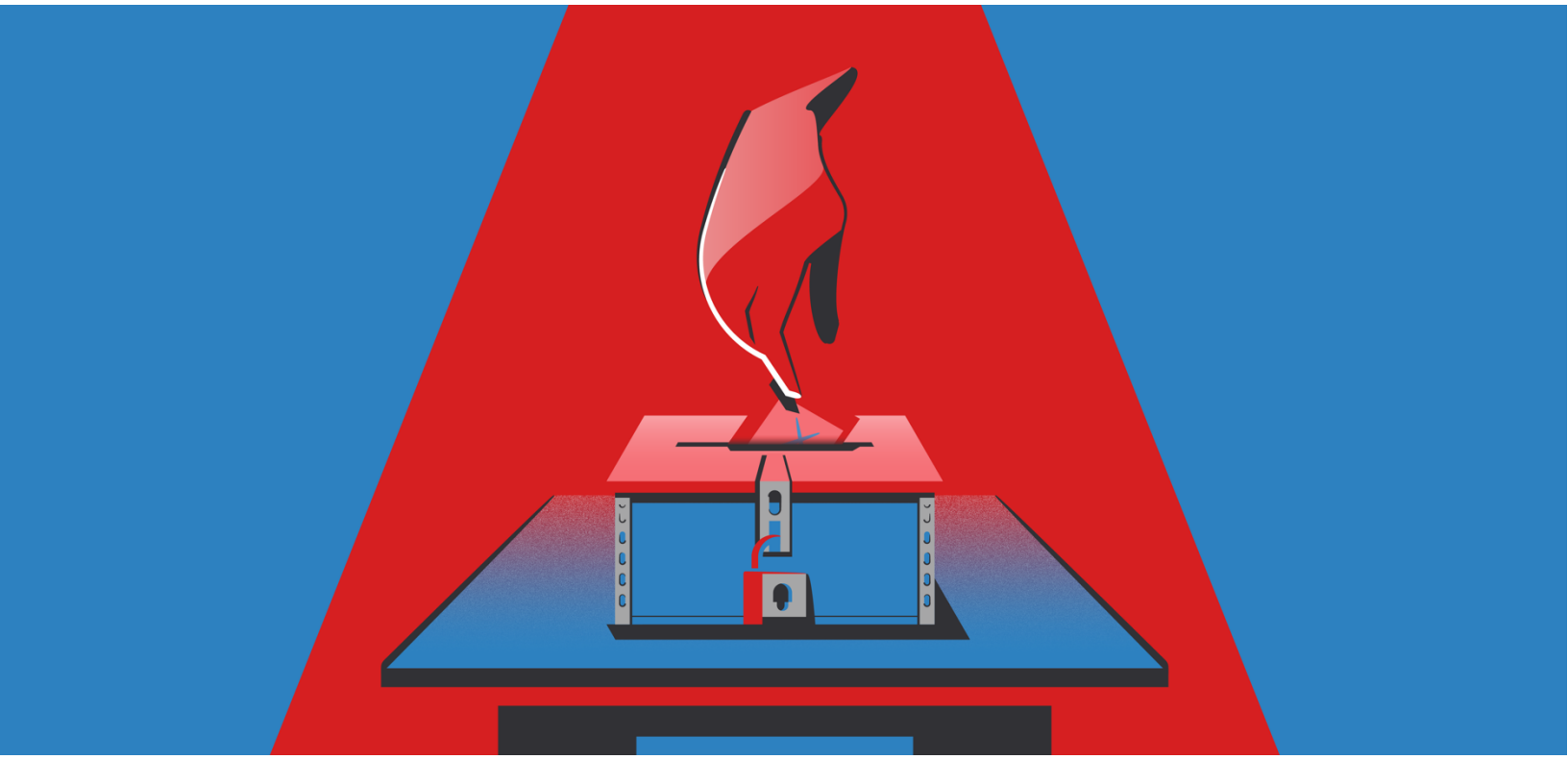

Source: Marcus Marritt, NPR

Securing American Democracy

A Forward-Looking Analysis of the Modern US Election System

Shruti Das
Institute of Electrical and Electronics Engineers
Summer 2021

WISE | WASHINGTON INTERNSHIPS for STUDENTS of ENGINEERING

IEEE-USA

"If you think technology can solve our voting problems, then you don't understand the problems and you don't understand the technology."

— Sarah Rovito

Former IEEE-USA WISE Intern and Congressional Fellow

"We have to decide that the goal of our election system is for the most people to be able to vote with the least amount of effort. We have already declared our election system to be critical national infrastructure. We can do much more. We owe it to democracy to do it."

— Bruce Schneier

Fellow & Lecturer at Harvard Kennedy School

"My position hasn't changed over the years. Which is that online voting is a very unsafe idea and a very bad idea and something I think no technological breakthrough I can foresee can ever change.

— Aviel D. Rubin

Professor of Computer Science at Johns Hopkins University

Foreword

About the Author

Shruti Das holds a Bachelor's degree in Computer Engineering from the University of Maryland (UMD) located in College Park, Maryland. In addition to being involved in the UMD IEEE student chapter, she assisted in human-centered computer security research at the SP2 Lab within the Maryland Cybersecurity Center. In 2019, she was the Co-Executive Director for Technica, the world's largest hackathon for underrepresented genders, where she oversaw 900+ participants and an organizing team of 80+ students. Starting in October 2021, Shruti will be joining Apple as a Software Engineer in the San Francisco Bay Area.

About the WISE Program

The Washington Internships for Students of Engineering (WISE) program was founded in 1980 through the collaborative efforts of several professional engineering societies and has become one of the premier Washington internship programs. Each summer, the WISE societies select outstanding 3rd or 4th year engineering and computer science students, or students in engineering and computer science graduate programs, from a nation-wide pool of applicants. The students gain exposure to legislative and regulatory policymaking through leaders in the Administration, federal agencies, and advocacy groups. In addition, each student is responsible for independently researching, writing, and presenting a paper on a topical engineering-related public policy issue that is important to the sponsoring society. For more information about the WISE program, visit www.wise-intern.org.

About IEEE

The Institute of Electrical and Electronics Engineers is the world's largest technical and professional organization dedicated to advancing technology for the benefit of humanity. IEEE and its members inspire a global community through its highly cited publications, conferences, technology standards, and professional and educational activities. There are more than 422,000 members in more than 160 countries, with more than 50% outside the United States. It includes 543 affinity groups, 39 technical societies, 4.5 million publications, over 1,250 active standards, and more than 1,900 conferences in 103 countries a year.

Acknowledgements

Special thank you to my IEEE-USA hosts Erica Wissolik, Russell Harrison, James Savage, Aline McNaull, and especially to our Faculty Member in Residence, Mark Ames. I would also like to thank Sarah Rovito, Dr. Tomoko Steen, Dr. Will Adler, Nathan Smith, Dr. Janet Abbate, Dr. J.P. Auffret, and Susan Reed for their expertise, mentorship, and editing assistance. Finally, I would like to express my sincere gratitude towards my fellow intern cohort for their continuous support and friendship this summer.

Acronyms

BMD	Ballot Marking Device
CARES	Coronavirus Aid, Relief, and Economic Security Act
CISA	Cybersecurity and Infrastructure Security Agency
DoD	US Department of Defense
DoS	Denial-of-Service
DHS	US Department of Homeland Security
DRE	Direct Recording Electronic (voting machine)
E2E-V	End-To-End Verifiability
EAC	US Election Assistance Commission
ECC	Elliptic Curve Cryptography
ES&S	Election Systems & Software
EAVS	Election Administration and Voting Survey
FBI	Federal Bureau of Investigation
FEC	Federal Election Commission
HAVA	Help America Vote Act of 2002
IEEE	Institute of Electrical and Electronics Engineers
IFES	International Foundation for Electoral Systems
IMb®	Intelligent Mail Barcode
IT	Information Technology
IoT	Internet of Things
MOVE	Military and Overseas Voters Empowerment Act of 2009
NASEM	National Academies of Sciences, Engineering and Medicine
NCLS	National Conference of State Legislatures
NIST	National Institute of Standards and Technology
OECD	Organization for Economic Co-operation and Development
OSET	Open Source Election Technology
RSA	Rivest-Shamir-Adleman (public-key cryptography system)
TGDC	Technical Guidelines Development Committee
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act of 1986
USPS	United States Postal Service
VAP	Voting-Age Population
VEP	Voting-Eligible Population
VRD	Voter Registration Database
VVPAT	Voter Verifiable Paper Audit Trail
VVSG	Voluntary Voting System Guidelines

Table of Contents

Executive Summary

In an age of high-risk election interference, voter suppression, and digital mis- and disinformation, American democracy has weathered the numerous challenges associated with a 21st century election system. 2020 was no exception as the nation overcame a grueling election cycle during the strains of a global pandemic. Once again, the US must preemptively acclimate its national security agenda to protect the sanctity of elections.

When looking to the next frontier of voting innovation, secure online voting proposes an intriguing vision for the future of elections. Yet, experts frequently warn against the notion. As Murphy's Law teaches, whatever can go wrong, will go wrong; this is a particularly apt depiction of what a dependency on nascent voting technologies could result in. Rather than striving for an increased reliance on technology, engineers and policymakers must critically analyze the legislative shortcomings that have commonly plagued election infrastructure. The federal government should address these issues through the following legal avenues and policy recommendations:

1) **Reinforce security and accessibility standards.** The federal government should encourage that states meet federal standards recommended by the EAC and NIST.
2) **Streamline federal election assistance.** Federal support should be efficiently and equitably allocated to immediately reciprocate local needs, but also sustainably and pro-actively support states in achieving long-term improvements.
3) **Promote innovation in the election technology sector.** Congress should expand relationships across public, private, and academic institutions to accelerate growth of open-source election technology and encourage local officials to hold vendors accountable.

These recommendations will empower state legislators and local officials to combat matters of election security and strengthen confidence in their constituents, while continually researching emerging technologies. Future voting solutions will require a new level of ingenuity and creativity where security, reliability, accessibility, and verifiability are the benchmarks for evaluating the effectiveness of American democracy.

1. Introduction

The United States remains to be the longest-standing democracy in the world [1]. Since 1789, the Constitution has promised to create and sustain a government that serves all[1] its citizens [2]. Amongst the many existing democracies, very few choose to hold elections as frequently as the US does. Experts speculate a few reasons why other nations have yet to model a system after the US electorate [3]. Principally, hosting federal elections are immensely complex endeavors but still, the US manages to undertake such a feat every[2] two years. For more than two centuries, American democracy has been upheld, in large part, by the dispersed nature of the US election infrastructure.

In a joint statement from the Elections Infrastructure Government Coordinating Council (GCC), Cybersecurity and Infrastructure Security Agency (CISA), and several other departmental agencies, the 2020 election was deemed to be "the most secure [election] in American history" [4]. Although election officials managed to operationally tackle the residual threats from 2016, the democratic process was still publicly undermined by the very people Americans had entrusted into power [5]. Now, experts believe the widely regarded success of the 2020 election will "prove to be hard to replicate in future election cycles" without proper investment and reinforcement [6].

The reality is that election administration remains underfunded and unpredictable. While politicians regularly pour billions of dollars into election campaigns, the country comparatively spends a fraction of that cost towards critical election infrastructure [7]. Therefore, in an attempt to mitigate future risks, policymakers must champion the election ecosystem through immediate infrastructural innovation and longstanding social reform.

1.1. Election Administration in the United States

Elections in the US are highly decentralized down to local districts — precincts are usually subdivided at the county, city, or town levels [8]. Referring back to the Constitution, Article I Section 4 grants power to the states to regulate voter eligibility and run their own elections [9]. As of 2020, this duty has been split across more than 10,000 state jurisdictions. As a result, the electoral system encompasses diverse

[1] Delivering the promise of democracy is an ongoing process — one which was not fully realized until the unanimous 1922 Supreme Court decision which defended women's voting rights and ratification of the 24th Amendment in 1964 which eliminated poll taxes keeping African Americans from voting.

[2] Special elections are held to temporarily fill vacancies for members of Congress in both even and odd years. Kentucky, Louisiana, Mississippi, New Jersey, and Virginia, hold major general elections in odd-numbered years.

methods of operations with each polling location facing its own unique obstacles and funding requirements [10]. In particular, ballot casting and tabulation varies considerably between local polling stations. These various mechanisms are further detailed in Section 2.2.

Generally, voters are eligible to vote in the jurisdiction which is associated with their home address. When a voter moves to a new state, he or she must re-register since information from prior states' registration rolls do not carry over. This leads to the common occurrence of voters appearing on multiple states' voter registration rolls[3] [12]. In 2002, Congress established that states must adhere to a "single, uniform, official, centralized, interactive computerized statewide voter registration list" [13]. This requires each state's voter registration database (VRD) to reflect up-to-date information about changes in voters' addresses, names, or affiliation.

Figure 1 below gives a high-level overview of the election process from start to finish. The phases are cyclically depicted, emphasizing that elections are administered through an ongoing[4] series of events [14].

Figure 1. 6 Stages of US Election Process

According to the US Census Bureau, 2020 experienced the highest voter turnout since 1992 totaling at 66.8% (158.4 million) among voting-age population[5] (VAP) [16].

---

[3] Appearing on multiple voter rolls does not equate to voter eligibility. Voters are only eligible to vote in one state, regardless of how many rolls they are registered in [11].

[4] The EAVS is administered every two years following a federal election so that laws, rules, policies, and procedures can be revisited and ratified before the start of the next election cycle.

[5] When calculating voter turnout, using denominator of VAP (citizens 18 years and older) instead of voter-eligible population (VEP) can skew rates [15].

Historically, voter turnout rates tend to fluctuate between midterm and presidential election years. Public policy experts consistently study turnout levels because they signal the health of a democracy [17]. In spite of recent upward trends, IFES research suggests that the US still lags behind the international community in democratic participation. For many other developed democracies, compulsory voting and automatic voter registration has led some nations[6] to turnout rates nearing 90% [18].

2. Background

2.1. Secure Voting Requirements

Trust in the American electoral process has, time and again, been proven to be extremely fragile. Hence, DHS and CISA have deemed safeguarding elections to be one of the nation's highest security priorities [19]. State and local governments, election officials, and technology vendors are amongst some of the fiercest defenders responsible for passing legislation and enacting policies that define fair and free elections. The following five criteria form the basis of systems that reflect free expression and the will of the people [20].

(i) Integrity: the votes are cast as intended and the votes are counted as cast
(ii) Secrecy: nobody can figure out how someone voted, even if the voter tries to prove it, ensuring receipt freeness and coercion resistance
(iii) Authentication: only authorized voters can cast votes and each voter can only vote up to the permitted number of times, according to state laws
(iv) Enfranchisement: all authorized voters have the opportunity to vote
(v) Availability: election system is able to accept all votes on schedule and produce results in a timely manner

Security rarely comes for free and this realistically depicted by the various tradeoffs that arise between pairs of requirements [21]. For instance, one can imagine that integrity and secrecy are fundamentally in conflict with one another. Consider the following example: a final exam is being administered with the aim of ensuring high integrity. It is, therefore, unlikely that the professor would allow a student to submit the exam without verifying his or her identity. The integrity of the exam is dependent on the fact that each student took his or her own exam. If the professor was no longer able to trace each exam back to each individual student, the exam's integrity would be in question. Similarly, a sovereignty may wish to improve voting access by waiving the need for early registration or valid identification. While this might enfranchise more citizens, it might also allow foreign adversaries to freely participate on the claim that

[6] Turkey, Sweden, and Australia consistently rank highest in voter turnout among OECD nations [18].

they were also entitled to vote. Throughout history, voting schemes have long struggled to enforce a comfortable balance between all five requirements [22]. The exact recipe for success is not always clear — public policy experts are often left to deciding which security pillars are absolutely necessary and which concessions can be made for the sake of progress.

In some ways, civic technology is now addressing classical security tradeoffs in ways that Americans twenty years ago could not have imagined possible. With the Internet's omnipresence, government officials are now leveraging online platforms to engage with the public and mobilize social change [23]. This phenomena is often referred to as a "digital democracy" or "e-government" which utilizes the Internet along with other computer technologies to enhance governance processes [24]. Thus, in attempts to increase voter turnout[7], some public officials are envisioning a future where the >200 million registered Americans can participate in online elections[8] [26].

While the initial concept might sound appealing, experts have long debated the integrity and feasibility of hosting online federal elections [22]. If the events of the 2016 presidential election have taught Americans anything, it is that election security must not be taken for granted [27]. So it was no surprise that the scientific community expressed significant unease when states contemplated online elections in 2020 [28]. In a recent letter, many cybersecurity experts implored the DHS, EAC, and FBI to urgently remind states of the tremendous security risks that internet-based voting systems pose [29]. When looking to secure a digital democracy, innovative election technology may certainly help alleviate factors of cost, accessibility, and convenience but should never be compromised over security and integrity [30].

It is reasonable to wonder why internet-based voting solutions cannot be properly engineered while millions of other services are ubiquitously and securely conducted online. The imminent dangers of fraud, coercion, and foreign interference have always played a huge role in traditional elections. But when assessing the speed at which information travels through the Internet, the stakes become drastically higher. This scope presents possibilities where adversaries can massively hinder millions of votes; a scenario that is unimaginable in physical paper-ballot elections. Attacks on physical voting systems simply don't scale. Furthermore, the need for a secret ballot introduces additional layers of complexity that cannot be understated [31]. Consider, for example, the case of online shopping or banking services. Both Capital One and Amazon have established the user's identity and have appropriate methods of verifying these transactions with this identity in the case of errors. Ultimately, what

[7] It remains inconclusive whether online voting actually increases voter turnout. Research speculates whether it could conversely increase disenfranchisement [25].

[8] Refer to Section 4.2 for international online voting implementations.

makes voting so different from other online activities, is the designation of two tenets: anonymity and security [21]. With the existence of one, it becomes increasingly difficult to ensure the other, especially on the Internet. Discussions surrounding internet voting is further explained in Section 4.1.

2.2. Vote Casting & Tabulation Methods

Election technology plays an integral role in upholding the critical infrastructure of democracy. Traditionally, it had been compulsory for eligible voters to physically travel to their designated polling booth on Election Day. Over time, accessibility improved for numerous voter groups — including deployed soldiers, overseas citizens, disabled populations, out-of-state college students, and more. Today, Americans cast their ballots in one of three ways: in-person, vote-by-mail[9], or digitally from a remote location[10]. Figure 2 provides an overview of election infrastructure (not including digital remote voting) and how the entire system operates before, during, and after election day [32].

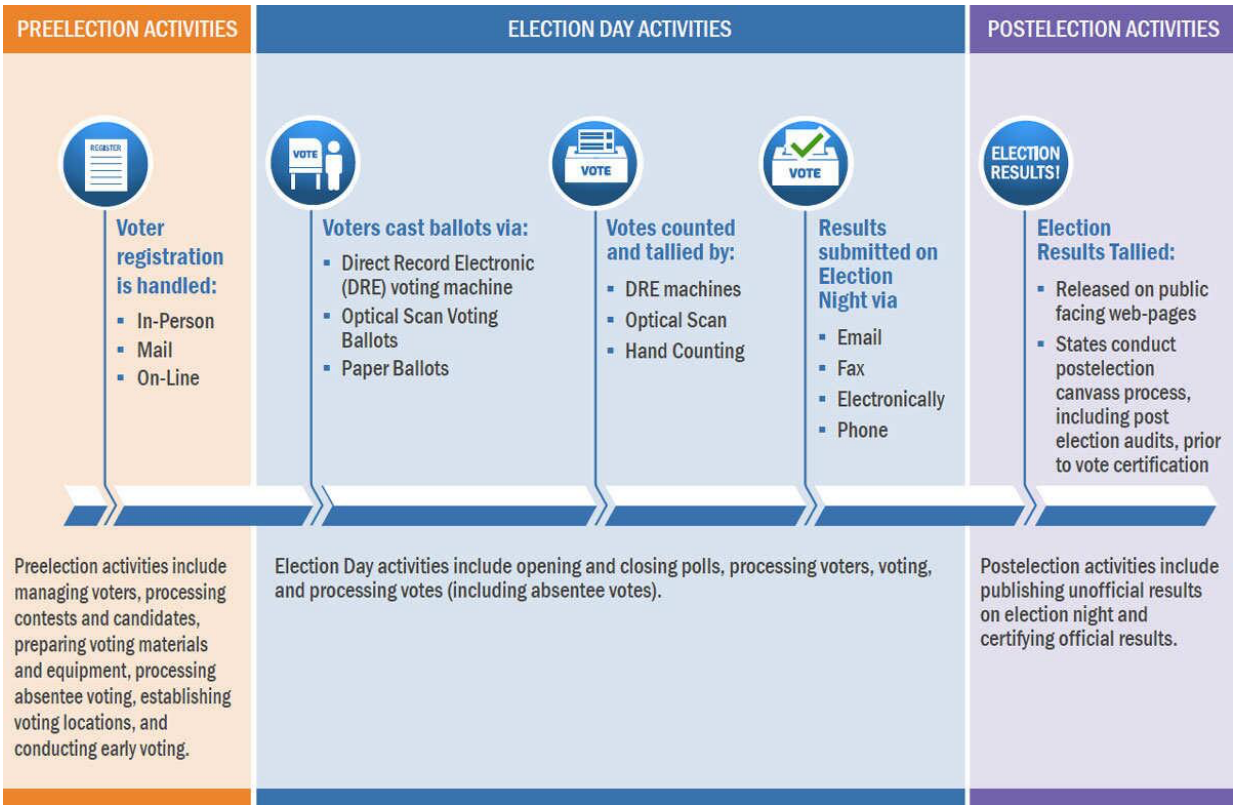

Figure 2. General Overview of US Election Infrastructure

[9] Depending on the state, vote-by-mail is synonymous with mail-in voting, early voting, and absentee voting. This paper will be using the term vote-by-mail.

[10] Reserved only for military and overseas voters.

Paper ballots cast in-person are far less susceptible to large-scale interference and have, for good reason, been accepted as the most resilient form of voting [33]. Paper-based voting can, however, be extremely prone to logistical errors. From stray pen lines and tears to the arduous tallying process, electronic voting or e-voting has ostensibly modernized voting. Since 2002, the US has seen a rapid progression of e-voting systems and tabulation methods [13]. Below is a brief overview highlighting key differences between the types of voting equipment [34].

(1) **Optical Scan Paper Ballot Systems** are scanning devices that tabulate hand-marked paper ballots. Ballots may either be scanned on optical scan systems in the precinct polling place or collected in a ballot box to be scanned at a central location. Older optical scan systems have infrared capabilities to scan ballots according to the timing marks on the edges. Newer systems scan ballots digitally.
(2) **Ballot-Marking Devices (BMDs)**, which can also be referred to as machine-marked paper ballot systems, are computerized devices that display a digital ballot, allow voters to make selections, then print a paper record of the voters' choices. BMDs can be enabled with accessible user interfaces, providing essential assistive technology for voters that may be unable or uncomfortable marking a paper ballot by hand.
(3) **Hand Counted Paper Ballots** is the system of tabulating votes without any technological assistance. This method is normally reserved for much smaller jurisdictions or for counting absentee and provisional ballots.
(4) **Direct Recording Electronic (DRE) Systems** record voter selections directly into computer memory via a pushbutton, touchscreen or dial user-interface. The choices are then stored either in a memory cartridge, diskette, or smart card and automatically tabulated by the machine.
(5) **Punch Card Voting Systems**[11] **(discontinued)**
(6) **Mechanical Lever Voting Systems**[12] **(discontinued)**

Regardless of the new efficiencies found in e-voting, the equipment also introduced many features, which are now known to be, acutely exposed to attacks. Following the investigations of the 2016 election, US intelligence officials declared that any e-voting system which does not produce a paper record or allow for voter verification should be abandoned altogether [5]. In 2018, the NASEM released a report urging all states to adopt paper ballots by the 2020 election. For this reason, DREs

[11] In 1996, 20.7% of US registered voters used mechanical lever machines. As of 2010, all jurisdictions have discontinued these machines and they are no longer federally in use [35].

[12] After causing many tabulation irregularities during the 2000 election, jurisdictions moved towards discontinuing punch card voting systems. By the 2016 election, they were no longer in use [35].

have been increasingly equipped with a voter-verifiable paper audit trail (VVPAT), allowing voters to independently confirm their selections by printing a paper record before casting their vote. The paper record is then preserved and may serve as the ballot of record during an audit or recount due to malfunction [8]. Compared to 2016 where only 79% of votes maintained a paper trail, nearly 90% of votes in 2020 were cast with some sort of paper record [36]. However, in the absence of sufficient funds, some states continue to circulate paperless voting systems.

The Verified Voting Foundation maintains a detailed record of the polling place equipment operated by each voting district. The foundation regularly gathers information from local election officials, state-level mandates, and certification documents in order to make accurate directories for voting systems [37]. Based on the map in Figure 3, which visualizes projected polling place equipment in 2022, it is clear a number states are still at high-risk from using unreliable DREs with no paper trail.

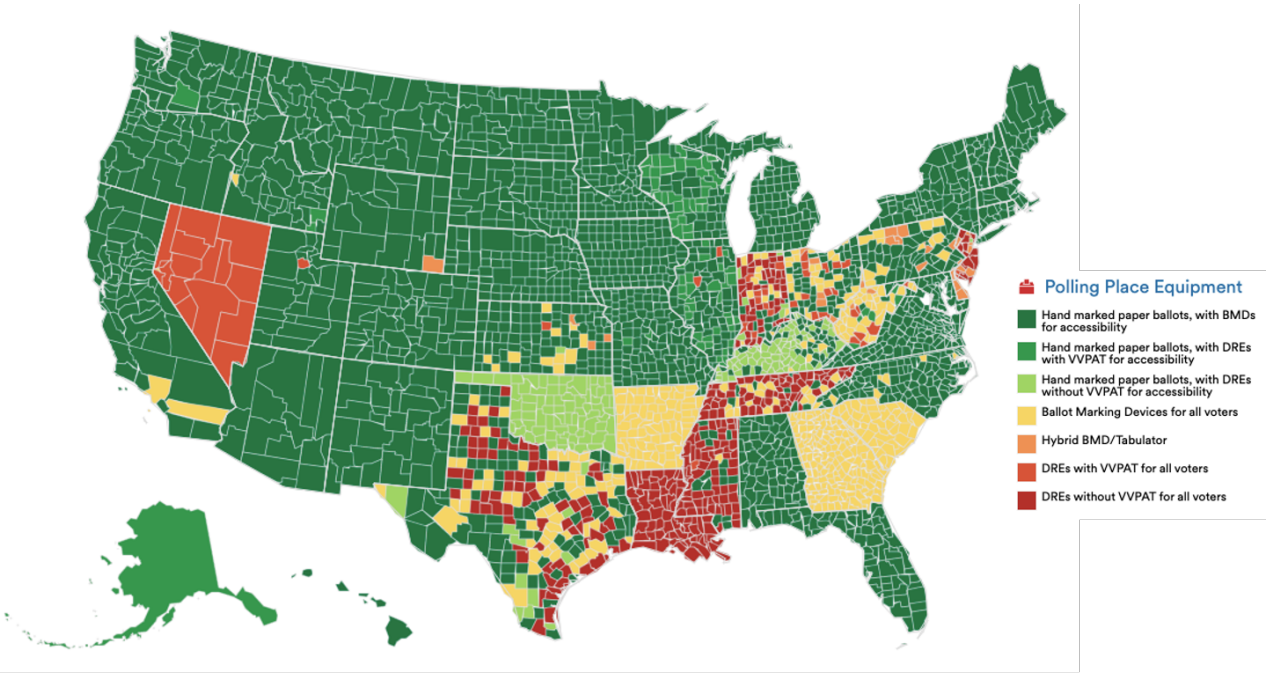

Figure 3. Polling Place Equipment in 2022

Generally, the software used for e-voting systems is considered proprietary and is subject to very little oversight and regulation [38]. However, open-source software[13] has gained some traction amongst election administrators in recent years. States typically install commerical off-the-shelf operating systems which are packaged together with a set of hardware and maintenance services [39].

[13] The benefits of using open-source software are further discussed under the policy recommendations in Section 5.3.

Created through the passage of HAVA in 2002, the Election Assistance Commission (EAC) is an independent agency that is responsible for developing and administering voluntary guidance and federal certification of voting systems [40]. Along with the technical expertise of the NIST, the EAC drafted lifecycle policy for the past, present, and future of elections.

As of February 2020, the Technical Guidelines Development Committee (TGDC) voted for the second iteration of the Voluntary Voting System Guidelines (VVSG 2.0) to be circulated for public review. While the VVSG recommends hardware and software testing specifications, voting equipment certification is mainly carried out under state authority. The EAC has since adopted VVSG 2.0 which focuses on major functional changes that states should consider, detailed below [41].

(1) stricter cybersecurity requirements of election management systems (i.e. software independence[14], physical security, multi-factor authentication, system integrity, data protection)
(2) interoperability to ensure encoded data uses publicly available methods and can be formatted between devices
(3) improved accessibility requirements for voters with disabilities
(4) improved auditability
(5) improved user-centered design
(6) updated manuals in penetration and component testing

3. Current Regulatory Environment

As mentioned before, it is the state legislatures which prescribe the exact details of election administration. However, Congress has periodically retained some power over election administration when it comes to altering regulations or setting national standards. The general legal framework views Congress as a supervisory power that may supplement state regulations and occasionally substitute its own [43].

Most notably, Congress passed the Civil Rights Acts of 1870, 1957, 1960, 1964, and 1965 which federally expanded protection against voter discrimination [44]. In 1975, Congress established the Federal Election Commission (FEC) to enforce federal campaign finance laws and regulate campaigns for the presidency, vice presidency, Senate, and House of Representatives [45]. Here is an overview of the federal legislation passed in recent years that have expanded voting rights:

[14] Deems "a voting system software-independent if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome" [42]

- **The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986** allowed members of the armed forces and overseas voters to vote by mail [46].
- **The National Voter Registration Act of 1993** created a national voter registration form, new registration methods, and call for states to keep more accurate voter registration lists [47].
- **The Help America Vote Act (HAVA) of 2002** provided federal funds to update voting equipment, create the EAC to offer guidance to state election administration, and help states comply with minimum voting standards surrounding education, registration, and ballots [48].
- **The Military and Overseas Voting Empowerment (MOVE) Act of 2009** improved access to voting for military and overseas voters. Both UOCAVA and MOVE are overseen by the DoD's Federal Voting Assistance Program [49].

3.1. Impact of Help America Vote Act

In the aftermath of the deadlocked 2000 presidential election, a Florida recount crisis over punch card ballots revealed severe shortcomings in the electoral system. From unreliable voter registration rolls, obsolete voting machines, poorly designed ballots, and the infamous "hanging chads" voter cards nightmare, the list simply went on [50]. In 2002, former President George W. Bush, with joint bipartisan support, signed HAVA into law which appropriated several billion dollars to remedy future voting system irregularities [13].

Within a few short months, Georgia became the first state to adopt paperless [15] DRE systems, deploying them to every county through the use of state funds [51]. DRE systems rose to prominence across the nation as government entities everywhere upgraded DREs to be their primary polling place equipment [8]. But very few critically questioned the security guarantees that the machine vendors boasted. In short, the passage of HAVA dramatically accelerated the computerization of voting systems with little, to no, IT security training for election officials.

In 2003, computer security experts conducted the first independent security analysis about DREs based on source code they found on the Internet. Their report disclosed critical security concerns and concluded DREs *should not be used* for federal elections [52]. Further demonstrations uncovered vulnerabilities in e-voting machines where hackers managed to change mock election outcomes and go unnoticed [53].

Flash forward to 2016, the international debate over the use of e-voting machines is still ongoing. While the Senate Intelligence Committee found "no evidence that any

[15] Paperless refers to the lack of VVPAT-backed systems used to audit voting machines.

votes were changed or that any voting machines were manipulated", what the Russian government achieved was, in fact, was far worse [5]. Russian cyber actors may not have altered a single vote but in launching its massively coordinated mis- and disinformation attack, the nation-state ensued chaos surrounding the integrity of the election and successfully undermined confidence in the American electoral system.

3.2. For the People Act of 2021

H.R. 1 For the People Act of 2021 is a pending federal election bill in the 117th Congress. The bill calls for comprehensive, structural democracy reform that will expand voting rights, enforce stricter campaign finance laws, ban partisan gerrymandering, and create new set of ethics for federal officeholders [54]. Those in favor, assert that the bill's key provisions will make American democracy "fairer, stronger, and more inclusive" [55]. Much of the bill affirms federal authority to regulate congressional elections through enforcement of the Fourteenth and Fifteenth Amendments. In March of 2021, the bill passed in the House of Representatives and has since been introduced and received in the Senate as S. 1.

Despite receiving popular support, leading opponents have labeled S. 1 as a "partisan power grab" by rigging the system in the Democrats' favor. At the May Senate hearing, some claimed this bill would permit "millions of people to vote illegally" [56]. Other major criticisms are that the bill is far too broad and ambitious with its scope. But its defenders argue that the bill's comprehensive is actually its greatest strength by attracting "a vast and unprecedented coalition of civil rights activists, labor organizers, faith-based organizations, environmental groups, consumer advocates, voting rights experts, and many others" [57].

3.3. Voter Empowerment Act of 2021

S.954 Voter Empowerment Act of 2021 was introduced by the Senate in the 117th Congress. The bill is meant to "modernize voter registration, promote access to voting for individuals with disabilities, protect the ability of individuals to exercise the right to vote in elections for Federal office, and for other purposes" [58]. The bill has been read twice and since referred to the Committee on Rules and Administration.

4. Future of Voting Technology

4.1. Shortcomings of Internet Voting

Not to be mistaken for e-voting — secure voting through the Internet, or i-voting, remains one of the most open-ended research challenges within the technology governance space. Since 2009, special populations of military and overseas voters have participated in i-voting under state provisions which broaden the scopes of

UOCAVA and MOVE. In 2018, an estimated 3 million eligible voters resided overseas [59]. In light of COVID-19 restrictions, a handful of states considered expanding i-voting privileges to the masses in 2020, but not without spurring considerable controversy. The lingering debate over i-voting alludes to one of the core tensions in election infrastructure: voting accessibility versus voting security.

First and foremost, the concept of "end-to-end verifiability" or E2E-V is exceptionally important in the examination of prospective i-voting technologies. An election is E2E-V if both the following properties are met:

(1) individual verifiability: voters can verify the accurate recording of their votes
(2) universal verifiability: anyone can verify the accurate tallying of the recorded votes [60]

Some argue that public distributed ledger technology provides a promising illustration of E2E-V schemes by allowing voters to check whether their vote was cast on a publicly viewable "bulletin board" [61]. In its most primitive form, blockchain technology[16] exemplifies this concept. All the data is put into "blocks" which are then encrypted and timestamped so that the full voting record is publicly accessible by everyone, but personally identifiable information remains protected. Since everyone holds a copy of this ledger, the historical record cannot be changed, and illegitimate votes cannot be added to the "chain" [62]. The premise of the E2E-V scheme is satisfied since the voting record can be easily verified and the entire database of transactions cannot be taken down as it does not exist in a single place.

During the 2018 midterm elections, West Virginia became the first US state to pilot i-voting through a blockchain-based mobile voting solution called Voatz [62]. Governor Jim Justice extended UOCAVA to cover West Virginia's higher-than-average disabled voter population, enabling nearly 30% of West Virginians to vote online [63]. Although the platform boasted the use of "cutting-edge security", biometrics, hardware-backed key storage, and mix-nets [17], much of Voatz's "proprietary technology" was kept under wraps [30]. Not soon after, a team of MIT researchers released a troubling report denouncing Voatz's platform after finding, if hacked, they could change the individual votes casted on the Voatz's server altogether [64]. Regardless of Voatz's claim to using blockchain technology, the "secure" app-server vote transmission was clearly not E2E-V certified.

Furthermore, MIT recently conducted another independent security analysis of the Democracy Live platform, OmniBallot Online, a fully accessible, HAVA-compliant i-

[16] Not to be confused with cryptocurrencies like Bitcoin. In this context, Blockchain is the system of recording information in a way that makes it difficult to change, hack, or cheat the system.

[17] Mix-nets routing protocols create hard-to-trace communications by using a chain of proxy servers known as mixes.

voting system deployed for thousands of military and overseas voters. The analysis revealed critical security flaws that compromise "personally identifiable information including the voter's identity, ballot selections, and browser fingerprint" [65]. In response, Democracy Live acknowledged that no i-voting system can be 100% secure. Apart from a few more pilots in Oregon, Utah, and Colorado, glaring security issues and public outcry have led the US to mostly abandon its efforts in finding national i-voting strategies [25]. Plainly put, these trials confirmed that current online solutions are not comprehensive enough to be able to ensure the five basic security requirements[18] of fair and free elections.

4.2. Global Voting Advancements

Advanced cryptographic breakthroughs in recent years have persuaded some governments that i-voting systems are the next-generation of voting infrastructure. Today, at least 23 major countries have begun seriously investigating online elections in efforts to revitalize democratic participation, making it more efficient and universally accessible. While conceivable implementations of i-voting systems do exist, careful and thorough cost-benefit analysis is required before fully embracing any one of these systems.

Presently, the paradigm of i-voting is in limited use around the world — Estonia remains to be the only country to have fully modeled and successfully deployed such a system. Since 2005, the Baltic state has grown its e-governance to ensuring 99% of their public services are available online 24 hours a day, 7 days a week [66]. In their 2015 parliamentary election, 30.5% of all votes were cast through the Estonian national i-voting system [67]. The system is facilitated by the use of digital national identification cards, each containing two asymmetric (RSA or ECC) cryptographic keys with corresponding public-key certificates [68]. Originally introduced in 2002, Estonians use the digital signature keys that are encrypted on their physical ID card as their legally binding signature. When accessing any basic government service or transaction, they simply insert the physical ID into a card reader connected to any computer or smartphone and complete two-factor authentication [69]. Another necessary facet of i-voting systems is ensuring that the ballot does indeed reflect voter intent. Estonians are able to cast their ballots multiple times over a ten-day window, with each vote overriding the last. This gives some assurance that even if a voter was intimidated or coerced, they are able to recast their vote at a later time [69].

A number of countries have since followed Estonia's lead in incorporating i-voting into their systems, but many are still in the stages of developing proof-of-works

[18] Refer to Section 2.1 for the five security requirements of free and fair elections.

before scaling up to national elections. In 2012, Norway ran a pilot project where they individually verified votes using the concept of "return codes" which effectively replaces the notion of a public bulletin board [70]. In 2016, Ukrainian election officials approved an Ethereum vote-casting platform called E-vox to be integrated into online and smartphone voting applications. The platform uses government and bank-issued digital signatures for voter authentication [71]. In 2017, Switzerland began experimenting with another Ethereum-based mobile i-voting application for small-scale government elections. Nearly 300 blockchain-based electronic IDs were issued in the Zug municipality, also known as Switzerland's "Crypto Valley" [72].

2018 marked the year where several countries announced prototyping multiple blockchain-based i-voting systems. In South Korea, the National Election Commission announced their i-voting system as K-voting. Among these also included Japan's Tsukuba city council elections, Spain's autonomous community of Catalonia, Thailand's Democrat Party, Sierra Leone's presidential election, and Russia's Moscow City Duma election [73]. In lieu of the May 2020 consular elections, the Ministry for Europe and Foreign Affairs sanctioned an i-voting platform for French citizens living abroad [74]. As it stands today, expert consensus remains that more research is required before progressive rollout to the masses.

With that being said, the US is more than 200 times larger than Estonia, with a population comparable to the size of Maine [75]. Although the security that underpins the blockchain architecture is largely considered to be hack-proof, problems begin to arise with remote voting outside of the physical polling stations. Even with a zero-trust security model [19], thorough end-to-end testing of mobile i-voting systems has revealed ballots are still vulnerable to tampering [77]. The cybersecurity arm of the DHS released a bulletin alongside the FBI that warned states about the dangers of i-voting systems asserting, "securing the return of voted ballots via the internet while ensuring ballot integrity and maintaining voter privacy is difficult, *if not impossible*, at this time" [78].

Casting votes through personal mobile devices is an abstraction to be extremely wary of. The insecurity of personal computers, tablets, and smartphones range far and wide, dramatically increasing the number of entry points in which an attack could take place. Attackers could firstly infect voters' personal devices with vote-tampering malware. Not to mention, experts have routinely estimated that at least 30% of computers in the US are already infected with some form of malware [79]. Consequently, the jeopardized devices could propagate the worm or virus to election servers and largely go undetected. From there, attackers can covertly hijack the

[19] Zero-trust refers to the security governance model that assigns the least required access needed to perform specific tasks to maintain a secure network [76].

servers with a slew of man-in-the-middle attacks which would ultimately interfere with the ballots before they reached the server. The anonymous ballot makes it all the more difficult to distinguish malware from a legitimate voter, especially when anti-malware software can be subverted [80].

Another massive concern with mobile i-voting involves attackers launching a denial-of-service (DoS) attack with armies of "botnets" or mobs of malicious computers that are created upon infection [81]. These further spread spam and other forms of malware that inundate voting servers with garbage traffic, preventing actual voters from being able to cast their ballot. This was painfully depicted during the 2007 distributed DoS cyberattack targeting Estonian government portals, news outlets, internet service providers, major banks, and small businesses over a three-week period [82]. To illustrate this point even further, a team of researchers from the University of Michigan simulated an analytical cyberattack on the i-voting system used during the 2013 Estonian elections. The team was able to exploit a number of the software's vulnerabilities among which included a severe barrage of the voter verification channel [83]. This completely compromised the integrity of the vote and the researchers were able to surreptitiously override previous voters without alerting the security measures put in place by the Estonian Election Commission.

The science is clear: no i-voting system can be completely secure against all cyberattacks. It can be concluded that i-voting systems function on the foundation of trust: citizens must have underlying faith that no single party or foreign entity will attempt to usurp power [84]. Until this basic sentiment can be reached, national i-voting systems are just unrealistic.

5. Viable Policy Directions

Due to the decentralized characteristics of the US election system, issues of state and local autonomy are rather tricky topics to navigate. Thus, hybrid policy solutions must be carefully considered in order to level set the national voting regime and unify processes that are currently disjointed. The following recommendations account for complex election law tradeoffs in facilitating open collaboration between election professionals at the local, state, and federal levels.

5.1. Reinforce Security and Accessibility Standards

It is clear that voting access and voting security are two essential pillars for democracy, but prioritizing one often comes at the expense of the other. When voting equipment is eventually replaced, it is usually due to competing security and safety concerns, while accessibility and efficiency requests get placed on the backburner. Juan Gilbert, who studies accessible voting systems, testified in a House hearing, "the

most secure thing in the world, whatever it is, is going to be the most inaccessible thing, just by definition" [85]. Therefore, there should be a federal push towards easing tensions between security and accessibility priorities while also setting national standards for state and local governments to work towards.

5.1.a. Federal agencies should routinely assess statewide security and accessibility guidelines. The NASEM released a 2018 report detailing the as seen by Figure 4. From this table, it is clear that most states either meet federal standards or have implemented their own stricter set of standards. However, eight states still have not election certification requirements and could present liabilities to national security. The states that have yet to disclose security and accessibility standards are: Florida, Maine, Montana, Nebraska, New Hampshire, New Jersey, Oklahoma, and Vermont [8].

States Requiring Testing to Federal Standards	States Requiring Testing by a Federally Accredited Laboratory	States Requiring Full Federal Certification (in Statute or Rule)
Connecticut, DC, Hawaii, Indiana, Kentucky, Nevada, New York, Tennessee, Texas, and Virginia	Alabama, Arkansas, Arizona, Colorado, Illinois, Iowa, Louisiana, Massachusetts, Maryland, Michigan, Minnesota, Missouri, New Mexico, Oregon, Pennsylvania, Rhode Island, Utah, and Wisconsin	Delaware, Georgia, Idaho, North Carolina, North Dakota, Ohio, South Carolina, South Dakota, Washington, West Virginia, and Wyoming

Figure 4. Voting Systems Certification Standards by State

Some policymakers like Senator Amy Klobuchar of Minnesota and former Georgia House of Representatives Minority Leader Stacey Abrams have pushed for minimum voting accessibility standards to be included S. 1 For the People Act. They are pushing for states to prioritize automatic and same-day voter registration as well as longer early voting periods and no-excuse absentee voting [86]. This remains to be a point of partisan contention as Congress continues to discuss the provisions of S. 1. Nevertheless, strong cybersecurity standards should be incorporated into the standards-setting and certification processes at the federal and state levels.

5.1.b. Develop a united cybersecurity strategy with some level of standardization at the state level. It is a well-known cybersecurity notion that a system's security is only as strong as its weakest link. Therefore, state leaders play a crucial role in defending critical IT infrastructure. A prime example was former Michigan Governor, Rick Snyder, who made cybersecurity a top priority and saw to it that all IT governance be

consolidated at the state level. Michigan's 2011 and 2015 Cyber Initiatives provide excellent frameworks for collectively approaching IT risk management alongside local leaders [87]. Municipalities that lack resources and funds may struggle to adhere to a comprehensive IT strategy. To accommodate this, states can opt for a hybrid model where responsibilities then fall under the state legislatures to ensure that each district is compliant.

In May 2021, NIST released their cybersecurity playbook which examines the entire election infrastructure, offering a roadmap for local election officials to prepare and respond to election threats [39]. States can refer this to guide their cybersecurity standardization and consolidation operations. The simplest changes that states can make is helping local jurisdictions transition to dot gov (.gov) secure domains. In conjunction with the DOTGOV Online Trust in Government Act of 2020, states can funnel funding down to the local level and switch all "election websites, email addresses, and online voter-registration portals" to .gov addresses [6].

5.1.c. Consolidate all voting system issues into a nationwide incident database. To aid with the systematic upkeep and refinement of standards, Congress should oversee the creation of a publicly available, national database that accurately reports voting system malfunctions and vulnerabilities. Currently, the EAC distributes voting system reports that have been specifically commissioned or conducted by state and local governments. However, these reports follow a rather disorganized and scattered approach.

Furthermore, research suggests system failures usually persist across the same machines in different jurisdictions. Yet, election machine vendors are not always legally obligated to disclose recurring problems to other customers or federal agencies like the EAC [88]. Therefore, local election officials would greatly benefit from a publicly available, searchable, centralized online repository of past system issues.

Analogous implementations have taken shape in light of voter intimidation and suppression. The "See Something, Say Something" initiative in 2020 created an online database which enabled real-time reporting of voter intimidation, voting machine malfunctions, registration issues, polling place wait times, and more [89]. This concept can be further realized by proposing a bill that sets provisions for the exact details and requirements of such a database. In fact, the Brennan Center for Justice called for such a solution more than a decade ago, but, to this author's knowledge, no such collection has been created yet. Their 2010 report stipulated that such a database should include: (1) make and model of voting machine in question (2) jurisdiction(s) in use (3) nature of problem (4) date of discovery (5) contact

information of person submitting report and (6) verification that information reported is accurate [90].

5.2. Streamline Federal Election Assistance

The federal government assumes a nebulous role in election matters in accordance with the Constitution, but this often leaves states reckoning with chronic under-funding and aging voting technology. Despite efforts made by the Consolidated Appropriations Act of 2020 which authorized an additional $425 million in new HAVA funds, several state and local election officials have turned to private donations due to financial constraints [91]. Other times, election officials must appeal to agencies like the DoD, DHS, and FBI in order to meet operational costs.

Therefore, the recommendation for streamlining federal election support is really two-fold (1) Congress should coordinate responsive funding to efficiently deliver immediate, need-based assistance to states and (2) the EAC should assess the proactive allocation of funds towards sustainable, long-term planning.

5.2.a. Congress should routinely allocate funding and expand initiatives for the EAC. Recall that the EAC was established in 2002 by HAVA as a 'one-stop-shop' for recommended best practices, election data, and independent certification of voting systems [10]. However, inadequate funding has forced the EAC to step back in their support efforts. Between 2011 and 2019, the EAC's budget was cut in half by nearly 50% [92]. Ideally, Congress should double down on funding and consolidation efforts, seeing that election technology is considered as critical national infrastructure. However, Congress' first priority still remains to authorize election funding without overstepping state discretion. Therefore, a careful balance must be struck in order to maintain local-level authority.

Support for increasing EAC funding has already received wide bipartisan support. In a letter addressed from seventeen Secretaries of State [20], Congressional leaders were requested to increase the EAC's 2021 budget [93]. Addressed leaders included Senate Majority Leader Mitch McConnell, Minority Leader Chuck Schumer, Speaker of the House Nancy Pelosi and House Minority Leader Kevin McCarthy:

> "Therefore, as the chief election officials of our respective states, we encourage robust funds be allocated to the EAC for fiscal year 2021 for various initiatives including, but not limited to:

[20] Alabama Secretary of State John Merrill was joined alongside Kevin Meyer of Alaska, Katie Hobbs of Arizona, John Thurston of Arkansas, Paul Pate of Iowa, Scott Schwab of Kansas, Kyle Ardoin of Louisiana, Jocelyn Benson of Michigan, Steve Simon of Minnesota, Maggie Toulouse Oliver of New Mexico, Frank LaRose of Ohio, Shemia Fagan of Oregon, Nellie Gorbea of Rhode Island, Steve Barnett of South Dakota, Jim Condos of Vermont, Mac Warner of West Virginia, and Ed Buchanan of Wyoming [93].

(1) Conducting a comprehensive post-election review with a special focus on procedures implemented due to COVID-19
(2) Improving the security and auditing of election systems
(3) Implementing a robust training program available to all election officials nationwide Assembling a team of experts to research and establish non-voting technology best practices and resources to better secure voter registration systems and other election related systems that are not a part of the current testing and certification program; Implementing procedures and a process to certify electronic poll books
(4) Establishing a team dedicated to recommending improvements to the VVSG and maintaining modern and agile certification requirements; Recruiting election personnel to assist with the clearinghouse function of the EAC to disseminate election administration information to election officials and educate the public
(5) Developing web tools for voters and election officials to provide information such as deadlines, registration, legislation, voter options, education, etc.
(6) Implementing a voter helpdesk team to assist voters
(7) Increasing grant related resources to assist states with technical guidance and oversight of grant funds, including CARES Act and other HAVA grants
(8) Establishing a new Federal Advisory Committee Act Board consisting of local election officials who will serve to increase the EAC's ability to communicate with and reach local officials with relevant information related to the elections process."

5.2.b. Congress should authorize the EAC to closely supervise local election appropriation. HAVA funds have substantially decreased and no new federal legislation has called for federal election appropriations since. Rather than simply replacing local funding with federal support, congressional legislation should call for appropriations that will enhance fundamental election practices and appoint the EAC to carefully monitor equitable distribution of funds to states.

Local election offices are frequently constrained to operate under state rules, and yet in most states, there is no well-defined way of allocating the cost of operating local elections [12]. In 2018, Pennsylvania's Advisory Committee on Voting Technology voiced jurisdictions' concerns that "[they] would not be able to afford voting technology that satisfies statewide recommendations." Moreover, some expressed worries over "not [being] able to maintain their current e-voting systems for much longer" [10]. Typically, larger counties are much more well-resourced, and this disproportionately leaves smaller counties with outdated voting equipment.

According to the Harvard Belfer Center, local jurisdictions often underestimate the required costs and overestimate the amount of federal funding they would receive. Consequently, states should submit their election budgets to the EAC for regular review [62] The EAC can then use these budgets to assess if states have accurately estimated the costs of administration and modernization and make appropriate recommendations well before peak election season. On the flip side, the

EAC can advocate for states that are lagging behind in modern equipment. This way, the federal government can ensure all states are meeting minimum federal standards in security and accessibility.

5.3. Promote Innovation in the Election Technology Sector

The market for voting machines has become increasingly consolidated by three major players: Dominion Voting Systems, ES&S, and Hart InterCivic. These vendors control nearly 92% of the voting machine market with nearly half of the country voting on machines manufactured by ES&S [38]. This kind of concentration could lead to major security breaches in cases where proprietary glitches in just one vendor could ripple down to a huge portion of equipment. To combat this market dominance in election technology, the federal government has the responsibility to step in with stronger regulation of these companies and properly invest in election cybersecurity talent across all levels of government.

5.3.a. Form buyer coalitions to combat voting machine market dominance. The main purpose for election coalitions is to take advantage of economies of scale and volume discounts. Currently, election officials lack the bargaining power needed to drive election equipment prices down. A 2016 Penn Wharton Public Policy Initiative study affirmed coalitions can minimize transaction costs, strengthen buyer power, and ultimately, decrease costs per unit to produce and transport equipment [94].

Such a strategy was trialed in 2015 when the Colorado's former election commissioner pushed for a uniform system that required all local jurisdictions to switch to Dominion voting machines. Thereby, the entire state was able to negotiate a six-year contract with Dominion at nearly half the price of leading competitor costs [95]. Many counties and states have since adopted similar coalition models and seen positive success [34].

The National Conference of State Legislatures (NCSL) could act as the leading body in the formation of coalitions across states and local counties. Multiple voting districts can enter a joint contractual agreement with one or more voting machine vendors in order to facilitate cheaper bulk equipment purchases.

5.3.b. Incentivize open-source development and additional vendor oversight. Congress should lead the shift in voting infrastructure towards an open-source election technology (OSET) model. Since current vendors are not obligated to disclose how their technology actually operates, casted ballots simply disappear into a proprietary "black box", which erodes public trust and confidence. Whereas, the open-source way is inherently inclined to preserve fair and free elections — the five basic principles being (1) transparency (2) cross-collaboration (3) rapid prototyping (4) inclusive meritocracy and (5) community [96]. Furthermore, the development and

distribution of OSET is driven by public iteration without limitation. OSET projects are typically maintained by a parent organization that publishes all the source code and documentation on a version-controlled public repository like Github or Bitbucket. In this manner, practically any interested civilian, not just software developers, can propose changes and modifications. The suggestions are then reviewed by experts, usually belonging to the parent organization, who then updates the main repository. A common misconception is that OSET may undermine election security if foreign adversaries were also able to access the information. However, studies have debunked these assumptions in asserting that OSET may actually "the opposite effect and contribute to increased transparency and consequently greater trust in the election process and its results" [97]. The popular Internet browser, Mozilla Firefox is perhaps the most famous example of a secure OSET project built by thousands of contributors from all over the world [98].

Since 2016, there has been a bipartisan push for OSET or publicly owned voting software. The House Administration Committee Chair addressed that a lot of election-related risk, "comes from election technology vendors ... who have little financial incentive to prioritize election security and are not subject to regulations requiring them to use cyber security best practices" [99]. Congress should, therefore, specify new funding incentives for OSET development and maintenance in the next critical infrastructure bill. These investments can be distributed as direct funding, infrastructure procurement regulation, and tax incentives for OSET organizations. The bill should also consider appointing a federal agency like CISA with enforcement powers to further investigate voting system failures and respond with civil penalties.

Congress should also encourage the distribution and utilization of USPS resources for vote-by-mail advancements throughout the OSET community. In the last year alone, the USPS filed numerous patents with system plans for blockchain voting, cryptographic identification verification, and postal IoT networks, to name a few [100]. But with drastic budget cuts and a dwindling labor force, the USPS lacks the agency to expedite the implementation of these projects [101]. Collaboration with USPS through the OSET model can reduce the strain on postal workers, improve the vote-by-mail chain-of-custody, create efficient ballot tracking mechanisms, and account for troubleshooting obligations during peak election season.

As technology continues to swiftly evolve into the 21st century, a digitally secure democracy will demand more Americans get involved in the OSET development process. Below are a handful of ongoing projects making huge contributions to the OSET community which Congress can look to for further insight:

- **TrustTheVote Project** has been the OSET Institute's[21] flagship initiative since 2006 working with the EAC and NIST to create new open data standards and machine certification models [102].
- **ElectionGuard** is a software development kit (SDK) that was first released in 2019 through a Galois and Microsoft partnership called the Defending Democracy Program. The SDK is publicly available in the interest of empowering everyone to build OSET that meets E2E-V properties [103].
- **VotingWorks** is the only non-profit US voting system vendor that delivers accessible VVPAT-backed equipment, risk-limiting audits, real-time election reporting for the public, and remote BMDs for military voters. They pride themselves in releasing all their source code for public review "from the moment [they] write it" and working with "leading academics in the fields of voting security and usability" [104].
- **TurboVote** has been Democracy Works' flagship product since 2010. The online service simplifies the voter registration process by consolidating forms from across all 50 states [98].
- **BallotTRAX, BallotScout, Ballot TRACE** are all tracking notification services that have revolutionized the vote-by-mail accountability. They integrate tracking technologies with official USPS mail tags, logos, and intelligent mail barcodes (IMb) that meet election mailing standards [105].

5.3.c. Encourage recruitment of technical talent for public service and research opportunities. Real world implementation of election innovation is slow. Hence, the federal government plays a vital role in sponsoring evidence-based research and development of election systems. Meanwhile, state and local election administrators would greatly benefit from having a diverse and well-trained pool of cybersecurity professionals at their disposal.

Thus, this recommendation provides an excellent opening for new contributions to be made towards election-related research while also informing public policy decisions at the local level. In particular, federal agencies like the EAC, NIST, DHS, DoD, and NSF should sponsor projects across academia and industry to confront today's most pressing election security obstacles.

In 2020, the University of Chicago matched volunteer cybersecurity professionals to local election officials with the aim of protecting services that could be targeted by foreign adversaries identified by US intelligence officials — namely, Russia, China, Iran,

[21] The OSET Institute brands itself as a "Silicon Valley non-profit non-partisan research institute" building "next generation voting systems for about 0.004% of all money raised during the 2020 campaign cycle" [102].

North Korea, and Saudi Arabia [106]. Similar organizations like Coding It Forward, BlueBonnet Data, TechCongress, and Presidential Innovation Fellows, exist with the goal of building talent pipelines for the civic technology industry. The federal government can look to aforementioned fellowships for guidance of such a program.

Ultimately, this plan of action will connect volunteers or contractors (depending on the availability of funds) to local election officials in need of technical services. The program can also mobilize volunteers to address operational matters outside of peak election seasons like VRD maintenance. Maintaining a year-long fellowship will also ensure that election stakeholders thoroughly conduct penetration testing of systems beforehand and adapt infrastructure to combat cybersecurity threats accordingly.

One model might consider employing professional societies like IEEE or the Association for Computing Machinery (ACM) to spearhead the recruitment of young, diverse technical talent. IEEE has hundreds of chapters and university branches located in the US alone. An arrangement like this could be instrumental in the investment of next-generation election security talent. Consequently, this partnership would unite local members based on similar technical expertise to wrangle the most relevant problems in their communities. Potential partnerships should focus on cryptographic auditing methods, E2E-V checks, and ballot integrity proofs.

In the interest of reporting a comprehensive set of recommendations, here are some specific issues that have garnered significant attention and could be useful research topics for local precincts:

- Evaluate the reliability of alternative voter authentication methods (i.e. written signatures, digital signatures, biometric scanning, electronic ID cards, etc.)
- Enhance end-to-end vote-by-mail tracking systems through IoT[22] applications (i.e. interconnecting USPS' Internet of Postal Things, IMbs, etc.)
- Explore use cases for write-only digital public ledger technology (i.e. national VRD maintenance, final precinct tallying, etc.)
- Potential use of automated processes for unofficial results reporting in order to improve efficiency and accuracy
- Better understand social effects of coercion, suppression, and theft on disadvantaged voter groups (i.e. racial minorities, ex-felons, disabled populations, etc.)
- Test usability and comprehensibility of ballot designs
- Assess voter verification practices (i.e. VVPAT, risk-limiting audits, etc.)

[22] Internet of Things (IoT) are sensor technologies that enable physical objects to collect and communicate data through the Internet in real time [107].

- Investigate various cause and effects that may factor into voter turnout (i.e. extending early voting period, automatic voter registration, establishing Election Day as national holiday, expanding vote-by-mail, etc.)
- Influences of machine learning, artificial intelligence, and data mining practices on large-scale elections

6. Final Notes

The 2016 election proved that our democracy is only as strong as the faith people place in it. Recent events have led many to weigh the future of America through the current state of voting infrastructure. While contemporary advancements in i-voting and digital technologies are seemingly the next frontier of civic engagement, it is crucial to remember that not all probable system failures can be accurately anticipated. The mass adoption of technology will always give birth to its own set of unforeseeable risks. When the price of failure is far too great, as it certainly is in the case of voting, the nation must approach change with caution.

At its core, American election infrastructure is safeguarded not by the cutting-edge machinery, but by the policies and practices that are employed by state and local election officials. Rather than upending the entire nation's voting blueprint, public officials should heed evidence-based recommendations in order to improve the resiliency of present-day systems.

References

[1] World Economic Forum, "Mapped: The world's oldest democracies," 2019. Available: https://www.weforum.org/agenda/2019/08/countries-are-the-worlds-oldest-democracies

[2] Facing History & Ourselves, "We the People in the United States," in *Democracy & Civic Engagement*, 2020. Available: https://www.facinghistory.org/holocaust-and-human-behavior/chapter-2/we-people-united-states

[3] Y. Mounk, "Why The US is The Only Country in The World to Have Elections So Often," *Ideas: Home for Bold Arguments and Big Thinkers*, Nov. 05, 2014.

[4] A. National Association of State Election Directors, "Joint Statement from Elections Infrastructure Government Coordinating Council and Sector Coordinating Council Executive Committees." Nov. 12, 2020. Available: https://www.nased.org/news/jointstatement111220

[5] National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections." Jan. 07, 2020. Available: https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

[6] A. Boral, A. Edwards, S. Jones, and K. Kothari, "Beyond 2020: Policy Recommendations for the Future of Election Security," Harvard Kennedy School: Belfer Center for Science and International Affairs, Feb. 2021.

[7] OpenSecrets.org, "2020 election to cost $14 billion, blowing away spending records," Oct. 2020, Available: https://www.opensecrets.org/news/2020/10/cost-of-2020-election-14billion-update

[8] E. National Academies of Sciences and Medicine (U. S.). and R. Committee on the Future of Voting : Accessible Verifiable Technology, *Securing the Vote: Protecting American Democracy*. 2018. Accessed: Jul. 08, 2021. Available: https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1906148

[9] "ArtI.S4.C1.1.1.1.1 Role of the States in Regulating Federal Elections." US Constitution. Available: https://constitution.congress.gov/browse/essay/artI-S4-C1-1-1-1-1/ALDE_00001036/#:~:text=Article%20I%2C%20%20Section%204%2C%20Clause,the%20Places%20of%20chusing%20Senators

[10] US Election Assistance Commission, "Election Administration at State and Local Levels." National Conference on State Legislatures, Feb. 03, 2020. Available: https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx

[11] US Vote Foundation, "Online Voter Registration." National Conference on State Legislatures, Apr. 06, 2021. Available: https://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx#Table%20of%20states%20w/ovr

[12] D. Root, L. Kennedy, M. Sozan, and J. Parshall, "Election Security in All 50 States: Defending America's Elections," *Democracy and Government*, Feb. 12, 2018. https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states

[13] "H.R. 3295 Help America Vote Act of 2002." US Congress, Oct. 29, 2002. Available: https://www.govinfo.gov/content/pkg/PLAW-107publ252/pdf/PLAW-107publ252.pdf

[14] US Election Assistance Commission, "2016 Election Administration and Voting Survey (EAVS)," Jun. 2016. Available: https://www.eac.gov/assets/1/6/2016_EAVS_Comprehensive_Report

[15] M. P. McDonald, "Voter Turnout Data," *United States Election Project*. http://www.electproject.org/home/voter-turnout/faq/vap-v-vap

[16] US Census Bureau, "2020 Presidential Election Voting and Registration Tables Now Available." Apr. 29, 2021. Available: https://www.census.gov/newsroom/press-releases/2021/2020-presidential-election-voting-and-registration-tables-now-available.html

[17] MIT Election Lab, "Voter Turnout." Apr. 28, 2021. Available: https://electionlab.mit.edu/research/voter-turnout

[18] D. Desilver, "In past elections, U.S. trailed most developed countries in voter turnout," *Pew Research Center: Fact Tank*, Nov. 03, 2020. Available: https://www.pewresearch.org/fact-tank/2020/11/03/in-past-elections-u-s-trailed-most-developed-countries-in-voter-turnout/

[19] CISA, "National Risk Management: Election Security." 2021. Available: https://www.cisa.gov/election-security

[20] J. A. Halderman, I. F. Hao, and P. Y. A. Ryan, *Real-World Electronic Voting: Design, Analysis and Deployment*. CRC Press, 2016. Available: https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf

[21] J. A. Halderman and G. Cherry, "Election Lessons from Michigan," *Michigan Engineering Research News*, Apr. 12, 2021. https://news.engin.umich.edu/2021/04/election-lessons-from-michigan/

[22] R. M. Alvarez and T. E. Hall, *Point, Click, and Vote: The Future of Internet Voting*. Washington, D.C.: Brookings Institution Press, 2004. Available: https://www.jstor.org/stable/10.7864/j.ctt1gpccv1

[23] C. Lee, K. Chang, and F. S. Berry, "Testing the Development and Diffusion of E-Government and E-Democracy: A Global Perspective," *Public Administration Review*, vol. 71, no. 3, pp. 444–454, May 2011, doi: 10.1111/j.1540-6210.2011.02228.x.

[24] J. A. van Dijk and K. Hacker, "Digital Democracy: Vision and Reality," *Digital Democracy. Issues of Theory And Practice*, Jan. 2000, Available: https://www.utwente.nl/en/bms/vandijk/research/itv/itv_plaatje/Digital%20Democracy-%20Vision%20and%20Reality.pdf

[25] S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from Bad to Worse: From Internet Voting to Blockchain Voting," *Journal of Cybersecurity*, vol. 7, no. 1, p. tyaa025, Feb. 2021, doi: 10.1093/cybsec/tyaa025.

[26] Reuters Staff, "Fact check: '133 million registered voters' argument uses flawed logic." Reuters, Jan. 01, 2021. Available: https://www.reuters.com/article/uk-factcheck-voters-133-million/fact-check-133-million-registered-voters-argument-uses-flawed-logic-idUSKBN296284

[27] Special Counsel Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." Mar. 2019. Available: https://www.justice.gov/archives/sco/file/1373816/download

[28] M. Parks, "States Expand Internet Voting Experiments Amid Pandemic, Raising Security Fears," *National Public Radio*, Apr. 28, 2020. Available: https://www.npr.org/2020/04/28/844581667/states-expand-internet-voting-experiments-amid-pandemic-raising-security-fears

[29] L. Norden and F. Reyes, "Why Online Voting Isn't the Answer to Running Elections During Covid-19," *Brennan Center for Justice*, May 2020, Available: https://www.brennancenter.org/our-work/analysis-opinion/why-online-voting-isnt-answer-running-elections-during-covid-19

[30] K. C. Desouza and K. Kabtta Somvanshi, "How Blockchain Could Improve Election Transparency," *TechTank*, May 20, 2018. https://www.brookings.edu/blog/techtank/2018/05/30/how-blockchain-could-improve-election-transparency

[31] C. Fitzgerald, P. Smith, and S. Goodman, "The Secret Ballot At Risk: Recommendations for Protecting Democracy." Electronic Privacy Information Center, Verified Voting, and Common Cause, 2016. Available: http://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf

[32] CISA, "Election Infrastructure Security." Available: https://www.cisa.gov/election-security

[33] National Election Defense Coalition, "Vulnerable Voting Systems." Available: https://www.electiondefense.org/ballot-marking-devices

[34] National Conference on State Legislatures, "Types of Voting Equipment." Jul. 09, 2021. Available: https://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx

[35] D. Desilver, "On Election Day, Most Voters Use Electronic or Optical Scan Ballots." Pew Research Center, Nov. 08, 2016.

[36] T. Riley and J. Marks, "The Cybersecurity 202: More states now have paper trails to verify votes were correctly counted," *Washington Post*, Nov. 05, 2020. Available: https://www.washingtonpost.com/politics/2020/11/05/cybersecurity-202-more-states-now-have-paper-trails-verify-votes-were-correctly-counted

[37] Verified Voting Foundation, "Polling Place Equipment." 2022. Available: https://verifiedvoting.org/verifier/#mode/visualization/year/2022

[38] L. Norden and A. Beard, "There Is Shockingly Little Oversight of Private Companies That Create Voting Technologies," *Brennan Center for Justice*, Mar. 2020, Available: https://www.brennancenter.org/our-work/analysis-opinion/there-shockingly-little-oversight-private-companies-create-voting

[39] NIST, "To Help Protect Our Elections, NIST Offers Specific Cybersecurity Guidelines," Mar. 29, 2021. Available: https://www.nist.gov/news-events/news/2021/03/help-protect-our-elections-nist-offers-specific-cybersecurity-guidelines

[40] US Election Assistance Commission, "Testing & Certification Program Manual." US Election Assistance Commission, Feb. 2020.

[41] US Election Assistance Commission, "Major Updates of the Voluntary Voting System Guidelines 2.0." Feb. 10, 2021.

[42] R. L. Rivest, "Software Independence Revisited." MIT Computer Science and Artificial Intelligence Laboratory, 2016. Available: https://people.csail.mit.edu/rivest/pubs/RV16.pdf

[43] *Smiley v. Holm, 285 U.S. 355 (1932)*. Available: https://supreme.justia.com/cases/federal/us/285/355/

[44] "Congress and the Voting Rights Act of 1965." Available: https://www.archives.gov/legislative/features/voting-rights-1965

[45] Federal Election Commission, "Mission and History." Available: https://www.fec.gov/about/mission-and-history

[46] "The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986." Available: https://www.justice.gov/crt/uniformed-and-overseas-citizens-absentee-voting-act

[47] "National Voter Registration Act (NVRA) of 1993." 1993. Available: https://www.justice.gov/crt/about-national-voter-registration-act

[48] M. Morley and F. Tolson, "Elections Clause." Common Interpretation. Available: https://constitutioncenter.org/interactive-constitution/interpretation/article-i/clauses/750

[49] "Military and Overseas Voter Empowerment Act." Available: https://www.justice.gov/crt/uniformed-and-overseas-citizens-absentee-voting-act

[50] CNN All Politics, "How We Got Here: A Timeline of the Florida Recount," Dec. 13, 2020. Available: https://www.cnn.com/2000/ALLPOLITICS/stories/12/13/got.here/index.html

[51] C. Cox, "Georgia's Unique Model for Election Reform." Nov. 01, 2002. Available: www.sos.state.ga.us

[52] A. Rubin, D. Wallach, T. Kohno, and A. Stubblefield, "Analysis of an Electronic Voting System," Johns Hopkins University Information Security Institute, TR-2003-19, Jul. 2003.

[53] H. Thompson, "Expert Calls for Increased E-Voting Security," *Computer World Magazine*, Jan. 2006.

[54] J. Sarbanes, "HR1, the For the People Act." Available: https://sarbanes.house.gov/issues/hr-1-the-for-the-people-act

[55] Brennan Center for Justice, "Annotated Guide to the For the People Act of 2021," *Policy Solutions*, Mar. 2021, Available: https://www.brennancenter.org/our-work/policy-solutions/annotated-guide-people-act-2021

[56] *S.1 For the People Act of 2021*. 2021. Available: https://www.rules.senate.gov/hearings/s1-the-for-the-people-act

[57] D. Weiner and G. Fowler, "The For the People Act: Separating Fact from Fiction." Brennan Center for Justice, May 13, 2021. Available: https://www.brennancenter.org/our-work/research-reports/people-act-separating-fact-fiction

[58] "S.954 - Voter Empowerment Act of 2021." 117th Congress. Available: https://www.congress.gov/bill/117th-congress/senate-bill/954/titles

[59] FVAP, "Overseas Citizen Population Analysis Report," OCPA, 2018. Available: https://www.fvap.gov/info/reports-surveys/overseas-citizen-population-analysis

[60] Subcommittee on Investigations & Oversight and Subcommittee on Research & Technology, "Written Testimony of Josh Benaloh." House Committee on Science, Space, and Technology, Jun. 25, 2019. Available: https://science.house.gov/imo/media/doc/Benaloh%20Testimony.pdf

[61] S. Dzieduszycka-Suinat, J. R. Kiniry, and J. Benaloh, "The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study," US Vote Foundation, Galois, Jul. 2015. Available: https://usvotefoundation-drupal.s3.amazonaws.com/prod/E2EVIV_full_report.pdf

[62] I. Solaiman, "Defending Vote Casting: Using Blockchain-based Mobile Voting Applications in Government Elections," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, Oct. 2018, Available: https://www.belfercenter.org/publication/defending-vote-casting-using-blockchain-based-mobile-voting-applications-government

[63] M. Chalfant, "West Virginia Tests Secure Mobile Voting App for Military Personnel," *The Hill*, Mar. 2018. Available: https://thehill.com/policy/cybersecurity/380690-west-virginia-tests-secure-mobile-voting-app-for-military-personnel

[64] M. A. Specter, J. Koppel, and D. Weitzner, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections," *MIT Internet Policy*, Feb. 2020, Available: https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

[65] M. A. Specter and J. A. Halderman, "Security Analysis of the Democracy Live Online Voting System," Jun. 2020, Available: https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf

[66] R. Fanni, M. Emmer, and O. Velsberg, "e-Governance: the Estonian Case," *European Science-Media Hub*, Oct. 2019, Available: https://sciencemediahub.eu/2019/10/16/e-governance-the-estonian-case

[67] V. Valimiskomisjon, "Voting Methods in Estonia." 2015. Available: http://www.vvk.ee/voting-methods-inestonia/engindex/statistics

[68] K. Dhillon and A. Appel, "Challenges for Large -Scale Internet Voting Implementations," *Princeton University Department of Computer Science*, 2015, Available: https://www.semanticscholar.org/paper/Challenges-for-Large%C2Dscale-Internet-Voting-Dhillon-Appel/b2cc807bfcb4d72ae4439f46ed5ae57e

[69] M. Summers, "Online Voting Isn't as Flawed as You Think—Just Ask Estonia," *IEEE Spectrum*, Oct. 26, 2016. https://spectrum.ieee.org/telecom/internet/online-voting-isnt-as-flawed-as-you-thinkjust-ask-estonia

[70] M. Chevalier, K, and j, "Internet voting and individual verifiability: the Norwegian return codes," *International Conference on Electronic Voting*, 2012, Available: https://dl.gi.de/handle/20.500.12116/18224

[71] N. Abouzeid, "Ukraine Government Plans to Trial Ethereum Blockchain-Based Election Platform," *Nasdaq: Bitcoin Magazine*, Feb. 2016. Available: https://www.nasdaq.com/articles/ukraine-government-plans-to-trial-ethereum-blockchain-based-election-platform-2016-02-25.

[72] L. Jakobson, "Swiss e-voting system hack shows value of blockchain-based election technology," *Modern Consensus*, 2019. Available: https://modernconsensus.com/regulation/europe/zug-switzerland-e-voting-flaw

[73] T. K. Sharma, "Top Countries That Conducted Elections on the Blockchain," *Blockchain Council*, Oct. 15, 2019. Available: https://www.blockchain-council.org/blockchain/top-countries-that-conducted-elections-on-the-blockchain/

[74] Scytl Election Technologies, "French Ministry of Foreign Affairs Approves Scytl Online Voting for 2020 Consular Elections," Jan. 22, 2020. Available: https://www.scytl.com/en/french-national-cybersecurity-agency-certifies-scytl-online-voting-for-2020-consular-elections

[75] MapFight.xyz, "Estonia Size Comparison." Available: https://mapfight.xyz/map/ee

[76] Microsoft Security, "Zero Trust Security Model and Framework." Available: https://www.microsoft.com/en-us/security/business/zero-trust

[77] B. Buchanan and M. Sulmeyer, "Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity," *Harvard Kennedy School Belfer Center for Science and International Affairs*, no. The Cyber Security Project, Oct. 2016, Available: https://www.belfercenter.org/sites/default/files/files/publication/hacking-chads.pdf

[78] Federal Bureau of Investigation, Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, and Election Assistance Commission, "Risk Management for Electronic Ballot Delivery, Marking, and Return." National Institute of Standards in Technology. Available: https://www.politico.com/f/?id=00000172-9406-dd0c-ab73-fe6e10070001

[79] Cisco Security, "Malware and Botnets." Available: https://dataprot.net/statistics/malware-statistics

[80] International Foundation for Electoral Systems, "Internet Voting: Past, Present, and Future," Jul. 17, 2013. Available: https://www.ifes.org/news/internet-voting-past-present-and-future

[81] D. Jefferson, A. Rubin, and B. Simons, "Analyzing Internet Voting Security," *Communications of the ACM*, vol. 47, no. 10, Oct. 2004, Available: https://people.eecs.berkeley.edu/~daw/papers/cacm-serve.pdf

[82] "2007 Cyber Attacks on Estonia," NATO Strategic Concept, 2010. Available: https://stratcomcoe.org/pfiles/cyber_attacks_estonia.pdf

[83] J. A. Halderman, D. Springall, and J. Kitcat, "Security Analysis of the Estonian Internet Voting System," *Open Rights Group*, 2014, Available: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

[84] J. Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," *Centre for Technology & Global Affairs*, Nov. 2016, Available: https://www.ctga.ox.ac.uk/article/strategies-cyber-crisis-management-lessons-approaches-estonia-and-united-0

[85] J. Gilbert, "Gilbert Testifies Before U.S. House Committee about Election Security." Jan. 22, 2020. Available: https://www.cise.ufl.edu/gilbert-testifies-before-u-s-house-committee-about-election-security/

[86] N. Corasaniti, "Stacey Abrams and her group will try to rally young voters of color behind the For the People Act," *New York Times*, Jun. 08, 2021. Available: https://www.nytimes.com/2021/06/08/us/stacey-abrams-hot-call-summer.html

[87] CISA, "Cybersecurity Governance in the State of Michigan." Dec. 2017. Available: https://www.cisa.gov/sites/default/files/publications/Michigan_Cyber_Governance_Case_Study_508.pdf

[88] L. Norden and G. Ramachandran, "A Framework for Election Vendor Oversight," Brennan Center for Justice, Nov. 2019. Available: https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight

[89] "See Something Say Something 2020." Available: https://seesay2020.com

[90] L. Norden, "Voting System Failures: A Database Solution," Brennan Center for Justice, Sep. 2010. Available: https://www.brennancenter.org/our-work/research-reports/voting-system-failures-database-solution

[91] M. Scherer and N. Tiku, "Mark Zuckerberg and Priscilla Chan donate $100 million more to election administrators, despite conservative pushback," *Washington Post*, Oct. 13, 2020. Available: https://www.washingtonpost.com/politics/zuckerberg-chan-elections-facebook/2020/10/12/0e07de94-0cba-11eb-8074-0e943a91bf08_story.html

[92] US Election Assistance Commission], "Agency Financial Report." US Election Assistance Commission, 2019. Available: https://www.eac.gov/sites/default/files/eac_assets/1/6/EAC_FY2019_Agency_Financial_Report.pdf

[93] Alabama Secretary of State, "Alabama Secretary of State and 16 Other Secretaries Support Robust Funding of the Election Assistance Commission." Available: https://www.sos.alabama.gov/newsroom/alabama-secretary-state-and-16-other-secretaries-support-robust-funding-election

[94] Penn Wharton Public Policy Initiative, "The Business of Voting: Market Structure and Innovation in the Election Technology Industry," University of Pennsylvania, Election Technology Industry Report, 2016.

[95] Colorado Election Assistance Commission, "Uniform Voting System." Dominion Voting Systems, Dec. 04, 2013. Available: https://www.sos.state.co.us/pubs/elections/VotingSystems/RFI/proposals/DominionVotingSystemsColoradoUVSProposal.pdf

[96] Open Source Forum, "Open Source Way 2.0." Available: https://opensource.com/open-source-way

[97] M. Clouser, P. Wolf, N. Handal Zander, and International Institute for Democracy and Electoral Assistance, *The use of open source technology in elections*. Stockholm: International IDEA, 2014.

[98] M. Linksvayer, "Vote, and contribute to democracy through open source," Oct. 22, 2020. https://github.blog/2020-10-22-vote-and-contribute-to-democracy-through-open-source

[99] Representative Zoe Lofgren (D–CA))Zoe Lofgren, chairperson, *Hearing on Election Security*. 2019.

[100] "Patents Assigned to United States Postal Service." Justia Patens. Available: https://patents.justia.com/assignee/united-states-postal-service

[101] M. Morrissey, "The war against the Postal Service." Economic Policy Institute, Dec. 16, 2020. Available: https://www.epi.org/publication/the-war-against-the-postal-service

[102] OSET, "TrustTheVote; Learn More." Available: https://trustthevote.org/learnmore

[103] T. Burt, "Protecting democratic elections through secure, verifiable voting." Microsoft Security, May 06, 2019. Available: https://blogs.microsoft.com/on-the-issues/2019/05/06/protecting-democratic-elections-through-secure-verifiable-voting

[104] VotingWorks, "VotingWorks Documentation." Available: https://docs.voting.works/vxsuite

[105] J. Blessing, J. Gomez, M. Patiño, and T. Nguyen, "Security Survey and Analysis of Vote-by-Mail Systems," *arXiv:2005.08427 [cs]*, Sep. 2020, Accessed: Jul. 08, 2021. Available: http://arxiv.org/abs/2005.08427

[106] C. Kempf, "Election Cyber Surge," *University of Chicago Harris School of Public Policy*, Oct. 13, 2020. Available: https://harris.uchicago.edu/news-events/news/keep-it-secret-keep-it-safe-election-cyber-surge-and-secure-2020-vote

[107] Office of the Inspector General, "The Internet of Postal Things," United States Postal Service, RARC-WP-15-013. Available: https://www.uspsoig.gov/sites/default/files/document-library-files/2015/rarc-wp-15-013_0.pdf