5-2019

American Digital Election Infrastructure: Policy, Risks, Options

Tyson S. Himes
The Graduate Center, City University of New York

American Digital Election Infrastructure: Policy, Risks, Options

By Tyson Himes

A master's thesis submitted to the Graduate Faculty in Political Science in partial fulfillment of the requirements for the degree of Master of Arts, The City University of New York.

2019

American Digital Election Infrastructure: Policy, Risks, Options

By

Tyson Himes

This manuscript has been read and accepted for the Graduate Faculty in Political Science in satisfaction of the thesis requirement for the degree of Master of Arts.

_____	_____Alan DiGaetano_____
Date	Thesis Advisor
_____	_____Alyson Cole_____
Date	Executive Officer

THE CITY UNIVERSITY OF NEW YORK

Abstract

"American Digital Election Infrastructure: Policy, Risks, Options"

By

Tyson Himes

Faculty Advisor: Alan DiGaetano

Why is US digital election infrastructure (DEI) in a vulnerable state and what are the possible options to better secure it? To answer these questions systematically, federal policy and current DEI are analyzed through a risk management lens, including both elite and democratic models of risk management. This analysis suggests that DEI is at risk because federal policy currently enables states to use Direct-Recording Electronic (DRE) voting machines without a paper trail and allows states to manage their own risk environment with respect to digital voter registration databases (VRDs). This in turn produces significant variance in outcomes in levels of cyber security and priority of VRD governance. These factors combine to present serious vulnerabilities that could be exploited in a targeted attack during a Presidential election to disastrous consequence. As a result, policy options and potential technical improvements to DEI should be explored.

Acknowledgements

Firstly, I would like to thank my faculty advisor, Dr. Alan DiGaetano, for his most valuable feedback and help throughout this process. His suggestions have substantially improved the quality of this work. I would also like to thank all of the staff and faculty at the Graduate Center for providing an open and collegial environment in which to grow. Attending this institution has been a priceless experience. Lastly, I would like to thank my partner, Charlotte Jeffries, for her diligent copy editing and feedback for the past two years. I would not have been able to do any of this without her.

TABLE OF CONTENTS

List of Tables

Abbreviations

CI - Critical Infrastructure

COTS - Commercial Off-The-Shelf

DDoS - Distributed Denial-of-Service Attack

DEI - Digital Election Infrastructure

DHS - The Department of Homeland Security

DRE - Direct-Recording Electronic Voting Machines

HAVA - The Help America Vote Act of 2002

NVRA - The National Voter Reform Act of 1993

VRA - The Voting Rights Act of 1965

VRD - Digital Voter Registration Database

Introduction

America's elections are under attack. In the age of the internet, those who wish to subvert elections can do so from the comfort of their home countries, out of the reach of US law enforcement. When data necessary for the smooth functioning of electoral democracy is transmitted and stored digitally, hackers only need the slightest crack in cyber security to affect the outcomes of elections. This raises concern about the integrity of US elections and national security.

New policy is necessary to properly regulate elections in ways consistent with the ideals of representative democracy. Article 1, Section 4 of the US Constitution empowers the states to regulate most aspects of the election environment. Additionally, the Tenth Amendment reserves powers for the states that are not expressly given to the federal government, nor prohibited by the Constitution. Since there are few explicit powers given to the federal government to regulate elections in the Constitution, the states have lawfully created election policies and the courts have upheld such policies as properly being under the purview of the states. Partly as a result of this decentralization, there has been a need over the years to enact federal policy to correct for practices that limit suffrage rights (The Voting Rights Act (VRA) of 1965, The National Voter Registration Act (NVRA) of 1993, the Help America Vote Act (HAVA) of 2002, etc.).

Currently there is a need for similar federal action to secure digital voter registration databases (VRDs) and Direct-Recording Electronic (DRE) voting machines in the age of the internet. These actions can be justified as an effort to protect to universal suffrage, as all registered US voters should be confident that their registration will be honored and that their vote will be counted. Given the critical role of elections in sustaining democratic governance, secure

functioning of the electoral environment is essential. VRDs and DREs are integral components in maintaining that environment.[1]

Especially in light of the ongoing investigations into Russian meddling in the 2016 election, protecting the integrity of the vote from foreign as well as domestic threats is now something the federal government recognizes as an urgent concern. In 2017, the Department of Homeland Security (DHS) designated election infrastructure as critical infrastructure (CI). Included in the designation of election infrastructure as CI is digital election infrastructure (DEI), which is defined here as any complex digital system used in the administration of elections:

> CI is a DHS designation established by the Patriot Act and given to 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters'[2]

The nature of the threat is important to understand. In 2016, sensitive information (names, birthdays, addresses, and the last four digits of social security numbers and driver's licenses) from nearly 200,000 records were stolen in Illinois, while malware was used to breach digital voting records in Arizona.[3] All told, foreign assailants scanned VRD systems in 39 states for vulnerabilities.[4]

---

[1] I consider VRDs and DREs part of America's digital election infrastructure which I will refer to as "DEI" throughout this thesis. I do not, however, consider remote digital voting in this thesis, as it is not a widely used method of voting in the US.

[2] "DHS Cybersecurity Services Catalog for Election Infrastructure." Accessed March 21, 2019. https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf.

[3] Norris, Pippa. *Why American Elections Are Flawed (and How to Fix Them)*. Vol. 1. Cornell University Press, 2017. Pp. 15.

[4] "Russian Hacks on U.S. Voting System Wider Than Previously Known." Accessed March 28, 2019. https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

In response to the above activity, studies examining American DEI have found systemic weaknesses. One study published by The Center for American Progress called "Election Security in All 50 States" was particularly damning. They assigned grades to the states based on basic security standards. No state received an A, while eleven received D's, and two received F's.[5] Further evidence of the state of DEI is proffered in the book *Why American Elections Are Flawed (And How to Fix Them)* by elections expert Pippa Norris:

> The aging equipment and vintage software used on many US electronic voting machines, and the lack of sophisticated security to protect state voting records, make these particularly vulnerable to external cyberattack by foreign powers and terrorist groups…it would just take minor security breaches to some digital voting registers, electronic voting machines, or software aggregating vote tabulations, in a few local polling places in a couple of swing states, to reduce the credibility of American elections, throw the outcome into chaos, and trigger doubts about the legitimacy of the eventual winner of the presidential contest[6]

This prompts the following research questions: Why is US DEI in a vulnerable state and what are the possible options to improve security? I answer these questions below by systematically analyzing federal policy and current DEI through a risk management lens. DEI is at risk because federal policy currently enables states to use Direct-Recording Electronic (DRE) voting machines without a paper trail. It also enables states to manage their own risk environment with respect to VRDs, which produces significant variance in levels of cyber security and the priority of VRD governance. These factors combine to present serious vulnerabilities that could be exploited (in a targeted attack on swing states) during a Presidential election.

This thesis develops a risk management analytical framework for assessing DEI security and then explains the methodology used in this assessment. Next, current federal election policy

---

[5] Root, Danielle, Liz Kennedy, Michael Sozan, and Jerry Parshall. "Election Security in All 50 States." Center for American Progress. Accessed April 4, 2019. https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/electio -security-50-states/. Pp. 31.

[6] Norris, *Why American Elections Are Flawed (and How to Fix Them)*, 15-16.

is analyzed through a risk management lens in order to understand better whether current policy is strong enough to guard against potential threats to the US election system. The vulnerabilities in current digital election systems, specifically VRDs and DREs, are also examined. Lastly, potential policy options as well as technical improvements are considered.

Frames of Analysis

The United States of America is the oldest democracy in the world. It is also the richest country in the world in terms of national net wealth.[7] So why does the US administer elections so poorly when compared to other democracies?

The Electoral Integrity Project (EIP) developed a Perceptions of Electoral Integrity (PEI) survey to compare how democracies perform among a wide array of electoral processes.[8] The results show that the US substantially underperforms most Western democracies and ranks 52nd globally (based on data gathered during elections in 2012 and 2014).[9] When compared to other Anglo-American democracies that share many common features like the UK, Australia, and Canada, the US scores nearly 20 points lower for voter registration integrity, which is one of the aspects of DEI that will be addressed in this thesis.[10]A large part of why Norris and the EIP have concluded that the US performs well-below other Anglo-American democracies in voter registration administration results from the lack of adequate DEI security.

[7] "Global Wealth Report 2018." Credit Suisse. Accessed April 11, 2019. https://www.credit-suisse.com/corporate/en/articles/news-and-expertise/global-wealth-report-2018-us-and-china-in-the-lead-201810.html.
[8] Norris, *Why American Elections Are Flawed (and How to Fix Them)*, 25.
[9] Ibid., 28.
[10] Ibid., 36.

Risk Management

Given the status of the US as a global political and financial power, why has it not been able to secure its elections adequately? To answer this and other questions (mentioned above), DEI is analyzed from a risk management frame of reference in order to compose an informed argument. Risk management of DEI includes decisions that affect cyber security of VRDs, and the use of DREs.

The definition of risk employed here derives from *Accident and Design: contemporary debates in risk management* by Christopher Hood and David K.C. Jones. For them, "'Risk'...connotes the assessment of *consequence* or 'exposure to the chance of loss".[11] Consequence in the context of elections is a high stakes game. As noted in the introduction, manipulation of VRDs or DREs in a few swing states could alter the results of a presidential election. This is an extremely sensitive issue from the perspective of ordinary Americans. Just one individual's vote not being counted adversely affects attitudes on election integrity.[12] If votes are successfully manipulated, the legitimacy of the US electoral systems could be undermined as popular confidence is vital to sustaining democratic processes. Altered vote tallies could affect outcomes on two levels: results and attitudes. This is the risk environment in which election security policy operates.

Having defined risk and the risk environment, two aspects of election security can be investigated: risk analysis and risk management. Risk analysis, also referred to as risk

[11] Hood, Christopher, and David K. C. Jones, Eds. *Accident and Design: contemporary debates in risk management*. London ; Bristol, Pa: UCL Press, 1996. Pp. 2-3.
[12] "Concerns about Voter Access and Eligibility | Pew Research Center," October 29, 2018. https://www.people-press.org/2018/10/29/concerns-about-eligible-voters-being-prevented-from-voting-and-ineligible-voters-voting/.

assessment, is the process of quantifying the probability of an adverse event as well as potential consequences using mathematical or engineering techniques.[13] Daniel J. Fiorino, in his article, "Technical and Democratic Values in Risk Analysis," claims that risk assessment is aligned with an elite theory of government, which privileges technical expertise over lay opinion. Fiorino claims that:

> The technical model of risk analysis reflects several characteristics of elite theory. Its emphasis on results (fatalities avoided, net benefits maximized) exhibits a one-dimensional approach, because it equates interest with the substance of policy outcomes and ignores process. It is assumed that the general public interest is achieved when governmental policy is in accord with the judgment of elites[14]

Risk management, on the other hand, is inherently political, and encompasses more than just assessment because it entails an approach to governance.[15] Deciding how to manage risk requires making choices that have political effects.

Hood and Jones explain how risk management is "a process involving the three basic elements of any control system…namely: goal-setting (whether explicit or implicit), information gathering and interpretation," and "action to influence human behavior, modify physical structures or both".[16] With risk management of DEI, "goal-setting" includes an approach to VRD governance at the institutional level. This includes making decisions on whether to require certification, regulation, and/or authorization by statute.[17] The "information gathering and interpretation" process allows states to assess the nature of the threat and to locate available

---

[13] Smith, Denis, and Alan Irwin. "Public Attitudes to Technological Risk: The Contribution of Survey Data to Public Policy-Making." Transactions of the Institute of British Geographers 9, no. 4 (1984): 419. https://doi.org/10.2307/621778. Pp. 419.
[14] Fiorino, Daniel J. "Technical and Democratic Values in Risk Analysis." Risk Analysis 9, no. 3 (September 1989): 293–99. https://doi.org/10.1111/j.1539-6924.1989.tb00994.x. Pp. 297.
[15] Fiorino, "Technical and Democratic Values in Risk Analysis," 297.
[16] Hood and Jones, *Accident and Design: Contemporary Debates in Risk Management,* 6.
[17] "Electronic Poll Books | E-Poll Books." Accessed April 11, 2019. http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

resources. This process includes analyzing the risk environment and tailoring it to the needs of the specific state and taking advantage of cyber security resources. The last level ("action to influence human behavior, modify physical structures or both") includes auditing systems after attacks, developing additional security measures, and properly training election officials in cyber security methods. These three elements (goal-setting, information gathering and interpretation, and action to influence human behavior, modify physical structures or both) act as a lens through which to assess how states manage risk in their DEI. State level risk is difficult to assess when viewed on the national level, as US elections are highly decentralized and risk is mostly localized under our federal system.

Rather than relying solely on a technical model of risk management (which is aligned with elite theory), the argument developed here also adopts a democratic model of risk assessment, as proposed by Fiorino:[18]

> The democratic model evaluates risk based on its social and political consequences, such as possible disruption in the social fabric or a loss of communality. Lay criteria for assessing the impact of risk decisions…are embedded in cultural values. Similarly, lay evaluations of risk incorporate substantive and procedural democratic values, such as the acceptability of processes for making decisions, the ethics of the distribution of risk, and the capacity to control a source of risk in the community's interests. Finally, the democratic model relates judgments about risks to the competence (Can we trust them?) and the legitimacy (Should we trust them?) of the social institutions that impose and control those risks[19]

This approach means a commitment to democratic processes and "a two-dimensional perspective that assesses policy processes and institutions not only by their end results, but by their compatibility with substantive and procedural democratic values".[20] To align with this approach, current policy and the resulting technical vulnerabilities are assessed, not only from a technical

[18] This will primarily be applied in the Policy Options section.
[19] Fiorino, "Technical and Democratic Values in Risk Analysis," 296.
[20] Ibid., 297.

point of view, but also from the perspective of democratic values, in accordance with the Constitution and the belief held broadly by the public. To bolster this democratic model approach, Pew Research Center survey data on public perception of digital election systems is used. Public confidence in the institutions responsible for safeguarding election infrastructure is thus necessarily a component in the democratic risk management model outlined above.

Hierarchy of Needs

An assessment of risk in the election environment would benefit greatly from the use of the concept of a hierarchy of needs. Table 1 reports the hierarchy of needs as applied to assessing policy and digital systems. Though voter suppression is a real threat, and voter ID laws can turn away potential voters, access is meaningless if voter registration is not honored and votes are not accurately reflected in final tallies. Equally, for accuracy of the vote, without proper security, the results can be manipulated. Most federal election policy to date (e.g. VRA, NVRA, HAVA, etc.) has been to promote access to the vote. The below research indicates that focus should now be shifted to security.

Table 1: Election Environment Hierarchy of Needs

Convenience
Efficiency (monetary efficiency and efficiency of operations)
Access / Accuracy
Security

Scale: Bottom = Most Important; Top = Least Important

Policy Research Methodology

Lastly, the analysis of election security is partly framed by the unique methodology of policy research. Moran et al. detail this methodology in *The Oxford Handbook of Public Policy*. They claim that:

> Policy research requires a profoundly different methodology from that on which basic research relies, because policy research is always dedicated to changing the world while basic research seeks to understand it as it is… Even those policies whose purpose is to maintain the status quo are promoting change—they aim to slow down or even reverse processes of deterioration[21]

The purpose of this thesis is to analyze current policy to determine why digital election systems are at risk and to explore whether a change in policy is warranted. If a change in policy is necessary, the challenge is to "determine the relative resistance to change according to the different variables that are to be tackled" systematically.[22] These methods are outside the scope of this thesis as policy researchers must "include at least all the variables that account for a significant degree of variance in the phenomenon that the policy aims to change".[23] This is a task for future, funded research, which is addressed at the end of this thesis.

Analysis of Current Voting Policy

The American policy regime that governs DEI is still in its infancy. For that reason, only modern voting policy will be analyzed, as policy crafted before the advent of the internet did not foresee the regulatory frameworks that would need to be created to account for the radical shift

[21] Moran, Michael, Martin Rein, and Robert E. Goodin, Eds. The Oxford Handbook of Public Policy. The Oxford Handbooks of Political Science. Oxford ; New York: Oxford University Press, 2006. Pp. 833.
[22] Ibid., 836.
[23] Ibid., 838-839.

in technology. The constitutional basis for elections needs to be examined first in order to provide context.

Constitutional Context

Elections are mostly managed by the states, stemming from Article 1, Section 4 of the US Constitution which states, "The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the place of Chusing Senators".[24] Also, the Tenth Amendment, which reserves power to the states that are not explicitly given to the federal government in the Constitution, heavily influenced the evolution of election policy in the United States. Since the Constitution provides few powers to the federal government for regulating elections, states are largely free to govern their own elections. This has ultimately resulted in discriminatory practices in election administration. In order to bolster suffrage in the face of these practices, several Constitutional Amendments (15th, 19th, and 26th) were ratified.

The Voting Rights Act (VRA) of 1965

The federal government has also stepped in to secure the right to the vote more firmly through national legislation. The Voting Rights Act (VRA) of 1965 was one of the earliest such modern policies of consequence. The VRA sought to protect the suffrage rights of African-Americans who were subjected to discriminatory practices like the Grandfather Clause, poll taxes, and literacy tests.

[24] US Const. art. I, sec. 4.

Digital security was not yet an issue when the VRA was passed as the technology to produce digital infrastructure was not yet available. The VRA largely left it up to the states (except for the states subject to federal preclearance) to maintain properly paper voter rolls and the administration of voting technology, which at the time included "hand-counted paper, mechanical lever machines, punch-card machines" and "scanned paper ballots".[25] In summation, the VRA did not anticipate a digital environment with complex systems that are vulnerable to compromise by malicious actors in a digital environment.

The National Voter Registration Act (NVRA) of 1993

In contrast to the VRA, the National Voter Registration Act (NVRA) of 1993 was passed after the advent of the internet, but digital technology was still not ubiquitous. The NVRA was tied to suffrage rights and mandated that citizens be offered the ability to register to vote in federal elections in all 50 states when getting a license at the department of motor vehicles (according to Section 5 of the NVRA) hence the nickname, the "motor voter law".[26] Additional sections of the NVRA of import include Section 6, which "requires that States offer voter registration opportunities by mail-in application," Section 7, which "requires that States offer voter registration opportunities at certain State and local offices," and Section 8, which "contains requirements with respect to the administration of voter registration by States and requires States to implement procedures to maintain accurate and current voter registration lists".[27]

[25] "Voting Technology | MIT Election Lab." Accessed April 11, 2019. https://electionlab.mit.edu/research/voting-technology.
[26] "The National Voter Registration Act Of 1993 (NVRA)," August 6, 2015. https://www.justice.gov/crt/national-voter-registration-act-1993-nvra.
[27] Ibid.

Furthermore, once signed into law, the NVRA effectively regulated both federal and state elections due to the need for efficiency:

> Although enacted pursuant to Congress's power to regulate congressional elections under Article I, Section 4 of the Constitution, the NVRA effectively changed the registration processes for all elections, given the impracticability and inefficiency of maintaining separate voting lists for federal and state elections[28]

One key component of the NVRA, Section 8, was the mandate to protect the integrity of the voter rolls.[29] Given that digital systems were still not commonplace, there were no instructions to the states regarding digital voter rolls, though states must apply the standard of maintaining up-to-date and accurate voter rolls to the digital context in order to comply with the NVRA.

The Help America Vote Act (HAVA) of 2002

The policy trailblazer for DEI was the Help America Vote Act (HAVA) of 2002, which was passed in the wake of the controversial 2000 Presidential election. The relevant portion of HAVA, as it pertains to VRD security is Section 303, which provides a framework for implementing a centralized, digital system at the state level. It requires that "Each State, acting through the chief State election official, shall implement, in a uniform and nondiscriminatory manner, a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level".[30]

After HAVA, the states set about creating the mandated computerized registration lists, which I refer to as VRDs (though they are sometimes referred to as e-poll books). The states

[28] Tokaji, Daniel. "Voter Registration and Election Reform." The William and Mary Bill of Rights Journal 17, no. 2 (2008): 453-506. Pp. 467-468.
[29] Ibid., 467.
[30] U.S. Congress. House. The Help America Vote Act of 2002. HR 3295. 107th Cong., 2nd sess. Introduced in House November 14, 2001. https://www.congress.gov/bill/107th congress/house-bill/3295/text.

created three different VRD systems (according to which level data is stored) in total: top-down, bottom-up, and hybrid.[31]

> Some states adopted a single, central platform at the state level that connected to terminals in local jurisdictions. This type of system is typically referred to as a "top-down" voter registration system. Other states have a state voter registration database that gathers and aggregates information from their local jurisdictions' voter registration databases. This type of system is typically referred to as a "bottom-up" system. Other states have what is termed a hybrid system, a system with a mix of top-down and bottom-up characteristics[32]

In addition to the variance in list construction there is significant variance in how the states have chosen to create legal frameworks for such lists (whether top-down, bottom-up, or hybrid). According to the National Conference of State Legislatures (NCSL):

> In some states, the use of e-poll books is specifically authorized in statute. In other states, e-poll books are mentioned in statute but their use is not specifically authorized. Some state statutes don't mention e-poll books at all, but state-level elections organizations issue regulations for their use. Finally, some states have some jurisdictions that use e-poll books but have no statewide guidance on their use. There are jurisdictions in 32 states that currently use e-poll books, and Alabama will soon become the 33rd, with the enactment of a pilot program for the use of e-poll books in the state[33]

Furthermore, VRDs are not certified in a uniform manner by the states.[34] Eight states require certification of VRDs by the Secretary of State in order for them to be used.[35]

Thus far, three levels of variance have been identified: variance in system (top-down, bottom-up, hybrid), variance in legal framework (some lists mentioned in statues, some are not), and variance in certification (eight states requiring certification). As it pertains to specific technical standards for cyber security, HAVA provides minimal requirements. In Section 303, it is stated that, the "appropriate State or local official shall provide adequate technological security

[31] "Statewide Voter Registration Systems | US Election Assistance Commission." Accessed April 5, 2019. https://www.eac.gov/statewide-voter-registration-systems/.
[32] Ibid.
[33] "Electronic Poll Books | E-Poll Books".
[34] Ibid.
[35] Ibid.

measures to prevent the unauthorized access to the computerized list established under this section".[36] This language avoids mandating specific systems that might provide enhanced cyber security or specific security measures that states must take in order to secure their systems. Compliance with the guidelines was entirely voluntary. Section 221 created a Technical Guidelines Development Committee aimed at developing voluntary guidelines once members were appointed and a nine month period had elapsed.[37] One component of the committee's work was to support the states in obtaining "the security of computers, computer networks, and computer data storage used in voting systems, including the computerized list required under section 303(a)".[38] This language gives broad latitude to the states in developing their own systems and according to what they judge to be best practices. HAVA, in short, permits states to make different judgments about best practices.

This adds another level of significant variance, that of technical cyber security standards. The states vary in their usage of the following common cyber security practices, such as: access controls, passwords, multi-factor authentication (MFA), logging and monitoring activity, training, regular back-ups, provisional ballots, and communicating with other states.[39]

When this variance is viewed through the lens of risk management (goal-setting, information gathering and interpretation, and action to influence human behavior) outcomes differ enormously. Goal-setting differs among states, as evidenced by variance in systems, legal frameworks, certifications, and technical standards for VRDs. Some states are more proactive and provide a more robust institutional basis for their VRDs, while some do not even mention

[36] U.S. Congress. House. The Help America Vote Act of 2002.
[37] Ibid.
[38] Ibid.
[39] "Election Security | Cybersecurity: What Legislators (and Others) Need to Know." Accessed April 5, 2019. http://www.ncsl.org/research/elections-and-campaigns/election security.aspx.

VRDs by statute.[40] This implies that some states have different goals for their VRDs. In states where robust, legal frameworks are created, VRDs are clearly being prioritized, while in states where VRDs are barely even mentioned, they are clearly less of a priority.

On the risk management level of information gathering and interpretation, most states do not have the appropriate resources to gather and interpret information on cyber security.[41] States do, however, have access to outside resources that can assist them in this task, like the Department of Homeland Security (DHS) and the Center for Internet Security (CIS), but these partnerships are entirely voluntary. For instance, DHS provides state partners with the tools to gather information and interpret threats through a comprehensive, cost-effective cyber security program.[42]

Lastly, the states vary in their actions to influence human behavior. States respond differently to the risk environment and to breaches in security. Some, like Illinois, underwent a complete review of cyber security after their VRD was compromised in 2016. They enhanced their cyber security in the aftermath of the 2016 election with monthly audits, daily back-ups, and by monitoring unsuccessful attempts to log into their system.[43] Meanwhile, Arizona, which was also attacked in 2016, received a below-average grade for election security in a February 2018 report by the Center for American Progress.[44] Other states have still not instituted simple measures like effectively training election officials in cyber security measures.[45] And if states do

[40] Root et al., "Election Security in All 50 States".
[41] Ibid.
[42] "Election Security." Department of Homeland Security, March 27, 2018. https://www.dhs.gov/topic/election-security.
[43] Becker, David, Jacob Kipp, Jack R. Williams, and Jenny Lovell. "Voter Registration Database Security." The Center for Election Innovation Research. September 2018. Pp. 15.
[44] Root et al., "Election Security in All 50 States".
[45] Ibid.

provide training to election officials, there is additional variance in the quality of training use these systems.[46]

These variations apply only to VRD cyber security and governance as analyzed through HAVA standards. DREs do not qualify as a control system, where the three levels of risk management (goal-setting, information gathering and interpretation, and action to influence human behavior, modify physical structures, or both) are leveraged to properly mitigate risk. Using DREs without a paper trial is a binary choice - either states use them or they do not. There are other voting technologies that could effectively replace DREs, but the states do not have a choice whether or not to deploy VRDs as they are mandated by HAVA.

HAVA brought Direct-Recording Electronic (DRE) machines into the election environment with their mandate to modernize voting technology and the funding that accompanied it (see Sec. 251, Sec 271, and Sec. 281 of HR 3295). After receiving this funding many states procured DREs that did not produce a paper trail and still use those original machines to this day. According to the Brennan Center, twelve states are currently using DREs without a paper trail "in at least some counties and towns" (Delaware, Georgia, Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Pennsylvania, South Carolina, Tennessee and Texas).[47] What is more, "Delaware, Georgia, Louisiana, and South Carolina continue to use such systems statewide".[48] Clearly, these twelve states are not properly managing their risk environment by relying on this voting technology. Evidence on DRE vulnerabilities will be provided in the next section.

---

[46] Ibid.

[47] "Voting Machines at Risk: Where We Stand Today | Brennan Center for Justice." Accessed March 16, 2019. http://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

[48] "Voting Machines at Risk: Where We Stand Today | Brennan Center for Justice," Ibid. Parentheses removed from original.

In summation, the hands-off approach of federal policy produces four levels of significant variance: system (top-down, bottom-up, hybrid), legal framework (some lists mentioned in statues, some are not), certification (eight states require certification), and cyber security standards. Dealing with the threat of cyber-attacks through federal policy would be difficult as American elections have been thoroughly decentralized historically. Given the modern threats of hacking, HAVA standards may not be sufficiently rigorous to protect presidential elections because they allow states to manage their own risk environments. This leads to significant variance in cyber security outcomes and provides vulnerabilities that can be targeted to great effect.

According to the hierarchy of needs in the election environment outlined in the frames of analysis section, security is now a more basic need than access. Most federal election policies to date have been passed to increase access to the vote (e.g. VRA, NVRA, HAVA, etc.). In the age of the internet, the focus should be shifted to security, as access can be affected through hacking, VRDs can be manipulated to remove voters from the rolls, and DREs can be attacked to alter votes cast. Given that we have robust policy in place ensuring access security has become a more basic need to properly ensure suffrage rights. The specific, technical vulnerabilities that reinforce the need for security in DEI are detailed below.

Current Digital Election Infrastructure Vulnerabilities

Direct-Recording Electronic (DRE) Voting Machines

This section addresses the question of technical complexity that stems from US election policy and focuses on the specific technical vulnerabilities with extant VRDs and DREs. Initially, states were given incentives to upgrade their voting technology through the Help America Vote Act of 2002. States could apply for grants to purchase DREs and other much-needed equipment from accredited vendors. But paper trails were not mandated by HAVA, this leading a number of states to invest heavily in DREs that did not produce a paper trail record of votes cast. These paperless DREs rely entirely on machine generated internal records. The lack of a paper trail makes DREs uniquely susceptible to manipulation when compared to the voting technologies that the DREs replaced, like hand-counted paper ballots, mechanical lever machines, punch cards, and scanned paper ballots.

According to some security experts, among voting technologies now in use, DREs are the most at risk of large-scale manipulation:

> Analysis of the machine, in light of real election procedures, shows that it is vulnerable to extremely serious attacks. For example, an attacker who gets physical access to a machine or its removable memory card for as little as one minute could install malicious code; malicious code on a machine could steal votes undetectably, modifying all records, logs, and counters to be consistent with the fraudulent vote count it creates. An attacker could also create malicious code that spreads automatically and silently from machine to machine during normal election activities - a voting-machine virus[49]

Once these security vulnerabilities are reported, commercial vendors who manufacture DREs often state that patches can be made to furnish greater security for the voting machines. But these machines use proprietary code and only election officials (sometimes with the help of outside agencies like DHS) can review the code for errors or malicious strings. Commercial vendors, as a rule, do not use open-source code. They have a commercial interest in their code remaining

[49] Feldman, Ariel J., J. Alex Halderman, Edward W. Felten. "Security Analysis of the Diebold AccuVote-TS Voting Machine." Center for Information Technology Policy and Dept. of Computer Science, Princeton University. https://www.verifiedvoting.org/wp-content/uploads/2016/11/ts06EVT.pdf. Pp. 1.

proprietary and always push back against suggestions to adopt open-source code. Our state election officials' sign contracts with these vendors but do not employ enough qualified cybersecurity experts to examine the vender code effectively. Thus, commercial vendors can make every assurance that their machines will operate properly because it is in their best commercial interest to do so and citizens are left in the dark.

Even if a vendor's code is examined, the machines that show up on Election Day could have their code changed from the time of the last audit. Since there is no uniform policy nationwide, states can be more or less thorough in how they structure contracts with vendors and review their code. This situation grants undue power to vendors in the administration of elections and, as with any complex systems, creates many opportunities for failure. DREs are also assembled from open supply chains that present specific risks. The Open Source Election Technology (OSET) Institute, which published a briefing on election infrastructure in 2017, observes that:

> One fundamental source of technical risk to core EI cyber-assets is at the hardware level, via threats from untrustworthy hardware components sourced from an open supply chain with no controls or provenance on acquired components. This risk is particularly notable for voting system components, certainly during the manufacturing process, but more notably for EO operator maintenance in the use of replacement parts over the system components' extended life cycle. This practice has increased over time, due to the effect of market forces on the vendors, and to the effect of EO's reduced capacity for capital expenditures[50]

As elections infrastructure has been declared critical infrastructure, this type of open supply chain must be properly regulated to mitigate risk more effectively.

Though DREs may have created a more user-friendly, voting experience, they have introduced more risk than prior technologies. According to Donald Moynihan, an expert in the

[50] OSET Institute. Critical Democracy Infrastructure: Protecting American Elections in the Digital Age, Threats, Vulnerabilities, and Countermeasures as a National Security Agenda. OSET Institute. September 2017. Pp. 26-27.

application of digital government services, DREs perform worse than prior technologies based on the residual vote. The residual vote is when votes are "lost because voters chose more than one candidate, created an unreadable ballot, or left a ballot blank".[51] He claims that older voting technologies were "relatively simple, with linear and predictable interactions between parts. To varying degrees, the different technologies were imperfect in their ability to count votes, but there was little risk of catastrophic failure".[52] He finds that based on the residual vote, voting systems that have been replaced, like lever machines and manual counting, were more reliable.[53] In summation, if vulnerable DREs are attacked and votes are manipulated, election outcomes could be cast in doubt. And without a paper trail, a recount may not be able to uncover irregularities.[54]

In the end, it may be preferable to remove the DRE machines altogether rather than adding security measures for expensive equipment that is still susceptible to manipulation, even when open-source code and a paper trail are mandated.

Digital Voter Registration Databases (VRDs)

Two widely publicized attacks on VRDs occurred in the 2016 Presidential election, both attributed to Russian election interference. Sensitive information from nearly 200,000 records was stolen in Illinois, while malware was used to breach digital voting records in Arizona[55].

[51] Moynihan, Donald P. "Building Secure Elections: E-Voting, Security, and Systems Theory." Public Administration Review 64, no. 5 (September 2004): 515–28. https://doi.org/10.1111/j.1540-6210.2004.00400.x. Pp. 518.
[52] Ibid., 517.
[53] Ibid., 518.
[54] Ibid., 522.
[55] Norris, *Why American Elections Are Flawed (and How to Fix Them)*, 15.

Even after these attacks, there are still a substantial number of states that have not instituted basic cyber security measures to protect their VRDs.[56]

The Center for American Progress, in a study called "Election Security in All 50 States," presents troubling facts about VRD security:

> Some states still use voter registration databases that are more than a decade old, leaving them susceptible to modern-day cyberattacks. If successfully breached, hackers could alter or delete voter registration information, which in turn could result in eligible voters being turned away at the polls or prevented from casting ballots that count. Hackers could, for example, switch just a few letters in a registered voter's name without detection. In states with strict voter ID laws, eligible voters could be prevented from voting because of discrepancies between the name listed in an official poll book and the individual's ID. In addition, by changing or deleting a registered individual's political affiliation, hackers could prevent would-be voters from participating in partisan primaries[57]

Before discussing the technical components and resulting vulnerabilities that give rise to VRD insecurity, it should be stated that information about specific aspects of systems is closely guarded by the states. Publishing this data could serve as a road map for assailants wishing to infiltrate VRDs. Thus researchers have largely published what the current, general standards are for list creation, maintenance, and cyber security.

VRD Architecture

According to "A Handbook for Elections Infrastructure Security" published by the Center for Internet Security, "Many of the components in elections infrastructure are built on general purpose computing machines, such as traditional web servers and database platforms".[58] Most election officials do not possess the budget or expertise to procure and run state of the art

[56] Root et al., "Election Security in All 50 States".
[57] Ibid.
[58] "A Handbook for Elections Infrastructure Security." CIS. Accessed April 11, 2019. https://www.cisecurity.org/elections-resources/. Pp. 15.

systems, thus the majority of VRDs are run on commercial off-the-shelf (COTS) hardware and software.

VRDs are created in three different ways with respect to data. According to the Center for Internet Security:

> In all of these cases, there is a master voter database at the state level. The 2014 EAC Statutory Overview describes this database as populated in one of three broad ways: 1. A top-down system in which the data are hosted on a single, central platform of hardware and maintained by the state with data and information supplied by local jurisdictions, 2. A bottom-up system in which the data are hosted on local hardware and periodically compiled to form a statewide voter registration list, or 3. A hybrid approach, which is a combination of a top-down and bottom-up system. For all three cases, voter registration systems consist of one or more applications that leverage general-purpose computing systems built on commercial-off-the-shelf (COTS) hardware and software[59]

Risk varies according to the degree of centralization in data storage. Top-down systems attract more attention from hackers because data is more centralized and therefore more easily hacked. Bottom-up systems create a structure where sensitive data is stored at the local level, so state agencies must contact local agencies for proof of registration. This makes it more difficult for hackers to obtain large swaths of voter registration information in a single attack. The next section will detail the resources available to election officials and the risks inherent in running a sensitive operation with internet-connected, COTS software and hardware.

VRD Risks

The risk analysis resources available to election officials include, but are not limited to, the following: International Organization for Standardization (ISO/IEC) 27005, National Institute of Standards and Technology (NIST) Special Publication 800-30, and multiple resources provided through The Cybersecurity Information Sharing Act (CISA) made available

[59] "A Handbook for Elections Infrastructure Security," 15.

by request.[60] These resources assist trained election officials in bolstering defenses and identifying threats. Those states who follow best practices, train election officials, and consult DHS have a *relatively* better chance of properly managing cyber threats than those states (of which there are at least ten) that fail to provide any training for their election officials.[61] But the advantage is only relative as:

> many election officials do not have the expertise or resources to conduct an adequate risk assessment. The ability to efficiently and effectively execute a risk assessment is further reduced by the difficulty in objectively assessing evolving threats, as well as the complexity of the elections processes and systems[62]

The exact risks that election officials face are similar to those faced by virtue of running commercial off-the-shelf systems (COTS).[63] These risks include:

> Risks associated with established (whether persistent or intermittent) internet connectivity, network connections with other internal systems, some of which may be owned or operated by other organizations or authorities, security weaknesses in the underlying COTS products, whether hardware or software, errors in properly managing authentication and access control for authorized users, difficulty associated with finding, and rolling back, improper changes found after the fact, and infrastructure - and process - related issues associated with backup and auditing[64]

These are general risks to COTS systems, which are also present in digital VRDs. There are two main forms of cyber-attack. The first would be to manipulate data in the VRD. This could be done if an assailant gained remote access to the database. Whenever an input operation is required, assailants potentially have the ability to gain remote access, either by stealing usernames and passwords or by installing malware, as occurred in Arizona. According to the Center for Internet Security, "the inputs to voter registration systems are registrations, removals

[60] "A Handbook for Elections Infrastructure Security," 8.
[61] Root et al., "Election Security in All 50 States".
[62] "A Handbook for Elections Infrastructure Security," 8.
[63] Ibid., 16-17.
[64] Ibid., 16-17.

due to ineligibility (e.g., an individual moving out of state, death of a voter), and record updates, most often due to an individual moving within the state".[65]

The second attack approach would be a distributed denial-of-service attack (DDoS), which would make the VRD unavailable for election officials.[66] Cisco, a multinational technology conglomerate, defines a DDoS attack as "bombardment of simultaneous data requests to a central server. The attacker generates these requests from multiple compromised systems. In doing so, the attacker hopes to exhaust the target's Internet bandwidth and RAM. The ultimate goal is to crash the target's system and disrupt its business".[67]

This assessment of DREs and VRDs susceptibility to attack was provided by experts and thus reflects elite opinion. However, lay opinion is also a necessary component in this discussion. In a representative democracy, public opinion should be taken into account, according to the democratic model proposed by Fiorino, when assessing risk environments that has a direct impact on the health of a democracy.

Public opinion on DREs is quite straightforward – most American's think that they should produce a paper trail.[68] When asked about "requiring electronic voting machines to print a paper backup of the ballot," 85% of respondents favored this, with 49% strongly favoring.[69] The results also hold across the partisan divide, with Democrats (and those who lean Democratic) and Republicans (and those who lean democratic) supporting paper trails at 87% and 84%

[65] "A Handbook for Elections Infrastructure Security," 15.
[66] Ibid., 18-19.
[67] "What Is a DDoS Attack? Distributed Denial of Service." Cisco. Accessed April 8, 2019. https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html.
[68] "Views of Election Policy Proposals | Pew Research Center," October 29, 2018. https://www.people-press.org/2018/10/29/views-of-election-policy-proposals/.
[69] Ibid.

respectively.[70] Thus, both elite and democratic models align here meaning there is a clear consensus for this policy.

For VRDs the picture is clouded by divisions in public opinion, and the lack of desire to propose measures that may be counter to US democratic norms. Experts have summarily agreed that improvements to state systems should be made, though no serious proposals for alternative systems have been offered. Technical experts have not projected what a centralized, federal VRD system, which could take the place of state VRDs, would look like. Also, there is no survey data specifically on the question of the efficacy of a federal VRD.

Ordinary Americans seem to be fairly confident in their state's system, while they seem to be skeptical of the efficacy of federal systems:

> The public is not highly confident that election systems in the U.S. are secure from hacking and other technological threats. Currently, 45% of Americans say they are at least somewhat confident that U.S. election systems are secure, though just 8% say they are very confident in the security of these systems and 55% say they are not too (37%) or not at all (17%) confident that these systems are secure…Americans express more confidence about election systems in their state: Two-thirds (66%) say they are very or somewhat confident that election systems in their state are secure from hacking and other technological threats (though just 16% say they are very confident). A third (33%) of adults are not too or not at all confident in the security of their state[71]

Also, public opinion on trust in the federal government to handle sensitive data provides evidence against the prospect of a federal VRD. About half of those polled by Pew are not confident that their private data will be properly protected by the federal government (only 12% are very confident).[72]

---

[70] "Democrats More Likely to Back Automatic and Same-Day Registration; Support for Voter ID Higher in GOP | Pew Research Center." Accessed April 11, 2019. https://www.people-press.org/2018/10/29/views-of-election-policy-proposals/4-2-3/.

[71] "Voter Views on U.S. Election Security | Pew Research Center," October 29, 2018. https://www.people-press.org/2018/10/29/election-security/.

[72] "How Americans Feel about Social Media and Privacy." Pew Research Center (blog). Accessed April 8, 2019. https://www.pewresearch.org/fact-tank/2018/03/27/americans complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

These concerns suggest that a policy solution that adds paper trails to DREs is needed (considering both elite and democratic models). The picture with VRDs is complicated by the fact that federal systems are judged to be susceptible by both experts and ordinary Americans but ordinary Americans also believe that their states do a better job in securing DREs.

Policy Options

One policy option would be the status quo. Current policy could be left intact while providing more funding to the states through HAVA (the federal government just provided 380 million dollars to the states to improve election infrastructure).[73] Providing additional funding to cash-poor states to improve election systems is one approach. In addition, the states could be urged to become more involved with DHS in cyber security measures to protect VRDs more effectively.

Secure Elections Act

An alternative policy option could look like the Secure Elections Act of 2017, which was introduced in the House of Representatives in 2017. It mandated "states to use backup paper ballots and to implement postelection audits to ensure that voting systems were not compromised".[74] This mandate would have required DRE machines to produce a paper trail that its internal tabulation could be checked against. The Republicans in Congress claimed the

[73] "2018 HAVA Election Security Funds | US Election Assistance Commission." Accessed April 11, 2019. https://www.eac.gov/2018-hava-election-security-funds/.
[74] Edmondson, Catie. "Once Bipartisan, an Election Security Bill Collapses in Rancor." The New York Times, August 31, 2018, sec. U.S. https://www.nytimes.com/2018/08/31/us/politics/election-security-bill.html.

mandate for paper trails was outside of their authority, while the White House declared that it violated states' rights.[75] If reconsidered, an effective argument would need to be made for how it aligned with the Constitution and it would need to be coupled with funding to the state's for this purpose, which the Act did not initially provide.

For the People Act

Another policy option could look like the For the People Act of 2019. Democrats in the House of Representatives introduced this Act to improve upon current federal standards. According to the Brennen Center For Justice, the For The People Act would make it "easier for voters to cast a ballot and harder for lawmakers to gerrymander, by transforming how campaigns are funded to amplify the voices of ordinary Americans, and by bolstering election security and government ethics".[76]

The For the People Act does not amend the related provisions in HAVA to mandate minimum cyber security standards; it is drafted to be in compliance with Section 303 from HAVA. The only significant, potential updates are in Section 1915, Section 298, and Section 321. Section 1915 calls for the Election Assistance Commission (EAC) to assess its own cybersecurity methods while Section 298 calls for cybersecurity enhancements, but the suggestions refer to best practices and the specifics are left to the states.[77] The last section to address digital security is Section 321, which provides grants to entities "for purposes of research

[75] Edmondson, "Once Bipartisan, an Election Security Bill Collapses in Rancor".
[76] "For the People Act of 2019 | Brennan Center for Justice." Accessed February 23, 2019. https://www.brennancenter.org/legislation/for-the-people-act-2019.

[77] U.S. Congress. House. The For the People Act of 2019. HR 1. 116th Cong., 1st sess. Introduced in House January, 3, 2019. https://www.congress.gov/bill/116th-congress/house-bill/1/text.

and development that are determined to have the potential to significantly to improve the security (including cybersecurity), quality, reliability, accuracy, accessibility, and affordability of election infrastructure".[78] These provisions largely leave in place current systems and do not provide specific standards, besides "best practices."

Both the Secure Elections Act and the For the People Act call for mandated paper trails for DREs, which, as noted, is supported by public opinion at a rate of 85%.[79] Thus, both elite and democratic models align, which means there is a clear consensus for this policy.

For VRDs experts express a mixture of opinions on the necessary changes to current policy and no expert advocate new policy for a federal VRD system. Some researchers suggest additional cyber security measures on the state level using known techniques, some suggest increased interaction with DHS, and others encourage experimentation with new technical standards at the state level. Also, survey data to gauge the public's opinion on different VRD policies does not yet exist. Further research is needed to gauge expert and lay opinion on different VRD policies.

Other Policy Options

New policy could induce the states to bolster their cyber security measures through federal funding, which would be unlocked by adopting pre-defined layers of cyber security. The first level of funding could be certification of VRDs. A second level could be for certification in addition to adopting basic cyber security measures like access controls, passwords, multi-factor authentication (MFA), logging and monitoring activity, training, regular back-ups, provisional

[78] U.S. Congress. House. The For the People Act of 2019.
[79] "Views of Election Policy Proposals | Pew Research Center".

ballots, and communicating with other states.[80] A third level could be unlocked with enhancements to supply chain security. This money, once unlocked, could be used by the states to improve all election infrastructure, not just digital systems, making the inducements more attractive. This would avoid creating a federal mandate, something that more conservative states might see as federal overreach.

Alternatively, an innovative policy option like a federal VRD system with state of the art cyber security features could be created and introduced in Congress. The features of this policy would need to take into account current path dependencies and technical limitations (current technology used in the states is larger made up of COTS hardware and software). The best way to administer a federal VRD system could be a top-down approach, where the sensitive information is stored at the local level. For instance, when individuals go to the DMV to get or renew a license, they can provide a hand-written signature attesting to their desire to register to vote. That paperwork could be stored at the DMV and then a federal VRD administrator could contact the DMV office and verify that attestation, and add that individual as qualified voter for an upcoming presidential election. This system could be enhanced with state of the art cyber security, perhaps with a KSI Stack, which is discussed below.

Potential Technical Improvements to Digital Election Infrastructure

Open-Source Technology

One option to improve DEI would be to adopt open-source technology. The open-source technology proposal could greatly increase transparency in DEI. Though this solution is not

[80] "Election Security | Cybersecurity: What Legislators (and Others) Need to Know"

comprehensive, it could lead to a more democratic model of election administration. Currently, proprietary code is used in DREs and other electronic voting machines. In addition, proprietary companies have large, open supply chains that introduce more risk, as hardware and software are vulnerable to tampering at several points in the supply chain. The Open Source Election Technology Foundation (OSET) has developed an open-source approach to improving DEI and voter confidence. Their mission is to "reinvent election technology by using open data, open standards, and open source to increase confidence in elections and their outcomes, and help preserve our democracy".[81] Open-source technology would be one effective way to improve cyber security of DEI, and language mandating this technology could be inserted in new, federal legislation. One significant advantage with this route is that it would avoid debate about federal overreach if it is mainly focused on improvements to technology.

Estonian KSI Stack

A more radical improvement would be the KSI Stack system, which could be used at either the federal or state level. The country of Estonia has a digital citizenship system, which is the resource that Estonian election officials reference when determining if a citizen is legally able to vote. The system provides state of the art cybersecurity while increasing efficiency. Their "once-only" policy says that by law, the government can only ask for information from individuals one time.[82] This information is then shared within the government and is released to private parties on a permission basis, and only in discrete amounts. The fact that information can only be asked for once means that it must be securely stored indefinitely, which led directly to

[81] "Mission." TrustTheVote (blog), September 5, 2014. https://trustthevote.org/home/mission/.
[82] Law of Obligations Act – Riigi Teataja. Accessed February 24, 2019. https://www.riigiteataja.ee/en/eli/524012017002/consolide.

the adoption of an innovative record management system referred to as the Keyless Signature Infrastructure (KSI) Stack. The KSI Stack creates a permanent and unalterable record of all data according to the following principles:

> KSI is a blockchain technology designed in Estonia and used globally to make sure networks, systems and data are free of compromise, all while retaining 100% data privacy. A blockchain is a distributed public ledger – a database with a set of pre-defined rules for how the ledger is appended by the distributed consensus of the participants in the system. Due to its widely witnessed property, blockchain technology makes it also impossible to change the data already on the blockchain. With KSI Blockchain deployed in Estonian government networks, history cannot be rewritten by anybody and the authenticity of the electronic data can be mathematically proven. It means that no-one – not hackers, not system administrators, and not even government itself – can manipulate the data and get away with that[83]

US states could experiment with this technology for their VRDs and the results could be valuable if a federal solution for VRD management is chosen in the future. Integration of this technology in the US is not just hypothetical either. Guardtime, the company that developed the KSI Stack for Estonia, has partnered with SICPA to offer their services to U.S. states for VRD management.[84]

According to David Collingridge (a contributor to the edited volume by Hood and Jones mentioned in my frames of analysis section) provides insight into why experimentation at the local and state level is desirable:

> Decision-makers can never relax in the assurance that they have identified the very best option; any choice may be shown to be mistaken by future events that surprise the decision-makers. However, much research and propaganda on risk assessment and management assumes the very opposite; that some choices can be known to be the best and, therefore, do not require any humility from the decision-makers' search for resilience as a counter to deep uncertainty. In reality, it is necessary to admit that all that

[83] "KSI Blockchain." e-Estonia. Accessed April 11, 2019. https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/.
[84] "SICPA and Guardtime Announce Solution to Architect Trust into U.S. Elections-Guardtime." Accessed February 24, 2019. https://guardtime.com/blog/sicpa-and-guardtime-announce-solution-to-architect-trust-into-u-s-elections.

> can be hoped for is a more or less efficient trial-and-error learning from experience of technology…[85]

Experimentation with new systems in the states is important because there are too many unforeseen consequences when these systems are deployed too soon. From a risk management perspective, if there is no experimentation stage then there will be little flexibility around the three components of risk management (goal-setting, information gathering and interpretation, and action to influence human behavior and modify physical structures).

Conclusion

To circle back to the research questions that guided this thesis: Why is US digital election infrastructure (DEI) vulnerable and what are the possible options to better secure it? To answer this question this thesis analyzed current federal policy governing DEI as well as current, technical vulnerabilities.

On the level of policy, HAVA no longer adequately protects suffrage rights as a result of its decentralized, hands-off approach to DEI. The hands-off approach of federal policy produces four levels of variance: system (top-down, bottom-up, hybrid), legal framework (some lists mentioned in statues, come are not), certification (eight states require certification), and cyber security standards.

On the level of technical vulnerabilities, DREs and VRDs are both susceptible to manipulation. Experts as well as ordinary Americans have provided a clear mandate to remove DREs, or at a minimum, to provide a paper trail to DREs. This is a fairly substantive integration

[85] Hood and Jones, *Accident and Design: contemporary debates in risk management,* 45.

of elite and democratic models in risk management. Risk, as it pertains to consequence, would clearly be mitigated if these machines are removed or at the very least paper trails are introduced.

For VRDs, the picture is muddied by lack of consensus, and thus there is little desire to propose measures that may be counter to US democratic norms. Experts have summarily agreed that improvements to state systems should be made. Technical experts have not projected what a federal VRD system would look like, however. Also, there is no survey data specifically on the question of the efficacy of a federal VRD.

Ordinary Americans seem to be fairly confident in their state's system, while they seem to be skeptical of the efficacy of federal systems.[86] If another federal system were to be proposed in Congress, an effective argument would have to be made as to why it would be superior to state systems. Also, public opinion on trust in the federal government to handle sensitive data provides further evidence for the prospect of a federal VRD.[87]

If a centralized system with superior cyber security was to be instituted, thus replacing the extant patchwork of state systems, it would have to be aligned with the Constitution, current policy, and democratic norms. The case therefore would need to be strong enough to overcome contemporary partisan polarization on the issue of election administration.

Creating new a new VRD system at the federal level without first conducting a rigorous trial of the system may introduce even more risk. It would be advisable to first experiment in the states with new VRD solutions before creating a new federal system. The resilience of this experimental system should undergo sufficient testing in a lower stakes environment, perhaps in one municipality or in one state, where negative results can be contained.

[86] "Views of Election Policy Proposals | Pew Research Center"
[87] Ibid.

Other options considered were two recent federal policy proposals, the Secure Elections Act and the For the People Act. While they do mandate a paper trail for DREs, they do not move the needle on cyber security of VRDs. Neither provides a comprehensive solution adequate to the threat level. Another option would be to induce the states to bolster their cyber security measures by offering federal funding, which would be unlocked by adopting pre-defined layers of cyber security. This option would avoid issuing a federal mandate but it is not clear whether states who have no interest in improving their election infrastructure for partisan reasons would be persuaded to improve security standards. Without a mandate, presidential elections may still be plagued by significant variance in cyber security, thus leaving the nation open to attack.

Lastly, two intriguing, potential technical improvements have been detailed, the OSET, open-source proposal, and the Estonian KSI Stack solution. The open-source technology proposal could greatly increase transparency in DEI. Though this solution is not comprehensive, it could lead to a more democratic model of election administration.

The second technical option discussed was the Estonian KSI Stack solution. States could experiment with this technology to improve their VRDs, and if the results are positive, this policy could diffuse to the federal government.

Suggestions for further research include scientific quantification of risk from the national perspective, gathering survey data specifically on different policies for VRDs, estimations of cost for different policy options, and projections of political feasibility. For the latter, a living sample study could be conducted to gauge how public opinion on cyber security of DEI changes as it is exposed to new data over time.

In summation, DEI is at risk because federal policy currently enables states to use Direct-Recording Electronic (DRE) voting machines without a paper trail and it also enables states to

manage their own risk environment with digital voter registration databases (VRDs), which produces significant variance in outcomes in cyber security and priority of VRD governance. These factors combine to leave the existing system in a vulnerable state. The security flaws in VRDs and DREs could be exploited in a targeted attack during a Presidential election, which would likely result in disastrous consequences. Policy options and technical improvements should be explored to properly secure suffrage rights. Regardless of partisan differences, all Americans should be confident that their registration will be honored and that their votes will be counted.

Bibliography

"2018 HAVA Election Security Funds | US Election Assistance Commission." Accessed April 11, 2019. https://www.eac.gov/2018-hava-election-security-funds/.

"A Handbook for Elections Infrastructure Security." CIS. Accessed April 11, 2019. https://www.cisecurity.org/elections-resources/.

Becker, David, Jacob Kipp, Jack R. Williams, and Jenny Lovell. "Voter Registration Database Security." The Center for Election Innovation Research. September 2018.

"Democrats More Likely to Back Automatic and Same-Day Registration; Support for Voter ID Higher in GOP | Pew Research Center." Accessed April 11, 2019. https://www.people-press.org/2018/10/29/views-of-election-policy-proposals/4-2-3/.

"DHS Cybersecurity Services Catalog for Election Infrastructure." Accessed March 21, 2019. https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Elect on_Infrastructure.pdf

"Concerns about Voter Access and Eligibility | Pew Research Center," October 29, 2018. https://www.people-press.org/2018/10/29/concerns-about-eligible-voters-being prevented-from-voting-and-ineligible-voters-voting/.

Edmondson, Catie. "Once Bipartisan, an Election Security Bill Collapses in Rancor." *The New York Times*, August 31, 2018, sec. U.S. https://www.nytimes.com/2018/08/31/us/politics/election-security-bill.html.

"Election Security | Cybersecurity: What Legislators (and Others) Need to Know." Accessed April 5, 2019. http://www.ncsl.org/research/elections-and-campaigns/election-security.aspx.

"Election Security." Department of Homeland Security, March 27, 2018. https://www.dhs.gov/topic/election-security.

"Electronic Poll Books | E-Poll Books." Accessed April 11, 2019. http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

Feldman, Ariel J., J. Alex Halderman, Edward W. Felten. "Security Analysis of the Diebold AccuVote-TS Voting Machine." Center for Information Technology Policy and Dept. of Computer Science, Princeton University. https://www.verifiedvoting.org/wp-content/uploads/2016/11/ts06EVT.pdf.

Fiorino, Daniel J. "Technical and Democratic Values in Risk Analysis." *Risk Analysis* 9, no. 3 (September 1989): 293–99. https://doi.org/10.1111/j.1539-6924.1989.tb00994.x.

"For the People Act of 2019 | Brennan Center for Justice." Accessed 23 Feb. 2019 https://www.brennancenter.org/legislation/for-the-people-act-2019.

"Global Wealth Report 2018." Credit Suisse. Accessed April 11, 2019. https://www.credit-suisse.com/corporate/en/articles/news-and-expertise/global-wealth-report-2018-us-and-china-in-the-lead-201810.html.

Hood, Christopher, and David K. C. Jones, Eds. *Accident and Design: Contemporary Debates in Risk Management*. London ; Bristol, Pa: UCL Press, 1996.

"How Americans Feel about Social Media and Privacy." *Pew Research Center* (blog). Accessed April 8, 2019. https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

"KSI Blockchain." e-Estonia. Accessed April 11, 2019. https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/.

Law of Obligations Act - Riigi Teataja. Accessed February 24, 2019. https://www.riigiteataja.ee/en/eli/524012017002/consolide.

"Mission." *TrustTheVote* (blog), September 5, 2014. https://trustthevote.org/home/mission/.

Moran, Michael, Martin Rein, and Robert E. Goodin, eds. *The Oxford Handbook of Public Policy*. The Oxford Handbooks of Political Science. Oxford ; New York: Oxford University Press, 2006.

Moynihan, Donald P. "Building Secure Elections: E-Voting, Security, and Systems Theory." *Public Administration Review* 64, no. 5 (September 2004): 515–28. https://doi.org/10.1111/j.1540-6210.2004.00400.x.

National Voter Registration Act of 1993, H.R. 2, 103rd Cong. (1993), 52 U.S.C. § 20507.

Norris, Pippa. *Why American Elections Are Flawed (and How to Fix Them)*. Vol. 1. Cornell University Press, 2017. https://doi.org/10.7591/cornell/9781501713408.001.0001.

OSET Institute. Critical Democracy Infrastructure: Protecting American Elections in the Digital Age, Threats, Vulnerabilities, and Countermeasures as a National Security Agenda. OSET Institute. September 2017.

Root, Danielle, Liz Kennedy, Michael Sozan, and Jerry Parshall. "Election Security in All 50 States." Center for American Progress. Accessed April 4, 2019. https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.

"Russian Hacks on U.S. Voting System Wider Than Previously Known." Accessed March 28, 2019. https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

"SICPA and Guardtime Announce Solution to Architect Trust into U.S. Elections - Guardtime." Accessed February 24, 2019. https://guardtime.com/blog/sicpa-and guardtime-announce-solution-to-architect-trust-into-u-s-elections.

Smith, Denis, and Alan Irwin. “Public Attitudes to Technological Risk: The Contribution of Survey Data to Public Policy-Making.” *Transactions of the Institute of British Geographers* 9, no. 4 (1984): 419. https://doi.org/10.2307/621778.

“Statewide Voter Registration Systems | US Election Assistance Commission.” Accessed April 5, 2019. https://www.eac.gov/statewide-voter-registration-systems/.

“The National Voter Registration Act Of 1993 (NVRA),” August 6, 2015. https://www.justice.gov/crt/national-voter-registration-act-1993-nvra.

Tokaji, Daniel. “Voter Registration and Election Reform.” The William and Mary Bill of Rights Journal 17, no. 2 (2008): 453-506.

U.S. Congress. House. The For the People Act of 2019. HR 1. 116th Cong., 1st sess. Introduced in House January, 3, 2019. https://www.congress.gov/bill/116th-congress/house-bill/1/text.

U.S. Congress. House. The Help America Vote Act of 2002. HR 3295. 107th Cong., 2nd sess. Introduced in House November 14, 2001. https://www.congress.gov/bill/107th-congress/house-bill/3295/text.

“Views of Election Policy Proposals | Pew Research Center,” October 29, 2018. https://www.people-press.org/2018/10/29/views-of-election-policy-proposals/.

“Voter Views on U.S. Election Security | Pew Research Center,” October 29, 2018. https://www.people-press.org/2018/10/29/election-security/.

“Voting Machines at Risk: Where We Stand Today | Brennan Center for Justice.” Accessed March 16, 2019. http://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

“Voting Technology | MIT Election Lab.” Accessed April 11, 2019. https://electionlab.mit.edu/research/voting-technology.

“What Is a DDoS Attack? Distributed Denial of Service.” Cisco. Accessed April 8, 2019. https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html.