Analyzing the Impact of Voting Technology on United States Election Integrity

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Jeremy Nathan
Spring, 2020

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Analyzing the Impact of Voting Technology on United States Election Integrity

Motivation

Guaranteed by the U.S. Constitution and expanded in the 15th and 19th amendments, the right to vote has always been a cherished tenet of U.S Democracy – so much so that many fought and died over it. The means by which citizens cast their vote, however, has constantly changed with technological developments. One of the more recent changes was the rise of electronic voting machines (Formally, DRE or Direct-Recording-Electronic machines), which surged in popularity in the 2000's (Garner et.al., 2005). Though these new machines have improved voting accessibility to previously marginalized groups, studies have demonstrated vulnerabilities which could provide malicious actors a way to unfairly influence the election process. These vulnerabilities call into question whether advances in voting technology such as DREs are truly compatible with the U.S. electoral system – and if they are, officials must find ways to safeguard the voting process to prevent subversion of the democratic process. Since voting technology in the United States is influenced by diverse factors that in turn influence each other, voting technology can be more easily analyzed in a network format. Consequently, the sociotechnical framework used to describe this research topic is Actor-Network theory.

Research Question and Methods

This thesis seeks to answer whether advances in voting-related technology impact the integrity of the voting process in the United States.

The two methods that this paper uses to frame supporting evidence are historical case studies and network analysis. Historical case studies will demonstrate the problem this research

is addressing by providing the context needed to understand how Actor-Network theory is applied. Two examples of these historical case studies include the 2000 presidential election in Florida and the 2016 presidential election, which have been outlined briefly in the previous section. For each of these cases, network analysis is applied by examining how each agent in the network, such as election management systems and local governments, is connected to each other. From there, use of the algorithm above outlines intermediaries and discover new actors. For instance, inputting the keyword "DRE Machine" into UVA's Virgo Database and into Google Scholar yields results corresponding to the history of DRE machines – how they gained popularity as a result of inadequate ballot-punching mechanisms associated with the 2000 presidential election. In addition, this search yields results on how vulnerabilities have been detected in the systems that make use of the machines. As a result, two new relationships and actors are added to the network. By repeatedly applying this approach to new nodes that are unraveled in the network, this method will also serve as a way of developing the Actor Network Theory-based framework used to frame the research conducted as part of this paper.

Background

The 2000 United States election, in which George W. Bush narrowly defeated Democratic challenger Al Gore, was particularly notable in comparison to other presidential elections in the 20th century: the result of the overall election was only decided months after the election itself was held. The primary reason this delay occurred was due to discrepancies in vote counting in the state of Florida, whose 29 electoral votes would decide the outcome of the election. At the time, a punch card-style ballot was employed in Florida in which voters used a hole puncher to mark their desired candidate. However, many ballots had been incompletely

punched, and as a result, a formal, detailed set of rules had to be devised for processing these ballots.

Electronic voting machines, also known as DRE (Direct Recording Electronic) machines, were developed in the late 1990's, and what happened in the 2000 election regarding the improperly marked ballots – referred to as the "Hanging Chads" controversy – facilitated their adoption across the United States (Garner et.al., 2005). DRE voting machines consist of an installed software that allows verified voters to navigate through a digital ballot (usually through an accessible touchscreen) to submit their vote. When votes are stored and recorded, they are written to a storage disk that exists on each machine, similar to a personal computer. This localized data storage adds a layer of security, since hackers must gain physical access to many machines in order to significantly affect a vote count. However, the data these machines store must eventually be uploaded to some other system which tallies the votes. These election management systems, which often receive data from all DRE machines in their jurisdiction, are the prime target of hackers – by gaining access to these systems, they can have a broader impact on an election's outcome with less effort compared to physically altering data in individual machines (Moynihan, 2004).

Unfortunately, the United States has already experienced a breach of election management systems by foreign entities. In the 2016 presidential election, Donald Trump narrowly defeated Democratic challenger Hillary Clinton, amassing just enough votes to flip key states such as Florida, Michigan, and Pennsylvania – which were initially thought to be safely Democratic – and secure his presidency. While the difference in poll opinions between Bush and Gore was thin prior to the 2000 election (Gallup, 2000), the result of the 2016 presidential election shattered most predictions of the election's outcome. Now, an official government report

from the Senate Intelligence Committee detail how Russian hackers were able to gain widespread access to election management systems in the 2016 election, including systems in some of the key swing states mentioned above (Senate Committee on Intelligence, 2019). Though the report also states that there was no evidence found that definitively proves vote counts were altered, that this type of breach happened in the first place has fueled discussion among cybersecurity experts and political groups alike regarding solutions to be implemented in the next presidential election in 2020.

STS Framework

Actor-Network theory is an algorithm that facilitates the unraveling of links between non-human and human "actors" that could influence a sociotechnical problem. This method defines actors as entities in a network that perform a broad set of actions, including recruiting other actors into the network through common themes ("languages"). Actor-Network Theory is effective as a lens through which STS researchers have viewed diverse topics such as Wildlife Tourism in Antarctica and scallop farming sustainability in France (Rodger et.al., 2009). Regarding the broader topic of the American election system, multiple sociotechnical frameworks, including Actor-Network Theory, are applied to contextualize discourse and research.

One example is the Politics of Technology framework, which was used to examine one impact of the use of DRE voting machines in the 2016 election (Justice et.al., 2019). Specifically, Justice et.al. was able to demonstrate how media outlets were able to take advantage of a lack of public familiarity with how DRE machines fit to create the narrative that Russia had "hacked" into the 2016 election to influence the outcome. In reality, this narrative

was not completely true: Russian hackers had gained access to some election management systems at a state- and county- level, but no manipulation of vote counts was found. As a result of this narrative, Justice argued, these media outlets could better argue for the urgency of election security measures and highlight Republicans' lack of willingness to address the issue. Next, a variant of Actor-Network theory was used to analyze the link between internet use and participation in the 2008 presidential election (Buente, 2015). In this analysis, though the initial scope outlined only contained one link, Buente was able to effectively use two steps in the Actor-Network theory algorithm – problematization and interessement – to elucidate other factors that contributed to the link. For instance, through interessement, Buente found that factors such as race, socioeconomic status, frequency of overall internet use, and internet availability all played a role in the network; as a result, he was able to include these variables as part of the statistical analysis he completed to demonstrate the significance of certain links between elements in the network compared to others.

Actor Network Theory is an extremely generalized framework, and as a result, has multiple critiques. One such critique (Whittle et.al., 2008) argues that Actor Network Theory framework attributes the separation between human and nonhuman actors as natural or inevitable as a result of its process, when these separations may be deliberate. However, Whittle et.al. reserve this critique for using Actor Network Theory on hierarchical organizations; the network that the analysis of election security produces is not as rigidly structured. Another challenge associated with Actor-Network theory is that the network must be constantly maintained and re-examined as new actors or relationships are discovered. These discoveries threaten to open "black boxes," which represent abstractions of certain nodes in the network that can be expanded further. To resolve this problem, this paper focuses on developing a snapshot of the network as it exists

currently. This will also enable the scope of the research to be more targeted towards answering the research question.

Results and Discussion

DRE machines make use of technological advances in computation, data storage, and user interface design in order to streamline the citizen voting experience in the United States. However, they must be woven into an effective system in order to be a true benefit to the US electoral process. The implementation of such a system must ensure the accuracy and consistency of the vote recording process. This consistency is best achieved through a combination of reliable underlying technology, as well as increased government oversight in the development and deployment of the voting machines. This increased oversight would also include a framework for rapid and efficient response to attacks on voting systems. To support the design of a secure DRE machine-based system, a network of actors is examined in which two central languages include cybersecurity—the focus on preventing the use of the designed voting system in unintended, potentially malicious ways—and government regulation of technology.

Problems with voting mechanisms gained widespread media coverage and public concern with the hanging chad controversy of the 2000 presidential election (Garner, 2005). In response, many political science experts have proposed fixes to the current voting system that would potentially remedy some of the reliability and security issues that current DRE machine-based voting systems face. Though some propose the elimination of DRE machines altogether (Lindley, 2008), such a measure would prevent the widespread benefits of DRE machines from being realized (Dill & Castro, 2008). For instance, since most DRE machines require the tap of a touchscreen to navigate through the voting process, accessibility is increased to those who may

not be able to properly use a pen to fill in a ballot. The ballots and instructions could also easily be viewed in a multitude of languages and font sizes, increasing convenience for citizens who may not be able to read English well and for those with impaired vision. Finally, last-minute ballot changes are much easier to accommodate, since new ballots do not have to be reprinted (Dill et al, 2003). This paper examines two potential solutions that would preserve the DRE machine as the main user interface: a blockchain-based voting system, and a system that combines DRE machines with a paper trail through optical ballot scanning.

Following the language of the network, one key element that underpins modern cybersecurity practices is cryptography, which involves the encryption and decryption of sensitive data to prevent unintended access to the data. One system, which is a framework that heavily relies on cryptography to solve multi-layered problems, is blockchain. Since the rise of the blockchain concept in the early 2010's through its flagship application–BitCoin—scholars have expanded the idea to electoral systems (Khan et al., 2020). At a high level, blockchain is a decentralized ledger of transactions that is added to by nodes in a network; since each node has a copy of the ledger, they are all updated when a transaction occurs. Each transaction can be represented as a "block" with a unique fingerprint that dedicated computers independently verify. Moreover, each block contains unique elements derived from the previous block's fingerprint; as a result, adding transactions is like adding "blocks" to the existing "chain." This system provides two key advantages: low overhead, and the lack of a need to place full trust in a centralized record of transactions (ledger). For bitcoin, this system allows fee-free transactions between users, and also allows users to have increased faith in the integrity of their transactions. Since each user in the network has a copy of the ledger, and each transaction is independently verified through many sources, it is difficult for an errant transaction (i.e. a transaction whose

information does not match the agreed intents of the sender and receiver) to be recorded. For the voting process, this decentralized ledger is also one of blockchain's most salient benefits. Each transaction would have a unique cryptographic signature that corresponds to a one-to-one match between a voter and a candidate. Since each node (i.e. voting machine) in the network has its own copy of the transaction record that must cryptographically match the others' copies by design, it is more difficult for external influences to manipulate the record of votes.

While blockchain is a relatively new technology that has seen success with BitCoin, a blockchain-based voting system has logistical drawbacks. One major flaw is the specific architecture that needs to be in place for the system to function. As detailed by Khan, et. al, transaction verification and generation of blocks to add to the chain are both computationally intensive tasks that require adequate processing power. A lack of the necessary processing capabilities could lead to bottlenecks in vote recording times and ultimately cause the system to slow down by orders of magnitude. Confirming this, even with an optimal experimental setup, Khan et. al recommend the use of the blockchain-based voting system they suggested for "small to medium voting environments." Another drawback relates to the novelty of the technology. Blockchains have many parts, from transaction verifiers to block generators and a dedicated network of nodes, that must integrate seamlessly for the entire system to function. Election agencies across the United States would require administrators with blockchain expertise to properly set up blockchain systems in electoral districts prior to each election; currently, due to the niche applications of blockchain, such expertise is not widespread (Grover et al. 2019).

Investigating the individual components that comprise the blockchain actor yields a solution to another issue that one part of the voting system faces. The concept in question is the decentralization of data: since each node in the blockchain independently stores an equivalent

copy of the record of transactions, the record becomes more secure. As a result, this idea of having a distributed system (a network of computers that share identical copies of a set of data) would be particularly useful for securing systems that tally votes for a given state or large district by collating the votes received from each subdivision. Security of these vote-tallying systems an important issue, since a recent study conducted by the Senate Intelligence Committee determined that Russian hackers had gained access to such systems (Senate Committee on Intelligence, 2019); though no evidence of vote count tampering was conclusively proven, manipulation of these systems which have a broader reach over multiple voting districts would easily eclipse the harm done by exploiting a single voting machine. Since distributed systems store copies of data across a network, the total vote tallies become more secure. Finally, a distributed system of central vote tallying is also much leaner to implement, since distributed systems do not need to account for transactions at all; they simply store data.

At the user level, a simpler alternative to a blockchain-based voting involves an extension of the paper trail method. This method involves a small modification of the current DRE machine technology, in which the receipt that the DRE machine produces is what is analyzed as the primary record of the machine's votes (as opposed to the normally used memory card). The receipt containing the machine-marked ballots can be fed through an optical ballot scanner as a means of tallying the votes. Optical Ballot Scanning technology has been present in a wide range of applications (such as the famous Scantron for standardized testing) since the mid-20th century and is able to read marks on pre-formatted ballots with high accuracy (Smith et al., 2008). Since the machine would be marking the receipt in a consistent manner with each vote submitted, the efficacy of the optical scanner method would be extremely high. This consistent, accurate performance results because optical ballot scanning performs best if markings are dark and

consistent (Smith et al., 2008). Finally, if there is need for a recount, the memory cards can be analyzed to corroborate the tallies provided by the optical ballot scans. This method would be much easier to implement than blockchain, since it requires a comparatively trivial change to current voting technologies and systems. In conjunction with the distributed electoral management system described earlier, this implementation would afford increased security of large-scale vote tallying systems, such as state-wide ones.

The two languages of the network, cybersecurity and government regulation of technology, are intricately linked: foreign actors are capable of infiltrating key technological infrastructure, as was demonstrated in the 2016 election. As a result, the next major component of a more robust solution to modernizing the US voting process involves active government oversight. Currently, private companies manufacture their own voting machines and develop their installed software through closely guarded, highly confidential processes (Lindley, 2008). At first glance, this seems like an effective security measure that would prevent attackers from gaining information about the machine and software that could be used to find and exploit vulnerabilities. However, the decision to not disseminate information about the underlying software of manufactured DRE machines requires the voter to have complete faith in the manufacturing process of the voting machines, since there is practically no way to verify the security and reliability of the machine before it has to be used in an actual election (Lindley, 2008). This lack of oversight can have dire consequences: if the company responsible for the development of the DRE machine software does not properly secure their code base with the necessary hierarchy of permissions, for instance, attackers could manipulate the software to their favor prior to their upload onto the physical machines' hard drives.

Oversight of consumer systems commonly used by US citizens by Federal Agencies is not a foreign concept. Since 2000, the National Institutes of Standards and Technology (NIST) has maintained a National Vulnerability Database (NVD), a centralized repository to which external cybersecurity experts can submit vulnerabilities discovered consumer systems (NVD-general, n.d.). One such entry was CWE-119 (CWE-119, NVD), a vulnerability associated with certain functions in the C language that allowed attackers to overwrite sensitive data if they submitted maliciously formed data to the function. For this vulnerability, the NVD even recommended patches for every part of an infrastructure that it could affect, from software to system architecture. In contrast to the NIST NVD, however, the National Security Agency (NSA) operated through the early 2010's largely without reporting vulnerabilities to the public. This style of operation was one consequence of the Patriot Act, passed by President George Bush in the wake of the 9/11 terror attacks. The Patriot Act caused the NSA to focus on exploiting vulnerabilities in consumer hardware and software to monitor citizens' interactions with technology, therefore providing federal agencies with a way of monitoring suspicious activity and identify potential terrorist threats. However, after whistleblower and former NSA employee Edward Snowden revealed the extent of data collection the NSA performed on American citizens, the NSA lost a significant amount of trust with the American public. Consequently, this precedent of independent operation has shifted in recent years. In early January 2020, an update to Microsoft's Windows 10 Operating System enabled a vulnerability in the cryptographic signature interface that the Operating System used (National Security Agency, 2020). This vulnerability was particularly dangerous, since malicious users could use the vulnerability to disguise malware as a verified Windows update, leading users to unknowingly install the

malware onto their devices. For the first time in the case of a significant, wide-reaching vulnerability, the NSA – not an external source – was the primary reporter of the vulnerability.

Regardless of how secure the technology underlying the US voting system is, one of the core tenets of cybersecurity states that attackers will always find new vulnerabilities. Consequently, federal agencies such as the NSA would have to actively ensure the adequacy of a voting system's defenses, just as they discovered and reported the vulnerability in Windows 10. One effective way to accomplish this active security testing is through a red/blue team dynamic (Oakley, 2019). Commonly implemented in organizations that require a high level of data security, a red team emulates the behavior of a hacker by trying to find and exploit vulnerabilities in a software before it is deployed for broader use. The blue team, on the other hand, is responsible for patching the discovered vulnerability as quickly and efficiently as possible to minimize damage to the system. A federally created election technology red/blue team would need to work closely with all levels of the voting infrastructure – including developers of voting machine software, manufacturers of DRE machines, and system administrators of election management systems responsible for tallying and reporting vote counts for large districts.

This analysis can be augmented through a more formal construction of the network of actors discussed. Problematization, the first step of the Actor-Network theory, is achieved through formulating the main research question, and determining that the American electorate is the main group affected by the problem. Using DRE machines as the starting actor, and cybersecurity as the language of the initial network, new actors are enrolled that promise an increased level of protection from outside influences. These actors include the two schemes discussed: an optical scanning system, and blockchain voting systems. Blockchain voting systems introduce a new

language—decentralization of data storage as a means of increasing data integrity—which enrolls election management/vote tallying systems into the network. Next, applying the government oversight language to DRE machines enrolls two relevant government agencies, the NIST and NSA, as actors. Finally, using cybersecurity as a linking language, the NSA actor enrolls red/blue team testing as a means of effective oversight of privately manufactured DRE machines supported by optical ballot scanning.

Two of the main limitations of this analysis are the finite period during which this analysis was conducted, and the scope of the network analysis. Actor-Network theory provisions for a constantly evolving network of actors connected to each other through various links and languages. For the purposes of this analysis, a snapshot of the network representing its state as of the 2019-2020 timeframe was examined. Next, the scope of the analysis focused mainly on how different actors, including non-human ones such as DRE machines and human actors such as federal agencies relate to each other through the language of cybersecurity. A more complete analysis would include other languages, especially government policy. By including this additional language, future research can perform a more complete comparison of legislative guidelines on the implementation of voting systems at different levels of government.

Conclusion

Through an Actor-Network Theory-focused analysis of the research question, this paper recommends that a three-part solution be implemented to increase the security and reliability of United States elections. First, a secure system would rely on DRE machine technology as a user interface, but tally votes using Optical Ballot Scanning of the paper trail recorded for each machine. Second, centers where machine-marked ballots are collated would make use of

distributed data storage to minimize the risk of large-scale data manipulation. Finally, a dedicated government agency or task force would use a red and blue team to actively detect and efficiently repair vulnerabilities in the voting system. With these three components, the United States would be able to create a more secure and reliable voting system, leading to an increase voter confidence. This would lead to a higher level of engagement in the voting process, which in turn creates a more effective democracy.

Works Cited

Allers, M. A., & Kooreman, P. (2009). More evidence of the effects of voting technology on election outcomes. *Public Choice*, *139*(1), 159–170. https://doi.org/10.1007/s11127-008-9386-7

Card, D., & Moretti, E. (n.d.). DOES VOTING TECHNOLOGY AFFECT ELECTION OUTCOMES? TOUCH- SCREEN VOTING AND THE 2004 PRESIDENTIAL ELECTION. *THE REVIEW OF ECONOMICS AND STATISTICS*, 15.

ContentServer.pdf. (n.d.). Retrieved February 18, 2020, from https://content.ebscohost.com/ContentServer.asp?EbscoContent=dGJyMNLr40Sep7Y4xNvgOLCmsEiep7dSr6y4TLKWxWXS&ContentCustomer=dGJyMPGpsUm0qq5NuePfgeyx847f1d%2BI5wAA&T=P&P=AN&S=R&D=f5h&K=34976626

CSA-WINDOWS-10-CRYPT-LIB-20190114.pdf. (n.d.). National Security Agency. Retrieved February 18, 2020, from https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF

CWE - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (3.4.1). (n.d.). Retrieved February 20, 2020, from https://cwe.mitre.org/data/definitions/119.html

Dill, D. L., & Castro, D. (2008). The U.S. Should Ban Paperless Electronic Voting Machines. *Communications of the ACM*, *51*(10), 29–30. bth.

Dill, D. L., Schneier, B., & Simons, B. (2003). Voting and technology: Who gets to count your vote? *Communications of the ACM*, *46*(8), 29. https://doi.org/10.1145/859670.859692

E. H. Barney Smith, D. Lopresti, & G. Nagy. (2008). Ballot mark detection. *2008 19th International Conference on Pattern Recognition*, 1–4. https://doi.org/10.1109/ICPR.2008.4761549

Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems*, *105*, 13–26. https://doi.org/10.1016/j.future.2019.11.005

Lindley, D. (2008). US election: Ghosts in the machine. *Nature*, *455*(7217), 1171–1174. https://doi.org/10.1038/4551171a

NVD - General. (n.d.). Retrieved February 19, 2020, from https://nvd.nist.gov/general

Oakley, J.G. (2019) *1. Red Teams in Cyberspace - Professional Red Teaming: Conducting Successful Cybersecurity Engagements*. Retrieved February 21, 2020, from https://learning.oreilly.com/library/view/professional-red-teaming/9781484243091/html/469885_1_En_1_Chapter.xhtml

REINAUER, P. (2019). From Hanging Chads to Data Hacks: Maintaining Election Integrity in the Digital Age. *Journal of Business & Technology Law*, *14*(2), 533–551. bth.

Grover, Purva, et al. "Diffusion of Blockchain Technology : Insights From Academic Literature and Social Media Analytics." Journal of Enterprise Information Management, vol. 32, no. 5, 2019, pp. 735 - 757.