of the election. The United States employs a decentralized voter registration system, with each state responsible for maintaining its own registration rolls. State-level agencies, such as election boards or secretaries of state, oversee the voter registration process. To register to vote in the United

States, individuals must meet certain eligibility requirements, which typically include being a US citizen, meeting the minimum age requirement of eighteen years old, and being a resident of the state or jurisdiction in which they wish to vote. Some states also require individuals to provide proof of identity or residency during the registration process. States provide various methods for citizens to register to vote, including in-person, online, and mail-in registration.

Individuals can register to vote in person at designated government offices, such as election offices, Department of Motor Vehicle (DMV) offices, or public assistance agencies. Many states also offer online voter registration systems, allowing eligible individuals to register conveniently through secure websites. Some states allow individuals to register to vote by mailing in registration forms obtained from election offices or through voter registration drives. States are also responsible for maintaining accurate voter rolls by regularly reviewing and updating voter registration records. This process includes removing ineligible or deceased voters and updating address changes.

Voter identity and pollbooks are key components of the voting process in the United States and help to ensure the integrity and accuracy of elections. Voter identity verification refers to the process of confirming the identity of individuals who show up to vote. The purpose is to prevent voter fraud and ensure that only eligible voters cast their ballots. The specific requirements and methods for verifying voter identity vary across states. Some states have implemented strict voter identification laws, while others have more lenient or no specific requirements. Voter identification laws, enacted by individual states, determine the types of identification documents that voters must present at the polling place. These laws aim to verify the identity of voters and prevent fraudulent voting. The specific requirements and accepted forms of identification differ among states. Some states require a photo ID, such as a driver's license or a state-issued ID card, while others accept non-photo IDs, utility bills, or other documents showing the voter's name and address. Pollbooks are registers or electronic databases that contain voter information, such as names, addresses, and registration status. They serve as a reference for poll workers to verify voter eligibility and ensure that individuals are registered to vote in a particular precinct or district. Pollbooks help prevent individuals from voting more than once and allow election officials to track and update voter participation (U.S. Election Assistance Commission, 2023). Around three-quarters of registered voters live in jurisdictions where pollbooks are used (Verified Voting, 2020).

Ballot Casting

Voting machines are used in the United States to facilitate the casting and counting of votes in elections. It is up to individual states to decide which machines to purchase; states are also responsible for maintaining these systems and ensuring their readiness for election day. Nine states and the District of Columbia require testing against federal standards (the Voluntary Voting System Guidelines (VVSG), discussed later), sixteen require testing by a federally accredited laboratory, and twelve require full federal certification (Verified Voting, 2021).

For most of the nation's history, voting machines were mechanical devices that a voter used to mark a ballot. In the past two decades, however, the United States has replaced a substantial percentage of wholly mechanical machines with ones incorporating digital functionalities. These include optical scan machines, direct-recording electronic (DRE) machines, and ballot marking devices (BMDs). Optical scan machines read marked paper ballots, which are manually filled out by voters. The machines scan and tabulate the votes recorded on the paper ballots. DRE machines are electronic devices that allow voters to make their selections directly on a touchscreen or through other input mechanisms. These machines store and tally the votes electronically. BMDs assist voters, including those with disabilities, in marking their ballots electronically. Voters use the device to make their selections, which are then printed on a paper ballot for tabulation.

Vote Counting and Certification of Election Results

Vote counting involves the aggregation and tabulation of individual votes to determine the outcome of an election. The specific methods and technologies used can vary by state and jurisdiction. Common vote counting methods include manual counting of paper ballots, electronic scanning of marked ballots, or the use of electronic voting machines that tally votes electronically. Election laws and procedures govern the entire vote counting process. These laws vary at the federal, state, and local levels, and they cover areas such as canvassing and certification, recounts and audits, and reporting requirements.

Canvassing refers to the official examination and verification of election results, including the validation and counting of provisional or absentee ballots. Once the canvassing process is completed, election officials certify the results, declaring the winners. Election laws often provide procedures for recounting votes in cases where the margin of victory is close or when requested by candidates. Recounts can be conducted manually or through machine recounts. Some states also require post-election audits to verify the accuracy of the voting system and ensure the integrity of the results. Election laws mandate the reporting of election results to the appropriate authorities and the public. These requirements include timelines for reporting, formats for result presentation, and mechanisms for transparency and public access to the reported data (U.S. Election Assistance Commission, 2022). A state official, often a state's secretary of state, certifies the results of elections.

News organizations track these counting processes and results so that they can report on developments and election outcomes in a timely manner. For example, the Associated Press maintains a network of stringers – thousands of local reporters with "first-hand knowledge of their territories and trusted relationships with county clerks and other local officials" – and public sources such as state and county websites for its reporting on elections (Associated Press, n.d.).

Vulnerabilities

As we shall see subsequently, hackers have exploited vulnerabilities in each component of election infrastructure for centuries, but the digitalization of this infrastructure adds an additional attack surface for threat actors to attempt to exploit. For example, campaign organizations strive to keep their internal communications confidential, but threat actors might try to breach confidentiality to collect intelligence on campaign strategy and policy preferences – as China did with its cyber intrusions into campaigns of presidential candidates Barack Obama and John McCain in 2008 (Isikoff, 2013) – or distract and embarrass the campaign by leaking information – as Russia did in 2016 when it hacked the Democratic National Committee and leaked emails (Nakashima & Harris, 2018). Voter registration purges can be performed for the legitimate purpose of ensuring that registration rolls are up to date, but the technique can be hacked by unscrupulous election officials to purge eligible voters who are likely to vote for the opposition. Hackers might also target voter registration rolls, as Russia did in 2016, and potentially alter them in ways that threaten their integrity (McFadden, Arkin, & Monahan, 2018).

These are just a few of the many ways in which hackers can identify and exploit vulnerabilities in election infrastructure. We discuss additional examples later in the chapter.

Breaking down election infrastructure into discrete components has analytic value, but it is also important to consider election infrastructure as a systemic whole, especially when overall public confidence in the integrity of an election is at stake. A threat against any one component of election infrastructure could shake confidence in the integrity of the voting process and the legitimacy of the outcome.

WHITE HATS HACK BACK

The Congress, the executive branch, and the federal courts have frequently intervened against efforts by states to curtail voting, especially when those efforts are animated by racism toward Black Americans. The Civil Rights Act of 1870 was Congress' first attempt at enforcing the 15th Amendment's ban on denying Black Americans the right to vote;[5] subsequent amendments in 1957, 1960, and 1964 further expanded federal protections for Black Americans' voting rights.[6] Congress enacted the Voting Rights Act of 1965 (VRA) to ban racial discrimination in the

[5] Specifically, the 1870 Act, referred to variously as the Enforcement Act or First Ku Klux Klan Act, made it a federal criminal offense to prevent Black Americans from voting or threatening violence or other retaliation for voting, such as loss of employment or eviction from their home.

[6] The 1957 amendment authorized the U.S. Attorney General to seek federal court injunctions to safeguard the voting rights of Black Americans. The 1960 amendment bolstered court enforcement of voting rights and mandated preservation of voting records. The 1964 amendment required desegregation of voting places, among other provisions.

administration of elections and enforce the 14th and 15th Amendments; it has amended the VRA five times since then to expand its protections (Waldman et al., 2021b).

Legislation enacted in 1984 required polling places to be accessible to people with disabilities, and the 1986 Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) permitted service men and woman and overseas US voters to register and vote by mail. In 1993, Congress legislated federal voter registration guidelines in the National Voter Registration Act of 1993, which required each state to have a designated official for overseeing election administration and streamlined the voter registration process (National Conference of State Legislatures, 2022).

Following the controversial presidential election of 2000, where "hanging chads" in Florida required Supreme Court intervention to decide the winner,[7] Congress enacted the Help America Vote Act (HAVA), which aimed to bring about significant changes in election administration. Congress has not enacted major new voting rights legislation since HAVA.[8]

Meanwhile, the Supreme Court has intervened in ways that tilt constitutional momentum away from protecting voting rights – especially among Black Americans – and toward giving states greater discretion to make changes to their election infrastructure to save money and guard against voter fraud, even when those changes foreseeably erect barriers for eligible voters, especially Black Americans, to cast their ballots.

John Lewis, White Hat Hacker

In June 1964, three voting rights activists were murdered in Mississippi for helping Black Americans register to vote.[9] The violent episode galvanized support for the Civil Rights Act, which Congress passed, and President Lyndon B. Johnson signed, one month later.[10] The Civil Rights Act outlawed segregation in public places and in businesses that serve the general public and banned discrimination on the basis of race, color, religion, sex, or national origin in employment. It also required that laws relating to voter qualification be applied equally within a jurisdiction, banned the practice of using errors in registration documents and ballots to disqualify a Black American from voting even when an error was not material to that person's eligibility

[7] *Bush v. Gore*, 531 U.S. 98 (United States Supreme Court, December 11, 2000).

[8] The VRA was reauthorized in 1970, 1975, and 1982, with the most recent reauthorization occurring in 2006 when President George W. Bush signed legislation to extend the VRA for an additional twenty-five years. In 2009, Congress enacted the Military and Overseas Voter Empowerment Act ("MOVE Act"), which amended UOCAVA to establish new voter registration and absentee ballot requirements for federal elections to further facilitate the ability of Americans living overseas to vote.

[9] *United States v. Price*, 383 U.S. 787 (Supreme Court of the United States, March 28, 1966).

[10] Civil Rights Act, Pub. L. No. 88-352, 78 Stat. 241 (1964).

to vote, and outlawed literacy tests unless all voters had to take them and certain transparency requirements about them were met.

On March 7, 1965, John Lewis, a prominent civil rights activist and future Member of Congress,[11] led a march of over 600 people across the Edmund Pettus Bridge in Selma, Alabama to protest racial discrimination in the American South. The peaceful protesters encountered violent resistance at the top of the bridge from Alabama state troopers, whose unprovoked brutality against the procession was captured by television cameras and broadcast nationwide, turning the event in Selma into a pivotal moment in civil rights history. Outrage over the local incident, known as Bloody Sunday, swept the nation and further fired up support for the civil rights movement (Klein, 2020). Congress passed the VRA five months later.

The VRA patched numerous vulnerabilities in America's election infrastructure at the time. Aimed at safeguarding the voting rights of racial minorities, it prohibits discriminatory measures in elections that hinder their ability to cast ballots, such as literacy tests and poll taxes. The VRA also introduced federal oversight of states with a history of voter suppression, requiring them to seek federal approval before changing their voting laws. This "preclearance" requirement aimed to ensure fair and equitable access to the ballot box. The immediate impact of the VRA was substantial, leading to the registration of 250,000 Black Americans by the end of the year and ensuring that by the end of 1966, only four out of the thirteen southern states had less than 50 percent of eligible Black Americans registered to vote (National Archives, 2022).

In 2013, the Supreme Court ruled 5–4 in *Shelby County v. Holder* that the VRA's preclearance requirements were unconstitutional because the coverage formula was, in the majority's view, "based on 40-year-old facts having no logical relationship to the present day."[12] The decision made it possible for state governments previously subject to preclearance requirements to move forward with a variety of measures that made it more difficult for eligible voters to cast a ballot, with the effects being disproportionately felt by Black Americans, who voted for Democratic candidates 86 percent of the time in 2022 (Alexander & Fields, 2022). These measures – which included voter registration purges, polling location closures, limitations on absentee and mail-in ballots, and restrictions on the ability of third-party groups to facilitate registration and ballot casting – were predominantly the product of Republican-led state governments, who justified them as saving money or guarding against voter fraud (Waldman et al., 2018).

In the decade since *Shelby*, the ideological composition of the Court has shifted further rightward. Senate Republicans refused to advance President Obama's

[11] John Lewis was elected to Congress in 1986, representing Georgia's fifth congressional district spanning most of Atlanta, Georgia, where he served as lawmaker until he passed away on July 17, 2020.

[12] *Shelby County v. Holder*, 570 U.S. 529 (Supreme Court of the United States, February 27, 2013).

nomination of Merrick Garland to the Court in 2016 to replace the late Justice Antonin Scalia, and so President Trump was able to replace Justice Scalia with another conservative, Neil Gorsuch. President Trump replaced the retiring Justice David Kennedy, a moderate, with the conservative Brett Kavanaugh and the late Justice Ruth Bader Ginsburg, a liberal, with the conservative Amy Coney Barrett. In a 2021 decision from the Court's six conservative justices, *Brnovich v. Democratic National Committee*, the Court upheld Arizona's policy of discarding out-of-precinct ballots and prohibiting third-party groups from returning early ballots for another individual, which had been challenged under the VRA as racially discriminatory due to the disproportionate effect the policies have on persons of color.[13]

Since 2021, lawmakers in at least nineteen states have passed thirty-three laws that make it more difficult for people to vote. In Iowa and Kansas, election officials who typically assist voters with ordinary and essential tasks in the electoral process, such as returning ballots on behalf of voters with disabilities, are now deterred from doing so by the threat of criminal charges. Similarly in Texas, election officials that attempt to regulate poll watcher conduct or encourage voting by mail can now face criminal prosecution. These laws disproportionately affect voters of color. Again in Texas, the recently enacted Senate Bill 1 (SB 1) makes it more difficult for those who face language barriers to get help to cast a ballot. The law additionally bans twenty-four-hour and drive-thru voting (Waldman et al., 2021a).

The policy objectives of protecting and expanding access to voting and preventing those who are ineligible to vote from voting are not necessarily in conflict. After all, votes cast illegally dilute the political power of eligible voters. Even so, there are trade-offs between these two objectives, which is where the ideological conflict lies. On the American left, the emphasis has long been on protecting and expanding access, with an implicit acceptance that this could in theory result in a higher incidence of voter fraud. The principal adversaries are partisan (Republican) legislators and elected officials. Voter fraud is a federal crime and an exceedingly rare one at that: In a 2007 report, the Brennan Center for Justice found incident rates of fraud between 0.0003 percent and 0.0025 percent (Levitt, 2007).

On the American right, the emphasis is on preventing fraud, even if it means that otherwise eligible voters encounter more barriers to casting their ballot. The principal adversaries are fraudsters and their partisan (Democratic) enablers. To the extent that these additional barriers are encountered primarily by the right's political opponents, it could be a feature rather than a bug of their efforts to address fraud. Following the Supreme Court's decision in *Brnovich*, Texas Governor Greg Abbott, a member of the Republican Party, approved the implementation of SB 1, a law aimed at imposing restrictions on voting methods and schedules (Wilder & Hira, 2021). The *Texas Tribune* reported that the legislation targets voting initiatives

[13] *Brnovich v. Democratic National Committee*, 594 U.S. _ (2021) (Supreme Court of the United States, July 2, 2021).

employed in Harris County, a populous and diverse county with a Democratic lean (Ura, 2021). The law prohibits overnight early voting hours and drive-thru voting, which were both well-received by voters of color in the previous year's elections.

Hanging Chads and the Help America Vote Act (HAVA)

On November 20, 2000, the State of Florida officially declared George W. Bush as the winner of its twenty-five electoral votes in the race for the U.S. Presidency. The declaration came three weeks after a tumultuous election night on November 7, with reports of significant problems plaguing Florida's administration of the election. The Florida Division of Elections reported that Governor Bush had beaten Vice President Gore by 1,784 votes, which was less than one-half of a percent of the votes cast. This triggered an automatic machine recount under Florida elections law. The machine recount showed Governor Bush still winning, but by a substantially diminished margin of just 537 votes.[14] Vice President Gore sought manual recounts in several key counties, but this would take more time; the State of Florida and Governor Bush opposed the manual recount on the grounds that there was no basis in law for extending the deadline for local county canvassing boards to submit their results to the Florida secretary of state – the official responsible for election administration in Florida. The dispute was eventually decided in a 5–4 decision by the Supreme Court in *Bush v. Gore*, which ordered a stop to the manual recount underway in Florida and effectively made Governor Bush the winner of Florida's electoral votes and, as a result, the winner of the presidential election (for a timeline of this episode, see Stanford Law School, 2021). As the Supreme Court observed in *Bush v. Gore*, "This case has shown that punchcard balloting machines can produce an unfortunate number of ballots which are not punched in a clean, complete way by the voter,"[15] resulting in ballots with paper fragments still attached – so-called hanging chads. County officials grappled with deciphering voter intent amid hanging chads and the controversial "butterfly ballot" design in Palm Beach County, which caused confusion and inadvertently affected thousands of votes.

The U.S. Commission on Civil Rights (USCCR) investigated the administration of Florida's election and issued a report in June 2001 that documented widespread problems. In the years before the election, Florida had purged from its voter registration rolls tens of thousands of individuals suspected to be ineligible to vote, but the purge snared thousands of eligible voters as well. The USCCR found that Black voters were placed on purge lists "more often and more erroneously than Hispanic or White voters" (U.S. Commission on Civil Rights, 2002). A person on the so-called exclusion list had to affirmatively prove their eligibility to be relisted in voter registration rolls – a nontrivial burden. The USCCR also found that Black

[14] *Bush v. Gore*, 531 U.S. 98 (Supreme Court of the United States, December 12, 2000).

[15] See ibid., p. 104.

voters' ballots were ten times more likely to be rejected on technical grounds, such that of the 180,000 spoiled ballots cast in Florida during the November 2000 election, over half were cast by Black Americans despite comprising around 11 percent of Florida voters (U.S. Commission on Civil Rights, 2002).

ELECTIONS GO DIGITAL AND A NEW THREAT TO ELECTION INTEGRITY EMERGES

In 2002, the Federal Election Commission (FEC) approved the Voting System Standards (VSS) on a partisan 3–2 vote, with the Republican commissioners critiquing the VSS as too burdensome on state and local governments and downplaying the problems that the 2000 presidential election had exposed (Federal Election Commission, 2002). The partisan split at the FEC helped catalyze Congress to act (Weiner, 2019), and its main answer to the problems that the 2000 election exposed in US election administration was the bipartisan HAVA of 2002 (U.S. Election Assistance Commission, 2023). HAVA is the most ambitious effort yet to modernize America's election infrastructure, and has three principal aims: "establish a program to provide funds to States to replace punch card voting systems," which produced the infamous chads; "establish the Election Assistance Commission to assist in the administration of Federal elections" and provide related support; and "establish minimum election administration standards for States and units of local government with responsibility for the administration of Federal elections."

Going chadless meant embracing digital systems, using them to replace punch card voting systems. By January 2004, states were also obligated to establish computerized statewide voter registration lists to streamline and centralize the registration of voters. These lists were to be integrated with other agency records to verify the accuracy of information provided on voter registration applications. HAVA shifted the responsibility of defining, maintaining, and administering the voter registration lists from local officials to the states themselves. The legislation also mandated regular maintenance of the statewide lists to ensure ineligible voters and duplicate names were removed.

Cybersecurity and the Help America Vote Act (HAVA)

HAVA sought to facilitate the digitalization of election infrastructure presented by creating a new federal agency, the Electoral Assistance Commission (EAC), comprising four commissioners subject to Senate confirmation and a specialized staff, and creating new election-related responsibilities for the National Institute of Standards and Technology (NIST), an existing federal agency with deep experience developing digital governance standards, guidelines, and best practices. Among other responsibilities, the EAC would test and certify voting equipment as compliant with standards that the legislation tasked NIST to develop on the security, reliability, and accessibility of voting systems as chair of a Technical Guidelines Development Committee (TGDC).

HAVA set a deadline of nine months from the appointment of the four EAC commissioners for the TGDC to provide its first set of recommendations on voting system security, reliability, and accessibility. To meet this deadline, the TGDC formed three subcommittees focused on core requirements and testing, human factors and privacy, and security and transparency, hosting a series of workshops, meetings, and teleconferences in accordance with NIST's established practice of developing standards, guidelines, and best practices through open and transparent processes. The effort produced the VVSG 2005, which the TGDC submitted to the EAC in May 2005, meeting the established timeline.

The VVSG 2005 focused on usability, accessibility, and security of election systems. The goal of the usability-related guidelines was to ensure that the system was user-friendly and intuitive, allowing voters to interact with ease. Additionally, the guidelines emphasized the need for the system to incorporate error alert mechanisms, such as notifying voters about overvoting to reduce the number of improper ballots. The accessibility guidelines detailed requirements aimed at ensuring that individuals with limited vision and other disabilities, or non-English-speaking voters, would have equal access to the voting process – including accommodations to protect their privacy.

The security section of the VVSG 2005 provided explicit guidelines regarding the distribution and validation of voting system software. These requirements were put in place to guarantee that states and localities receive the accurate and verified version of the voting system software that has undergone testing and certification. By ensuring the correct software deployment, the integrity of the voting process is safeguarded, as the software used in the voting systems aligns with the approved and validated version.

Furthermore, the security section included provisions for validating the setup of the voting systems. This involved conducting inspections of the voting system software after it has been loaded onto the voting systems, verifying that it corresponds to the tested and certified software. This additional validation step played a crucial role in enhancing the security and reliability of the voting systems, reinforcing confidence in the accuracy and integrity of the election results. By emphasizing these security measures, the VVSG 2005 aimed to mitigate potential risks and protect the integrity of the voting process (U.S. Election Assistance Commission, 2005).

To help states meet HAVA's requirements, the law authorized $3.9 billion in funding for a grants program that the EAC would administer. Congress appropriated $2.8 billion for the first phase of the grants program to help states and localities purchase new voting equipment, upgrade their voter registration systems, and make other improvements to their election infrastructure. In 2006, Congress appropriated

$1.1 billion, which was used to continue the work of phase one and fund new initiatives such as the Help America Vote College Program (HAVCP). In total, the EAC has awarded $3 billion in grants to state and local governments.

Vulnerabilities in Digital Systems Identified

The passage of HAVA in 2002 and its push for digitizing voting systems led to greater interest among security researchers in the security of voting systems. For example, Bannet and coauthors demonstrated the relative ease of injecting malicious code in DRE systems and the difficulty of detecting them. Bannet et al. (2004), and Kohno et al. (2004) demonstrated major security problems in a Diebold DRE system by studying source code that an independent researcher, Bev Harris, found online.[16] In 2006, it was expected that electronic voting would be utilized by approximately 80 percent of American voters in the upcoming midterm elections, where control of the House of Representatives was on the line (Tapper & Venkataraman, 2006). In the run-up to the election, researchers identified new problems with the security and reliability of electronic voting systems. Princeton Professor Edward Felten and graduate students Ariel Feldman and Alex Halderman acquired a Diebold AccuVote-TS machine from an undisclosed source and successfully identified methods to rapidly upload malicious programs onto the machine (Feldman, Halderman, & Felten, 2006). They discovered that malicious programs could be installed by gaining access to the machine's memory card slot and power button, which were located behind a locked door on the side of the machine. The lock could be easily picked in a mere ten seconds, enabling unauthorized access. Once inside, the installation of the malicious software took less than a minute to complete.

The researchers developed software capable of modifying all records, audit logs, and counters stored by the voting machine. They ensured that even a thorough forensic examination would not detect any tampering. These programs had the ability to change vote totals or cause machine malfunctions, which could potentially impact the outcome of an election, especially if the compromised machines were located in critical polling stations. Furthermore, the researchers discovered the possibility of spreading malicious programs to multiple machines through a computer virus. This could be achieved by piggybacking on a new software download or an election information file being transferred between machines.

These studies are part of a line of research documenting security shortcomings in election infrastructure, with a primary focus on voting systems – the machines used to record and potentially document and count votes – and how an attacker could

[16] Harris wrote a book documenting her discovery and examination of the source code, which Diebold had previously refused to make public (Harris, 2004). A Government Accountability Office (GAO) report from September 2005 reviews these and other studies documenting security problems in digital voting systems (Government Accountability Office, 2005).

subvert those systems to affect election outcomes or undermine the public's perception of the integrity of an election. For example, a study from the Brennan Center for Justice on the security of voting systems documented numerous attack scenarios on voting systems that resulted in changed votes (Lawrence, 2006). The State of Ohio's EVEREST study examined the usability, stability, and security of voting systems and found that every voting system used in Ohio had "critical security failures that render their technical controls insufficient to guarantee a trustworthy election" (McDaniel et al., 2007, p. 3). Its threat model focused on how a threat actor could exploit cyber vulnerabilities to influence election outcomes by producing incorrect vote counts or blocking eligible voters, or undermine integrity by delaying the results or violating the secrecy of the ballot (McDaniel et al., 2007, pp. 14–15). California's "Top-to-Bottom Review" in 2007 of voting systems used in California yielded similar results (Bowen, 2007) and focused on how an attacker might change election outcomes (Bishop, n.d., p. 1);[17] it also "made no assumptions about constraints on the attackers" and did not consider the likelihood of any of its attacks (Bishop, n.d., p. 2). Florida and Connecticut pursued studies of their own, with a comparable threat model and similar results about the poor cybersecurity of voting systems. In 2015, Norden and Famighetti used interviews and data from the Verified Voting Foundation to document a range of vulnerabilities across election infrastructure (Norden & Famighetti, 2014). They too emphasized the risks of altered election outcomes and soured confidence, but in ranking the severity of threats, they also incorporated such factors as feasibility and cost. Finally, in the run-up to the 2016 elections, several other researchers and research groups issued recommendations about shoring up election systems considering the growing cybersecurity threat (National Institutes of Science and Technology, 2016).

A common thread running through many of these studies is a narrow focus on how an adversary might exploit cyber vulnerabilities to affect election outcomes and undermine confidence, in isolation from other means to achieve the same outcomes. As we have seen, however, hackers have exploited vulnerabilities in electoral infrastructure for centuries to affect election outcomes and challenge confidence in the integrity of elections: Hostile, black hat measures such as poll taxes and grandfather clauses were intended to affect election outcomes in favor of a dominant White majority, while white hat actions by civil rights leaders such as John Lewis exposed legitimacy shortcomings in electoral infrastructure that led to legislative reforms. The researchers behind the studies invested time and energy to acquire voting systems or their source code, identify vulnerabilities, and develop techniques to exploit them. A malicious hacker would have to as well, and if their goal is to subvert democracy, they might reasonably conclude that there are proven and

[17] The goal of the study was "to identify and document vulnerabilities, if any, to tampering or error that could cause incorrect recording, tabulation, tallying or reporting of votes or that could alter critical election data such as election definition or system audit data."

potentially more cost-effective ways to do so than carrying out cyberattacks against voting machines: Why go to the trouble, risk, and expense of hacking a voting machine when partisan gerrymandering or selective shuttering of polling places could yield a comparable result?

This reasoning could explain why the initiative that arguably most reflected the cyber policy zeitgeist in Washington, DC for much of the period between the enactment of HAVA and the 2016 presidential election did not mention voting system security at all. The Center for Strategic and International Studies convened a commission of experts chaired by the bipartisan pair of Representatives Jim Langevin (D-RI) and Mike McCaul (R-TX) in advance of the 2008 presidential elections to provide analysis and recommendations to the new presidential administration. The commission's report emphasized "the militaries and intelligence services of other nations" as the main cyber adversaries, and highlighted American economic competitiveness and US critical infrastructure – "electricity, communications, and financial services" as being most at risk from cyberattacks (Center for Strategic and International Studies, 2008). At the time, however, the US government did not consider election infrastructure to be part of critical infrastructure – that infrastructure's designation as critical by the Department of Homeland Security (DHS) would have to wait until shortly after the 2016 election (U.S. Election Assistance Commission, 2022).

THE 2016 PRESIDENTIAL ELECTION AND ITS AFTERMATH

Russia hacked the 2016 election at Vladimir Putin's direction to damage Hillary Clinton and undermine Americans' confidence in the legitimacy of the electoral process. How much the Russians contributed to Clinton's loss to Donald Trump and the precipitous drop in the aftermath of the campaign in Americans' trust in electoral infrastructure is a matter of ongoing debate; the fact of those outcomes, however, is not.

Understandably, the events of 2016 provoked unprecedented interest in the resiliency of electoral infrastructure against digital risks – not only cyberattacks on voting systems or other infrastructure but also the use of social media platforms to spread falsehoods and lies. It also injected partisan discord into what had previously been a largely technocratic and, to some election security researchers, an often quixotic quest to shore up election infrastructure against digital hackers – the salience of the research would resonate in even-numbered years in the run-up to an election, and then taper off once the election passed. As we have seen, the impetus for HAVA and its drive toward digitizing electoral infrastructure stems from the 2000 presidential election, where a contest for the president was lost due to voting system irregularities amid bitter partisan debate over the cause and consequences of those irregularities. HAVA was supposed to fix those irregularities, but its push for digitizing elections, warned security researchers, introduced new risks: voting systems that were vulnerable to hacking. The implied threat actor in this research on the machines that record and tabulate votes was not a foreign government, but a domestic political partisan trying to boost their preferred candidate. The cyber policy community, meanwhile, was focused primarily on foreign military and intelligence services as the primary threat actor and critical infrastructure – which didn't include electoral infrastructure at the time – and American economic competitiveness as the threat actors' main targets. Therefore, 2016 caught both the technocratic cyber research and cyber policy communities off guard: As it happened, it was a foreign government that sought to subvert electoral infrastructure through digital means. And the infrastructure it targeted was not voting systems, but other components of electoral infrastructure – notably, voter registration databases and partisan campaign infrastructure.

What Happened in 2016

The story of the 2016 election and its brush with cyberattacks is documented in the Senate Select Committee on Intelligence's bipartisan opus, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election" (Senate Select Committee on Intelligence, 2020). The condensed depiction presented here is intended to further contextualize efforts to shore up electoral infrastructure in the aftermath of 2016.

The digital elements of the Russian campaign involved cyberattacks aimed at compromising the confidentiality, integrity, or availability of targeted systems and information operations aimed at denigrating Hillary Clinton, exacerbating political polarization, and undermining the public's confidence in the integrity of democratic procedures. In June 2016, a hacker posted online a trove of nonpublic documents from the Democratic National Committee (DNC). One month later, a hacker calling themselves Guccifer 2.0 claimed to have shared 20,000 nonpublic DNC emails with WikiLeaks, the notorious publisher of stolen information (Thielman, 2016). Cybersecurity researchers and the US government have concluded that the Russian government was behind these operations, though Moscow denies the allegations. The emails, consisting of 19,252 messages and 8,034 attachments, were leaked on October 7 by WikiLeaks and a pop-up sister site called DCLeaks (Krawchenko et al., 2016). The leaked correspondence revealed a bias within the DNC toward Hillary Rodham Clinton over her primary rival, Bernie Sanders, despite the DNC's earlier claims of neutrality, and contained other embarrassing vignettes about the inner workings of the DNC. The timing of the leaks was noteworthy, happening within hours of video footage airing Clinton's rival Donald J. Trump boasting about sexually assaulting various women. Later that day, a statement from Federal Bureau of Investigation (FBI) Director James Comey, DHS Secretary Jeh Johnson, and Director of National Intelligence (DNI) James Clapper warned that the US government was "confident that the Russian

Government directed the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations" (Department of Homeland Security & Director of National Intelligence, 2016).

Russian government hackers also systematically scanned election-related state infrastructure in likely all fifty states and breached the systems of at least two of them.[18] The hackers were able to access voter registration data, and while there is no evidence that the hackers altered data, their access would have allowed them to do so. The hackers also researched voting systems and other aspects of electoral infrastructure, though there is no evidence that any such systems were compromised in 2016.

In August 2016, DHS Secretary Johnson hosted a conference call with state election officials to "to discuss the cybersecurity of the election infrastructure" (Department of Homeland Security, 2016). He told the officials that while "DHS is not aware of any specific or credible cybersecurity threats relating to the upcoming general election systems," he offered DHS assistance in helping state officials manage risks to voting systems in each state's jurisdiction. He also mentioned the possibility of designating electoral infrastructure as critical infrastructure, which would enable DHS to prioritize the sector for support and establish protected channels for information exchange.

The reaction to such a designation from officials who spoke out during the meeting, Secretary Johnson said later, "ranged from neutral to negative," with those expressing negative views asserting that administering elections was their responsibility, not the federal government's (Department of Homeland Security, 2016; Johnson, 2017). Later in August, the FBI issued an alert about malicious activity targeting election-related state infrastructure, and in September, Congressional leaders issued a bipartisan plea to state officials to accept DHS support. Forty-nine states requested technical assistance, which DHS delivered primarily in the form of remote scans of internet-facing election-related state infrastructure (Government Accountability Office, 2020).

In December 2016, Brian Kemp, then-secretary of state for the State of Georgia, sent letters to the DHS and President-elect Trump alleging that the DHS had scanned Georgia's voter registration systems as a precursor to attacking them and asking Trump to investigate the matter upon taking office (Fulghum, 2017). Secretary Johnson's response days later explained that there was no scan, and that the traffic described in Kemp's letter was from a DHS contractor at the Federal Law Enforcement Training Center (FLETC) conducting research on "whether incoming FLETC contractors and new employees had a certain type of professional license – a service that, as I understand it, your website provides to the general public" (Fulghum, 2017). He further explained that "the technical information we have corroborated [this explanation], and indicates normal Microsoft Internet

[18] Illinois has admitted to being one of them, and Arizona is believed to be the other.

Explorer interaction by the contractor's computer with your website" (Fulghum, 2017). DHS Congressman Jason Chaffetz, Chairman of the House Committee on Oversight and Reform, followed with a letter to DHS complaining that Secretary Johnson's written response and subsequent briefings from DHS staff "did not provide adequate information to verify or validate" this explanation; he requested that relevant records be preserved and that the DHS inspector general undertake an investigation. In June 2017, the inspector general notified Congress that Kemp's allegations were "unsubstantiated" and that "the activity Georgia noted on its computer networks was the result of normal and automatic computer message exchanges generated by the Microsoft applications involved" (Department of Homeland Security, 2017).

The bitterness of the 2016 election, with the incumbent administration warning that Russia had interfered in the election in support of the opposition's candidate, Donald J. Trump, and the opposition's distrust of the incumbent administration's motives as well as baseless claims throughout the election by Trump that the election was "rigged" against him, set the stage for post-2016 efforts to address cyber threats to electoral infrastructure.

Measures Taken between 2017 and 2020

The period between 2017 and 2020 – with the Congressional midterm elections in 2018 and the 2020 presidential contest – were an especially sensitive moment for American democracy, especially debates around electoral integrity and the resilience of election-related infrastructure. The 2016 election highlighted that cynical partisans were not the only potential threat to electoral integrity: Foreign governments also had reason to intervene. That the foreign government's preferred candidate, Donald J. Trump, won the presidential contest raised the uncomfortable question of the extent to which Russia's efforts contributed to it. His own linkages to Russia – including his public invitation in the summer of 2016 for Russia to find and presumably release deleted emails from Hillary Clinton's private email server – and the Department of Justice (DOJ) inquiry into those linkages further sharpened the potential ideological stakes of whether and how to make election infrastructure more resilient against digital threats. In particular, the Trump administration, facing a series of threats to its legitimacy built in part on the vulnerability of electoral infrastructure to digital threats, could have denied or played down the existence of the vulnerability in policy. The fact that it didn't is fairly remarkable.

Ten weeks would elapse between election day on November 7, 2016 and inauguration on January 20, 2017. On December 28, 2016, President Obama signed an Executive Order (EO) 13757, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," to authorize economic sanctions against actors involved in "tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions" and sanctioned Russian organizations and individuals in connection with the 2016 election interference. It also expelled Russian intelligence officers operating under diplomatic cover from the United States and forced the closure of two Russian diplomatic facilities. In January 2017, Secretary Johnson designated electoral infrastructure as critical infrastructure. In addition to enabling the DHS to forge a deeper partnership with the sector on security issues, the designation also signaled to international partners and adversaries the sensitivity of electoral infrastructure from a national security perspective. For example, the United States had been engaged in diplomatic deliberations over norms of behavior in cyberspace during peacetime and was advocating inter alia for a norm that states do not interfere with critical infrastructure during peacetime.

When Trump took the oath of office on January 20, 2017, he inherited a policy trajectory from the Obama administration of trying to hold Russia accountable for its actions while deterring Russia or any other country from running a similar play as Russia in future elections. He rejected the assessment that Russia had intervened in the election to support him, however, and instead focused his attention on alleged voter fraud. The threat actor he had in mind was not a foreign government such as Russia or even a cyberthreat actor, but a person who is ineligible to vote that nevertheless casts a vote.[19] Such instances are exceedingly rare – in the 2016 election, for example, the Associated Press identified "fewer than 475 – a number that would have made no difference in the 2020 presidential election (Cassidy, 2021). In May 2017, however, he signed an EO to launch a "Presidential Advisory Commission on Election Integrity" charged with identifying and rooting out fraudulent or improper voting and voting registration (Trump White House Archives, 2017). Not surprisingly, the commission had uncovered no evidence of widespread voter fraud when it disbanded in January 2018.

Inside the bureaucracy of the Trump administration, however, agencies such as the DHS and the FBI were positioning themselves as allies of state election officials in those officials' efforts to prepare for the 2018 midterm elections and later the 2020 presidential elections. The DHS and the FBI hosted briefings with state election officials on threats to election integrity and how to build resilience against them (Department of Homeland Security, 2018), and in March 2018, the DHS announced the launch of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) to coordinate the sharing and exchange of cyber threat information among election officials and organizations (Center for Internet

[19] The public record about the commission, including statements from President Trump and the commission's leadership, Vice President Mike Pence and Kansas politician Kris Kobach, is devoid of any mention of cyber threats.

Security, n.d.). In addition, the designation of electoral infrastructure as critical infrastructure enabled DHS to convene a Government Coordinating Council (GCC) and a Sector Coordinating Council (SCC) to facilitate information sharing among public and nongovernmental actors engaged in election administration. In September 2018, President Trump signed EO 13848, "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election" (Trump, 2018). The EO directs the DNI to prepare a report within forty-five days of an election on whether foreign governments interfered with it; the EO also directs that DOJ and DHS prepare a report within forty-five days of the DNI's report on whether the foreign interference affected the election outcomes. The order also authorized sanctions and other measures against actors found to have interfered with a US election.

Congress, meanwhile, had debated multiple major legislative proposals[20] and three passed both houses: the consolidated appropriations acts of 2018[21] (Royce, 2018) and 2020 (U.S. Government Publishing Office, 2019) appropriated $380 million and $425 million, respectively, to the EAC to give to states to improve election technology and security, and the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) included $400 million in HAVA emergency funds for the 2020 federal election cycle. The 2018 funding came too late to contribute much to the 2018 Congressional midterms, but by September 2020, states had spent nearly 94 percent of the 2018 funding, with thirty-five states spending their allocation completely and another thirteen spending above 90 percent of theirs (U.S. Election Assistance Commission, 2021). The CARES Act funding could only be used in direct connection with helping states manage elections in the context of a pandemic, though some states used the funding to purchase new enterprise IT in support of remote work, which could have some modest cybersecurity benefit as newer IT tends to be easier to secure than older IT (U.S. Election Assistance Commission, n.d.).

In October, the heads of the DHS, the DOJ, the FBI, and the Office of the DNI jointly warned of "ongoing campaigns by Russia, China and other foreign actors, including Iran," to influence elections as well as attempted intrusions into state election-related infrastructure, though in the latter instance, the heads explained, "[i]ncreased intelligence and information sharing among federal, state and local partners has improved our awareness of ongoing and persistent threats to election infrastructure" and there was no evidence of a successful breach (Office of the Director of National Intelligence, n.d.).

[20] Examples include the Secure Elections Act of 2017, the Election Security Act of 2018, the Protecting American Voting Rights Act of 2019, the Secure Elections Act of 2020, and the John Lewis Voting Rights Advancement Act of 2020.

[21] Relatedly, the legislation also appropriated $300 million to the FBI for combating Russian cyber operations against the United States.

A joint statement on November 5 from the same group took on a reassuring tone and described the government's efforts to guard against digital threats to election infrastructure as "unprecedented":

> Our agencies have been making preparations for nearly two years in advance of these elections and are closely engaged with officials on the ground to help them ensure the voting process is secure. Americans can rest assured that we will continue to stay focused on this mission long after polls have closed. (Office of the Director of National Intelligence, 2018)

The agency heads warned voters to be vigilant, especially in the face of foreign influence campaigns designed to shape "public sentiment and voter perceptions … by spreading false information about political processes and candidates, lying about their own interference activities, disseminating propaganda on social media, and through other tactics." Voters should seek ground truth about elections and election processes by contacting their local election organizations and be cautious consumers of information.

After the election, news reports surfaced that the U.S. Cyber Command had carried out cyberattacks against the Russia-based Internet Research Agency (IRA) to shut it down during the election. The IRA was a notorious "troll farm" engaged in propaganda operations, often using social media. The IRA, its leader Yvgeniy Prigozhin, and others connected with it had previously been indicted by the DOJ on criminal charges stemming from the IRA's interference in the 2016 election,[22] and in September 2018 the DOJ indicted a Russian accused of overseeing Project Lakhta, the Russian codename for a propaganda operation targeting the United States and other countries, carried out in part through the IRA. The goal of the attack, according to this reporting, was to keep the IRA out of commission from election day until election results were certified (Barnes, 2019). The attack was reportedly part of a broader campaign by US military and intelligence organizations to interfere with the ability of foreign actors, especially Russia, to interfere in the midterm elections (Barnes, 2018).

The DNI submitted the Intelligence Community (IC)'s required report under EO 13848 on foreign interference in the 2018 midterm elections to the President on December 21. DNI Coats' public statement about the classified report said that "the Intelligence Community does not have intelligence reporting that indicates any compromise of our nation's election infrastructure that would have prevented voting, changed vote counts, or disrupted the ability to tally votes." In their public comments about the required follow-on report, which was classified, the Attorney General and DHS Secretary said there was "no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the

[22] *Indictment, United States v. Internet Research Agency et al.*, 1:18-CR-32 (DLF) (D.D.C. Feb. 16, 2018).

integrity or security of election infrastructure or political/campaign infrastructure used in the 2018 midterm elections" (U.S. Department of Justice, 2019).

These efforts to enhance the resilience of electoral infrastructure and disrupt adversaries' operations continued into the 2020 election cycle, with similar results, at least as far as foreign interference goes. The DNI submitted a classified report to the president in January 2021 pursuant to EO 13848; in March, the Biden administration released a declassified version. According to that report, the USIC found "no indications that any foreign actor attempted to alter any technical aspect of the voting process in the 2020 US elections, including voter registration, casting ballots, vote tabulation, or reporting results." It also "identified some successful compromises of state and local government networks prior to Election Day – as well as a higher volume of unsuccessful attempts – that we assess were not directed at altering election processes" (Director of National Intelligence, 2021). The follow-on report from the DOJ and DHS echoed the DNI, reporting that there was "no evidence that any foreign government-affiliated actor prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspect of the voting process; or otherwise compromised the integrity of voter registration information of any ballots cast during 2020 federal elections" (U.S. Department of Justice, 2021, p. 2) Both reports, however, highlighted the growing range of foreign actors engaged in digitally enabled influence operations against the United States.

President Trump lost his reelection bid to former Vice President Joseph Biden in 2020. He claimed without evidence, however, that the election was stolen from him because of widespread voter fraud. He denigrated the results of the election as illegitimate and sought ways to stay in power, despite the election's outcome. In contrast, the DHS issued a joint statement from the elections infrastructure GCC and SCC nine days after the election describing it as the "most secure in American history" and said "[t]here is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised" (Cybersecurity & Infrastructure Security Agency, 2020).

CONCLUSION

Though cybersecurity of elections is a recent concern, hacking elections is not. The relatively limited constitutional discipline on elections and the fact that the constitution distributes responsibility for administering elections to state and local governments means that the attack surface of America's election infrastructure for would-be hackers is large. Technology has added a new dimension to this attack surface in the form of digital technologies that facilitate tasks ranging from voter registration to vote casting and vote counting. Digital technologies are prevalent throughout electoral infrastructure – which technologists were quick to identify risks to voting systems in the years following enactment of HAVA in 2002 – but the mainstream cybersecurity policy community did not consider these risks a priority on par with the risks to critical infrastructure (which at the time didn't include state election-related infrastructure) and economic competitiveness posed by foreign military and intelligence services.

The digitalization of election infrastructure has lowered one of the barriers to entry for threat actors seeking to disrupt democratic processes: Before then, a hacker usually needed partisan allies to carry out an attack. Gerrymandering, poll taxes, even organized violence at polling places all require partisan allies. Hacks like these are, in a sense, inside jobs that rely on willing partners and a complacent public. The digitalization of electoral infrastructure makes it possible for outside actors to potentially hack elections: A lone wolf, criminal group, or foreign government can potentially interfere with elections on their own.

The 2016 presidential election pulled election security into the mainstream of cyber policy, with the DHS, FBI, and other federal agencies investing significant effort in building partnerships with state election officials and taking direct action against suspected threat actors with criminal indictments and economic sanctions. The partnership-building efforts with state officials after the designation in January 2017 of election systems as critical infrastructure created new information sharing channels and trust relationships that facilitated the ability of the federal government to provide security and other assistance. That these efforts in the Trump administration thrived despite President Trump's open hostility toward the notion that Russia interfered in the 2016 election to support his candidacy speaks to the ability of the agencies and their partners in state and local government to pursue their efforts as a technocratic versus political or partisan initiative. President Trump's benign neglect of his administration's efforts to protect election infrastructure from digital threats ended when he fired Chris Krebs, head of the Cybersecurity and Infrastructure Security Agency (CISA), which leads federal government cybersecurity initiatives for critical infrastructure (including election infrastructure), for claiming that the 2020 election had been the most secure in the history of the country. Trump did not quibble with claims about the cybersecurity of the election against foreign interference; his cavil with Krebs and with others who touted the cybersecurity of the election was that it conflicted with his claim that the election was stolen by the Democrats.

The hack of the DNC and breach of election-related infrastructure by Russian government-directed actors in 2016 elevated concerns regarding the cybersecurity of election infrastructure. In the immediate aftermath of the foreign interference in the 2016 election, then President Obama signed an EO authorizing economic sanctions against actors seeking to interfere with or undermine electoral processes or institutions. Shortly thereafter the DHS designated electoral infrastructure as critical infrastructure, notably signaling to allies and adversaries alike the acute sensitivity and importance of election infrastructure to national security.

Despite partisan differences, noteworthy strides have been made to counter continued attempts at undermining US elections and election infrastructure. The passage of major legislative proposals such as the Consolidated Appropriations Acts of 2018 and 2020, as well as the CARES Act, have directed funds toward further improving election technology and security.

Following the 2016 election, a noticeable shift was made toward paper ballots to increase election security. In the 2020 election, it is estimated that 93 percent, up from 82 percent in 2016, of all votes cast had a paper record. This uptick resulted from states and local jurisdictions replacing outdated and vulnerable paperless voting machines (i.e., DRE machines). Paper-based systems are better for security because they create a paper record that can be reviewed by election officials in postelection audits. Further measures such as postelection audits – a process that enables states to verify the accuracy of voting equipment and counting machines – act as additional defenses against election interference. As of 2023, forty-five states have mandated some form of postelection audit, up from thirty-five in 2016 (U.S. Election Assistance Commission, 2023).

These measures have paid off. Reports on the 2020 elections from the DOJ, DHS, and DNI noted that while an increasing number of foreign actors had engaged in influence operations against the United States, there was no evidence that these foreign actors were able to compromise the integrity of election infrastructure during the 2020 federal elections. The same is true for domestic actors: There is no evidence of successful election-related hacking in 2020 by partisans or other politically motivated actors.

As the saying goes, however, past performance does not guarantee future results: Some states still lack some form of paper trail for ballots cast and some form of postelection audit. All states should eliminate paperless voting machines and implement postelection audits. In addition, as the epidemic of ransomware attacks against municipalities and other targets shows, vulnerabilities remain. Owners and operators of election infrastructure, from local governments to candidate campaign operations, must make cybersecurity a core priority for risk management. This prioritization must come from the top: Senior leaders involved in election administration must make cybersecurity a priority, ensure that resources are devoted to it, and hold themselves and their teams accountable for managing cyber risks. Fortunately, owners and operators have resources they can turn to for guidance and support. For example, the CISA maintains a "Cybersecurity Toolkit and Resources to Protect Elections" website with guidance on best practices and free or reduced-price cybersecurity tools from leading vendors (Cybersecurity & Infrastructure Security Agency, 2024).

History teaches us further that cyber risks to election integrity, though real, cannot (perhaps yet) shine a candle to the myriad other ways that intrepid hackers have sought to subvert democracy. An all-hazards approach to election integrity is warranted.

REFERENCES

Alexander, A., & Fields, G. (2022, December 30). *Black support for GOP ticked up in this year's midterms*. AP News. https://apnews.com/article/2022-midterm-elections-brian-p-kemp-stacey-abrams-politics-us-democratic-party-53d31c9c8a87231d00784b6effa8d59e

Associated Press. (n.d.). *Counting the vote*. Associated Press. https://ap.org/about/our-role-in-elections/counting-the-vote

Bannet, J., Price, D., Rudys, A., & Singer, J. (2004, February). Hack-a-vote: Security issues with electronic voting systems. *IEEE Security and Privacy Magazine*, *2*, 32–37.

Barnes, J. E. (2018, October 23). U.S. begins first cyberoperation against Russia aimed at protecting elections. *The New York Times*. https://nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

(2019, February 26). Cyber command operation took down Russian troll farm for midterm elections. *The New York Times*. https://nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html?searchResultPosition = 1

Baum, S., Cea, B., & Cohen, A. (2021, June 30). *The 26th amendment turns 50 amid renewed voter suppression*. Brennan Center. https://brennancenter.org/our-work/analysis-opinion/26th-amendment-turns-50-amid-renewed-voter-suppression

Bishop, M. (n.d.). *Overview of red team reports*. Voting Systems. https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/red-overview.pdf

Bowen, D. (2007, August 3). *Top-to-bottom review*. California Secretary of State. https://sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review

Cassidy, C. A. (2021, December 14). *Far too little vote fraud to tip election to Trump, AP finds*. Associated Press. https://apnews.com/article/voter-fraud-election-2020-joe-biden-donald-trump-7fcb6f134e528fee8237c7601db3328f

Center for Internet Security. (n.d.). *Elections Infrastructure Information Sharing & Analysis Center*. Center for Internet Security. https://cisecurity.org/ei-isac

Center for Strategic and International Studies. (2008, December 8). *Commission on cybersecurity for the 44th presidency*. Center for Strategic and International Security. https://csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/other-projects-2

Cybersecurity & Infrastructure Security Agency. (2020). *Joint statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees*. Cybersecurity & Infrastructure Security Agency. https://cisa.gov/news-events/news/joint-statement-elections-infrastructure-government-coordinating-council-election

(2024). *Cybersecurity toolkit and Resources to protect elections*. Cybersecurity & Infrastructure Security Agency. https://cisa.gov/cybersecurity-toolkit-and-resources-protect-elections

Department of Homeland Security. (2016, August 15). *Readout of Secretary Johnson's call with state election officials on cybersecurity*. Department of Homeland Security. https://dhs.gov/news/2016/08/15/readout-secretary-johnsons-call-state-election-officials-cybersecurity

(2017, July 5). *Allegations of unauthorized scans of Georgia voting systems are unsubstantiated*. Office of Inspector General. https://oig.dhs.gov/sites/default/files/assets/pr/2017/oigpr-070517-allegations-unauthorized-scans-georgia-voting-systems-unsubstantiated_1.pdf

(2018, August 24). *DHS, FBI hold joint briefing for election officials with Facebook and Microsoft*. Department of Homeland Security. https://dhs.gov/news/2018/08/24/dhs-fbi-hold-joint-briefing-election-officials-facebook-and-microsoft

Department of Homeland Security & Director of National Intelligence. (2016, October 7). *Joint statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*. Department of Homeland Security. https://dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national#:~:text=The%20U.S.%20Intelligence%20Community%20(USIC,including%20from%20US%20political%20organizations

Director of National Intelligence. (2021). *Foreign threats to the 2020 US federal elections*. Director of National Intelligence. https://dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

Federal Election Commission. (2002, May 15). *FEC approves new voting systems standards*. Federal Election Commission. https://fec.gov/updates/fec-approves-new-voting-systems-standards/

Feldman, A. J., Halderman, A., & Felten, E. W. (2006, September 13). *Security analysis of the Diebold AccuVote-TS voting machine*. Center for Information Technology Policy. https://citp.princeton.edu/our-work/voting/

Fulghum, C. (2017, February 28). *Correspondence between DHS and U.S. Representative Jason Chaffetz*. Department of Homeland Security. https://dhs.gov/sites/default/files/publications/Correspondence%20between%20DHS%20and%20U.S.%20Representative%20Jason%20Chaffetz%20%28R-UT%29.pdf

Government Accountability Office. (2005). *Federal efforts to improve security and reliability of electronic voting systems are under way, but key activities need to be completed*. GAO-05-956.

(2020, February). *DHS Plans Are Urgently Needed to Address Identified Challenges before the 2020 Elections*. U.S. Government Accountability Office. https://gao.gov/assets/710/706312.pdf

Harris, B. (2004). *Black Box Voting: Ballot Tampering in the 21st Century*. Talion Publishing.

Isikoff, M. (2013, June 7). *Chinese hacked Obama, McCain campaigns, took internal documents, officials say*. NBC News. https://nbcnews.com/id/wbna52133016#:~:text=on%20NBCNews.com.-,The%20U.S.%20secretly%20traced%20a%20massive%20cyberespionage%20operation%20against%20the,intelligence%20officials%20tell%20NBC%20News.

Johnson, J. C. (2017, June 21). *Statement of Jeh Charles Johnson before the House Permanent Select Committee on Intelligence*. Federation of American Scientists. https://irp.fas.org/congress/2017_hr/062117-johnson.pdf

Klarman, M. J. (2016). *The framers' coup: The making of the United States Constitution*. Oxford University Press.

Klein, C. (2020, July 18). *How Selma's "Bloody Sunday" became a turning point in the Civil Rights Movement*. History.com. https://history.com/news/selma-bloody-sunday-attack-civil-rights-movement

Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004). Analysis of an electronic voting system. *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE Explore.

Krawchenko, K., Judd, D., Cordes, N., Goldman, J., Flores, R., Shabad, R., et al. (2016, November 3). *The John Podesta emails released by WikiLeaks*. CBS News. https://cbsnews.com/news/the-john-podesta-emails-released-by-wikileaks/

Lawrence, N. (2006). *The machinery of democracy: Voting system security, accessibility, usability, and cost*. The Brennan Center for Justice. https://brennancenter.org/sites/default/files/press-releases/The%20Machinery%20of%20Democracy.pdf

Lebetter Jr., C. R. (1995). Arkansas amendment for voter registration without poll tax payment. *The Arkansas Historical Quarterly*, 54(2), 134–162.

Levitt, J. (2007, November 9). *The truth about voter fraud*. The Brennan Center for Justice. https://brennancenter.org/our-work/research-reports/truth-about-voter-fraud

McDaniel, P., et al. (2007, December 7). *Everest: Evaluation and validation of election-related equipment, standards and testing*. U.S. Election Assistance Commission. https://eac.gov/sites/default/files/eac_assets/1/28/EVEREST.pdf

McFadden, C., Arkin, W. M., & Monahan, K. (2018, February 7). *Russians penetrated U.S. voter systems, top U.S. official says*. NBC News. https://nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721

Nakashima, E., & Harris, S. (2018, July 13). How the Russians hacked the DNC and passed its emails to WikiLeaks. *The Washington Post*. https://washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html

National Archives. (2022, February 8). *Voting Rights Act (1965)*. National Archives. https://archives.gov/milestone-documents/voting-rights-act#:~:text = The%20Voting%20Rights%20Act%20had,African%20Americans%20registered%20to%20vote

National Conference of State Legislatures. (2022, November 1). *Election administration at state and local levels*. National Conference of State Legislatures. https://ncsl.org/elections-and-campaigns/election-administration-at-state-and-local-levels

National Institutes of Science and Technology. (2016, September). *Protecting the 2016 elections from cyber and voting machine attacks*. National Institutes of Science and Technology. https://nist.gov/speech-testimony/protecting-2016-elections-cyber-and-voting-machine-attacks

Norden, L., & Famighetti, C. (2014). *America's voting machines at risk*. The Brennan Center for Justice.

Office of the Director of National Intelligence. (2018). *Joint statement on election day preparations*. Office of the Director of National Intelligence. https://dni.gov/index.php/newsroom/press-releases/press-releases-2018/item/1921-joint-statement-on-election-day-preparations

(n.d.). *Combating foreign influence in U.S. elections*. Office of the Director of National Intelligence. https://dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections

Royce, E. R. (2018, March 23). *H.R.1625 – Consolidated Appropriations Act, 2018*. Congress.gov. https://congress.gov/bill/115th-congress/house-bill/1625/text

Senate Select Committee on Intelligence. (2020, November 10). *Russian active measures campaigns and interference in the 2016 U.S. elections*. Senate Select Intelligence Committee. https://intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures

Stanford Law School. (2021, October 15). *Timeline of Florida Recount, Florida litigation, and Bush v. Gore*. Stanford Law Library. https://guides.law.stanford.edu/c.php?g = 991108&p = 7170216

Tapper, J., & Venkataraman, N. (2006, November 2). *Hackable democracy?* ABC News. https://abcnews.go.com/Politics/Vote2006/story?id = 2623854&page = 1

The Brennan Center Task Force on Voting System Security. (2006). *The machinery of democracy: Protecting elections in an electronic world*. The Brennan Center for Justice, NYU School of Law. https://brennancenter.org/sites/default/files/publications/Machinery%20of%20Democracy.pdf

Thielman, S. (2016, July 26). DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach. *The Guardian*. https://theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2

Trump, D. J. (2018, September 12). *Executive Order 13848 – Imposing certain sanctions in the event of foreign interference in a United States election*. Authenticated U.S. Government Information. https://govinfo.gov/content/pkg/DCPD-201800593/pdf/DCPD-201800593.pdf

Trump White House Archives. (2017, July 13). *Presidential advisory commission on election integrity*. Trump White House Archives. https://trumpwhitehouse.archives.gov/articles/presidential-advisory-commission-election-integrity/#:~:text = On%20May%2011%2C%2020 17%2C%20President,serves%20as%20the%20vice%20chair.

U.S. Commission on Civil Rights. (2002, September). *Ten-year check-up: Have federal agencies responded to Civil Rights recommendations*. U.S. Commission on Civil Rights. https://usccr.gov/files/pubs/archives/10yr02/vol1/vol1.pdf

U.S. Department of Commerce. (1969, December 31). *Poverty in the United States: 1959 to 1968*. Census.gov. https://census.gov/library/publications/1969/demographics/p60-68.pdf

U.S. Department of Justice. (2019, February 5). *Acting Attorney General and Secretary of Homeland Security Submit Joint Report on Impact of Foreign Interference on Election and Political/Campaign Infrastructure in 2018 Elections*. U.S. Department of Justice. https://justice.gov/opa/pr/acting-attorney-general-and-secretary-homeland-security-submit-joint-report-impact-foreign

(2021). Joint report of the Department of Justice and the Department of Homeland Security on Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2020 US Federal Elections. https://justice.gov/media/1148336/dl?inline

U.S. Election Assistance Commission. (2005). *Voluntary Voting System Guidelines Volume 1, Version 1*. U.S. Election Assistance Commission. https://eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF

(2021, July). *2020 grand expenditure report*. U.S. Election Assistance Commission. https://eac.gov/sites/default/files/paymentgrants/expenditures/2020_State_Grant_Expenditure_Report_FINAL.pdf

(2022, March 11). *Elections – Critical infrastructure*. United States Election Assistance Commission. https://eac.gov/election-officials/elections-critical-infrastructure

(2023, June 7). *Help America Vote Act*. United States Election Assistance Commission. https://eac.gov/about/help_america_vote_act.aspx

(n.d.). *Election assistance commission plans for use of CARES Act report to the pandemic response accountability committee*. United States Election Assistance Commission. https://eac.gov/sites/default/files/paymentgrants/cares/PRAC%20Reports/15011%20EAC % 20Report%20on%20CARES%20Funding.pdf

U.S. Government Publishing Office. (2019, December 20). *Consolidated Appropriations Act, 2020*. U.S. Government Publishing Office. https://govinfo.gov/content/pkg/PLAW-116publ93/html/PLAW-116publ93.htm

Ura, A. (2021, September 7). *Gov. Greg Abbott signs Texas voting bill into law, overcoming Democratic quorum breaks*. Texas Tribune. https://texastribune.org/2021/09/01/texas-voting-bill-greg-abbott/

Verified Voting. (2020, August). *Electronic poll book use in the United States*. Verified Voting. https://verifiedvoting.org/wp-content/uploads/2020/08/Verified-Voting-Electronic-Poll-Book-Use-in-the-United-States-20200831.pdf

(2021, May). *The business of voting*. Verified Voting. https://verifiedvoting.org/wp-content/uploads/2021/05/the-business-of-voting-single-page.pdf

Waldman, M., Weiser, W. R., Moraels-Doyle, S., & Sweren-Becker, E. (2018, August 6). *The Effects of Shelby County v. Holder*. Brennan Center for Justice. https://brennancenter.org/our-work/research-reports/effects-shelby-county-v-holder

Waldman, M., Weiser, W., Morales-Doyle, S., & Sweren-Becker, E. (2021a, October 4). *Voting laws roundup*. Brennan Center for Justice. https://brennancenter.org/our-work/research-reports/voting-laws-roundup-october-2021

(2021b, October 1). *Voting Rights Act analyses, reports, and explainers*. Brennan Center for Justice. https://brennancenter.org/our-work/research-reports/voting-rights-act-analyses-reports-and-explainers

Weiner, D. I. (2019, April 30). *Fixing the FEC: An agenda for reform*. Brennan Center for Justice. https://brennancenter.org/our-work/policy-solutions/fixing-fec-agenda-reform

Wilder, W., & Hira, E. (2021, December 15). *How the Freedom to Vote Act can blunt the worst of Texas's Voter Suppression Law*. Brennan Center of Justice. https://brennancenter.org/our-work/analysis-opinion/how-freedom-vote-act-can-blunt-worst-texass-voter-suppression-law