TEXAS ELECTION SECURITY: HOW PREPARED ARE COUNTY OFFICIALS TO DEFEND AGAINST CYBER THREATS TO ELECTORAL INFRASTRUCTURE?

by
Elizabeth N Kasongo

A thesis submitted to the Department of Information and Logistics Technology
College of Technology
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in Cybersecurity

Chair of Committee: Chris Bronk, PhD

Committee Member: Matthew Bernhard, PhD

Committee Member: Rakesh Verma, PhD

University of Houston
May 2021

DEDICATION

I dedicate this thesis to my parents, Celestin and Jeannette Kasongo, who have supported me through my life, and educational career. I would also like to dedicate this thesis to all my siblings, especially Ntumba and Patric Kasongo (R.I.P), who began this journey in life since we were children and for inspiring me to keep pushing. Mulumba, Cedric, Tharcis, Benson, Robert, Yvonne, Celestin Jr, Jacob, Grace, and Paulette have been a blessing to me, and I did this for you all.

ACKNOWLEDGMENTS

I would like to thank my family and my friends for the love and support. Thanks to my friends for being there for me since the beginning of my graduate school and supporting me through my highs and lows. My advisor Chris Bronk, Ph.D., for assisting me throughout this process and my educational experience at the University of Houston. Special thanks to my sister from another mother, Sinclair Chapman, for helping me with my thesis and support me. Lastly, I would like to thank Vegedream, whose music encouraged me and motivated me to keep writing.

ABSTRACT

How prepared are county officials to defend against cyber threats to electoral infrastructure? To answer this question, research was conducted in Texas by collecting data on our recent national elections. The study included interviews performed with election officials from three counties in the state of Texas, who are tasked with safeguarding our electoral infrastructure. This thesis explores problems or threats associated with the various voting technologies used to better understand the vulnerabilities that have previously caused election interference from foreign actors. The thesis aims to explore whether county officials in Texas are prepared to secure elections, protect voter information, and defend against cyberattacks or foreign interference. Ultimately, it will offer recommendations on how to defend against future attacks by recommending measures to protect the electoral infrastructure and the American democracy.

TABLE OF CONTENTS

DEDICATION ..... **i**
ACKNOWLEDGMENTS ..... **ii**
ABSTRACT ..... **iii**
TABLE OF CONTENTS ..... **iv**
LIST OF FIGURES ..... **v**
ABBREVIATIONS PAGE ..... **vi**
I. INTRODUCTION **1**
I. EARLY HISTORY OF VOTING SYSTEMS **5**
II. CURRENT VOTING SYSTEMS **9**
Ballot Markinng Devices 10
Direct Recording Electronics 11
Hand-Marked Paper Ballots 13
Optical Scan 16
Hybrid Voting System 18
III. POSSIBLE DISRUPTIONS **21**
IV. THE HUMAN FACTOR **26**
Social Engineering 26
Insider Threat 30
Misinformation (Rumor Control) 30
Ballot Design 32
COVID-19 & Human Behavior 33
V. HIGH-LEVEL POLICIES **35**
Help America Vote Act of 2002 35
SAFE Act 35
For the People Act 36
VI. CASE STUDY: TEXAS **38**
Bexar County 39
Cameron County 44
Harris County 47
VII. FINDINGS **50**
VIII. RECOMMENDATIONS **53**
IX. CONCLUSION **57**
X. WORKS CITED **60**

LIST OF FIGURES

1.1 ExpressVote Universal Voting System.....40

LIST OF TABLES

2.1 Ballot-Marking Devices (BMD). 11
2.2 Direct Recording Electronic (DRE) 13
2.3 Hand-Marked Paper Ballots (HMPB) 15
3.1 Optical Scan System 17
4.1 Hybrid Voting System 19

ABBREVIATIONS PAGE

APT-Advanced Persistent Threat

BMDs-Ballot-Marking Devices and Systems

CARES- Coronavirus Aid, Relief, and Economic Security Act

CISA-Cybersecurity and Infrastructure Security Agency

COVID-19 – Coronavirus

DEI-Digital Election Infrastructure

DHS-Department of Homeland Security

DNC-Democratic National Convention

DoS/DDoS-Denial of Service/Distributed Denial of Service

DRE-Direct Recording Electronic

EAC-Elections Assistance Commission

EIP-Electoral Integrity Project

FBI-Federal Bureau of Investigation

FTP-File Transfer Protocol

HAVA - The Help America Vote Act of 2002

HB-House Bill

IR-Infrared

MIT-Massachusetts Institute of Technology

NAS-National Academy of Sciences

NVRA - The National Voter Registration Act of 1993

SOS-Secretary of State (Texas)

VPN-Virtual Private Network

VRA - The Voting Rights Act of 1965

VVPAT-Voter Verified Paper Audit Trail

INTRODUCTION

Dan S. Wallach, professor of computer science at Rice University in Houston, Texas, provided testimony before the Texas Senate Select Committee on Election Security in February 2018. During his presentation, professor Wallach highlighted vital areas on which the Texas Legislature must focus to protect the elections. Professor Wallach explains that,

> Texas's voting technology is aging. We would not expect a laptop or software program from over a decade ago to be reliable or secure today—but that is exactly what Texas is doing by using aging and in some cases, obsolete voting systems. Texas needs a plan for the orderly and expeditious retiring and replacing of its elections infrastructure.[1]

To better secure elections and reassure the public that their votes are safe, states such as Texas need to implement a law that will require jurisdictions to update their old voting systems. The security of elections, voting technology, and voter information depends on those in charge, and that is where change needs to begin.

As one of the oldest democracies and wealthiest countries globally, the United States of America has been experiencing more problems with elections of late than one might anticipate. The American democracy is under cyber-attack, and malicious actors are doing a great deal to undermine that democracy. Technological advancement increases threats because individuals who wish to compromise the election information have much greater access to it. American elections are a prime example of how nation-states have been interfering with the democratic franchise of citizens. In addition, the internet connectivity of voting infrastructure has increased vulnerability, allowing hackers to affect the outcome of elections. This raises concerns about the security of voting systems, the integrity of the United States' elections, and its effect on national security.

Contrary to the United States, other democracies have implemented centralized, nationwide elections. The U.S. Constitution grants individual states the right to administer and regulate elections as each state sees fit. Today, American elections are administered by various jurisdictions, including the presidential and local elections. Some jurisdictions have fewer voters than others, and elections are "overseen by state and local governments. Many elections offices have few dedicated staff and little access to the latest information technology (IT) training or tools."[2] To enhance voters' right to the democratic franchise, states have introduced various voting methods, including early voting, vote centers, and mail-in voting. Laws such as the Help America Vote Act have also been passed to implement voting systems that will accommodate all voters and cast their ballots without problems. While some states have stayed up to date with new digital voting systems, others have yet to transition, forcing the House of Representatives to pass regulations requiring all states to upgrade their voting systems and implement better security measures. The government passed the Help America Vote Act in October 2002 elections requiring all states to transition from lever machines and punch-card voting systems and implement Direct Recording Electronic voting systems. The new voting systems were implemented to provide a better and safer election because they offered features such as a touch screen and did not use paper ballots. The DRE allowed voters to have a clear view of their options and registered the votes electronically, which was believed to prevent tampering. In contrast, some provided a voter-Verified Paper Audit Trail (VVPAT), making it accessible for all voters.

In August of 2016, Russian attackers targeted the voter registration systems in approximately 21 states before the election[3]. The attack permitted them to gain access to thousands of voters' information. During this time, a group of Russian attackers searched the

voter databases, hacked the Clinton campaign, the Democratic National Committee, and more. They also released damaging information on social media sites intending to influence the voters' decisions. The Federal Bureau of Investigation sent alerts warning about the attack two months before the election when the voter registration databases in Arizona and Illinois were hacked.[4]

The United States Intelligence Community determined later that the motivation behind Russia's involvement in the 2016 elections was to spread a sentiment of distrust in the American democratic process. This attack left many voters with fear and questions regarding the security of voting systems, elections, and personal information. While updating voting systems might be the main objective, the United States needs to ensure that they continue to keep the public trust because lack of confidence can contribute to the insecurities of digital democracy. The human factor is becoming another threat that many did not expect because attackers find human beings the most accessible vulnerability they can exploit. The 2018 midterm elections and 2020 elections introduced misinformation, while the impact of the SARS-CoV-2 pandemic further complicated the 2020 election. States were forced to find new ways to ensure that the presidential election was not interfered with and voters could practice their right to vote. Voting technology was updated, funds distributed, and training provided to jurisdictions. However, how prepared are county officials to defend against cyber threats to electoral infrastructure? This thesis seeks to answer the question by analyzing the past and currently used voting systems across three counties in Texas, studying the potential disruptions to voting systems, understanding the human factor and their contribution to the insecurities of the elections, and examining the various high-level policies implemented to protect the voting machines. To complete these tasks, interviews are conducted with election officials from Bexar, Cameron, and

Harris Counties in Texas with the hope of understanding whether these counties are equipped and prepared to protect the elections, voter information and defend against future attacks.

EARLY HISTORY OF VOTING SYSTEMS

During the nineteenth century, the United States made innovations to voting systems to modernize and reduce the chances of election fraud. Paper ballots were used, and voters had trust in its government that they would "pick up a paper ballot preprinted with the names of candidates for one party and simply drop the form into the ballot box"[5] without believing that there could be an opportunity for fraud. Various voting systems have been used, including the punch card and mechanical lever voting machines. The DRE voting system was initially introduced in the 1970s in Illinois, becoming the first complete electronic voting system; however, its use did not expand until the Help America Vote Act in 2002 passed. The United States now has employed various voting systems that include: Optical Scan Paper Ballot system; Direct Recording Electronics; Ballot Marking Devices; Hybrid Voting Systems; and Hand Marked Paper Ballots.

Voice Voting

During the initial years of voting, Americans could not vote the way that is being practiced today, "instead, those with the right to vote (only white men at the time) went to the local courthouse and publicly cast their vote out loud,"[6] and this was known as "viva voce" or voice voting. For this voting method, voters stood before a judge who would request that the voter swears on a Bible as an authentication method. After pledging affirmation, the voter's name would be called, and they would approach a clerk and state their chosen candidates. This form of voting introduced various vulnerabilities that called for the United States to introduce a new method of voting, paper ballots.

Some of the problems of this type of voting had to do with identifying and authentication methods used. The voters were required to swear on the Bible, claiming that they are who they are and have not previously voted; however, there is no other way of confirming this. Not only did they have the authentication issues, "the most obvious problem with voice voting is that there is no ballot secrecy whatsoever. You're calling out how you want to vote, and everybody you know could be there listening to it."[7] Some of the problems surrounding voice voting also included coercion and the possibility of the election being undermined due to a lack of anonymity in the process.

Initial Paper Ballots

When the first paper ballots were introduced, they "were nothing more than scraps of paper upon which the voter scrawled his candidates' names and dropped them into the ballot box. Newspapers began to print out blank ballots with the titles of each office up for a vote which readers could tear out and fill in with their chosen candidates."[8] One of the problems concerning this form of voting was that "the technology was designed to provide integrity and a form of protection for ballot secrecy. But if the procedures weren't followed quite right or if people trying to violate the security of the election were clever enough, there were many ways in which this could fail [also] with paper ballots created new kinds of opportunities for fraud,"[9] and not much could be done to prevent it.

The Australian Paper Ballot

This form of voting was introduced when reports of voter fraud and calls for reforming elections began. Australia introduced the paper ballot, which was printed by the government and then used by voters to cast their votes. It was then adopted by New York and Massachusetts,

which involved ballots, "printed with the names of all candidates and handed to voters at the polling place."[10] Some of the problems with this voting method included "cost and complexity…violations of integrity and violations of ballot secrecy. There was just almost no end to the cleverness of the people trying to cheat. One place the things can go wrong is with the counting process."[11] While this form of voting was more secure than the initial paper ballot, new vulnerabilities were introduced, forcing the government to implement a new voting system.

Lever Machine

The Lever Voting Machine was invented by Jacob H. Myers, who believed that using a machine would solve the United States' voting problems. The lever machine "came into existence towards the end of the 1800s and was rising to prominence for many years [becoming]…the most widely used voting technology in the US."[12] The lever machines significantly changed voting because voters did not have to write down their choices; instead, the voting system would record them. One of the problems associated with the lever machine was complexity because the machine was designed for voters to select either Democrat or Republican candidates. However, if they were to choose independent candidates, they would have to follow complicated instructions. Another issue is that voters did not have access to a physical record of their votes that they can verify. Using the paper ballot allows one to see their choice and confirm that they marked their options while the lever machines did not allow that.[13]

While election officials viewed the lever machine as one of the systems that can change elections forever, the outcome was not anticipated by those who implemented the system. More problems were associated with using the lever machine due to the various gears and wheels voters had to

press, and the machine was very complex to use for voters causing more problems. The punch-card voting system replaced the lever machine and became the new form of voting.

Punch Cards

During the 1960s, a new method of voting was introduced, punch-card voting. This voting technique involved the voter entering the information and candidate choices by punching holes in a card provided. Like the Lever Machines, the punch card voting did not give the voters a way to verify their selections. One of the punch card voting's main problems was highlighted during the 2000 presidential election when Florida faced a recount for the elections. During the recount process, "election officials had to examine each punch card ballot by hand to determine if hanging or dimpled chads should be counted or thrown out,"[14] causing reports of fraud. Because of the problems found, such as recount difficulties and fraud reports, the United States Congress was forced to allocate funds to states encouraging them to upgrade their voting technology and introduce new voting systems. While the punch cards served their purpose, presenting the latest digital voting systems brought about the end of punch-card voting.

CURRENT VOTING SYSTEMS

While the United States has been making significant progress in ensuring that the electoral infrastructure is updated for each election, some experts believe that more can be done to secure voting machines. Even though these voting technologies continue to evolve, they remain vulnerable to errors and malicious attacks. In 2018, Andrea Cordova McCadney and Lawrence Norden proclaimed that "while significant progress has been made in shoring up this country's electoral infrastructure in recent years, local election officials maintain that much still needs to be done ahead of the 2020 election."[15] The Brennan Center found that despite various warnings regarding historical election interference, the U.S. has not made significant progress in replacing vulnerable and aging voting machines across the country. The lack of urgency to replace and secure these machines increases the chances of cyberattacks within elections. There are different reasons why changes need to be made, and electoral infrastructure needs to be updated,

> First, old systems are more likely to fail and are difficult to maintain. For instance, in the 2018 midterm elections, voting machines across the country began malfunctioning which caused frustration among voters and minimized the opportunity for some to cast ballots.
>
> Secondly, old voting systems are not as secure and do not have the appropriate hardware and software updates. Chris Krebs, the former head of Cybersecurity at the Department of Homeland Security (DHS) warned "the big game we think for the adversaries is probably [the 2020 presidential election]"[16] because of the Russian interference in the 2016 presidential election and the issues faced in the 2018 midterm elections. The National Academy of Sciences (NAS) also suggested that older voting systems need to be "removed from service as soon as possible in order to safeguard the security and integrity of American elections". The older systems do not print the voters' selections which hinders the verification and auditing processes. These elements are key to a successful election. [17]

In 2002, Congress passed the Help America Vote Act (HAVA), which addresses the issues involved with voting systems and provided $380 million to assist in the funding for better

election security. In March 2020, former President Donald J. Trump signed a Coronavirus Aid, Relief, and Economic Security (CARES) Act that included $400 million provided to states in response to the coronavirus pandemic. Many jurisdictions used the CARES Act funds to implement the mail-in ballot votes to prevent voters from being affected by the pandemic. The HAVA was passed to,

> [E]stablish a program to provide funds to States to replace punch-card voting systems, to establish Election Assistance Commission to assist in the administration of Federal elections and to otherwise provide assistance with the administration of certain Federal election laws and programs, to establish minimum election administration standard for States and units of local government with responsibility for the administration of Federal elections, and for other purposes.[18]

Because of this law, improvements to election infrastructure began with the replacements of the level machines and the punch card voting system. According to the Brennan Center, the Election Assistance Commission (EAC) distributed the HAVA funds to bolster election cybersecurity, acquire new voting systems, and improve post-election auditing. Even though funds were provided, they were not enough to replace all the vulnerable voting machines before the 2020 elections. This leaves many questioning whether America will ever be prepared for future elections and what needs to be done to ensure that the American democracy is secured.

Ballot-Marking Devices and Systems (BMDs) were initially presented to accommodate those with disabilities after a federal requirement was passed in 2006 stating that polling locations must provide the means necessary for voters with disabilities to vote independently and privately. However, BMDs are now used by all voters in states such as Philadelphia and Georgia. This type of voting system displays "a digital ballot, allow voters to make selections, then print a paper record of the voters' choices,"[19] making it easy to use. BMDs are one of the most common voting systems[20]; however, some experts would argue that while there are benefits of

implementing this type of voting system, we have to consider the risks of using this system and find ways to protect against cybersecurity threats and attacks. [21]

Table 2.1: Ballot-Marking Devices and Systems (BMDs)

Advantages	**Disadvantages**
Provides accessibility for all voters, including those who have disabilities. For instance, BMDs offer various languages, including voice or text, and help non-native English-speaking voters.	Vulnerable to hacks, programming errors, and misconfiguration. "a fundamental challenge we face in any BMD implementation is trying to combine the security properties of hand-marked paper ballots with the usability and operational benefits of a BMD."[22]
Ensures that voters check and confirm their final selections and provide a confirmation screen at the end of the session. Even though some voters ignore review screens, this voting system does provide them with the opportunity to review their selections before casting their ballots.	It does not offer enough inspection options because evidence shows that voters are not likely to find errors in their computerized ballot summary screen, which could record votes inaccurately if misconfigured or hacked. Thus, the voter might not catch the error.[23]
	They can become costly with maintenance, the need for additional storage, and if they need to be replaced if

Direct Recording Electronic is also known as DRE, is a voting system that allows for a ballot to be presented electronically. The voters can use touch screen features on some of the DREs to

navigate the process and cast their votes. According to the Verified Voting organization, Direct Recording Electronic (DRE) voting systems use,

> Three user interfaces (pushbutton, touchscreen, or dial) allow voters to record their selections into computer memory directly. The voter's choices are stored in DREs via a memory cartridge, diskette, or smart card and added to all other voters' choices. An alphabetic keyboard is typically provided with the entry device to allow for the possibility of write-in votes, though with older models, this is still done manually. Some DREs can be equipped with Voter Verified Paper Audit Trail (VVPAT) printers that allow the voter to confirm their selections on an independent paper record before recording their votes into computer memory. This paper record is preserved and, depending on State election codes, made available in an audit or recount event.[24]

DREs are used or have been used in many states across the United States. While this voting equipment is seen to be helpful when it comes to accommodating voters, it has its advantages and disadvantages.

Table 2.2: **Direct Recording Electronic**

Advantages:	**Disadvantages:**
Accessible to all voters, including those with disabilities.	Susceptibility of votes being tampered with due to the electronic platform.
Capable of showing texts in multiple languages to ensure that all voters can participate.	Vulnerability of the results due to the ability to alter or destroy votes with access to the memory card.
	It does not provide a verifiable record of the ballot; therefore, voters do not see the actual ballot, but "rather a representation of it on the face of the machine."[25]
	This type of voting system is known as one of the "most vulnerable parts of [the] American election infrastructure."[26]
	Difficult to detect errors and a high risk of tampering or fraud in elections.

Hand-Marked Paper Ballots are also standard among some states such as Arizona, New Hampshire, and Wisconsin, requiring that their voters use hand-marked ballots instead of electronic voting systems. This method requires voters to hand mark their ballot selections and then use an electronic scanner to scan and cast their votes. For states such as Arizona, no electronic voting system is used to either vote or scan their ballots. While some states prefer a hand-marked paper ballot, some find it more valuable and secure to use it along with BMDs or

DRE with VVPAT for accessibility. According to Dan S. Wallach, a professor in the Computer Science Department at Rice University,

> Legislators must recognize that paper ballots are the means to a much more important end: ensuring the final results are correct, even when sophisticated adversaries try to interfere. This requires implementing "risk-limiting" post-election audits, where auditors randomly sample paper ballots to make sure they match up with the digital records. Discussion about "paper trails" and "voter-verified paper audit trails" can seem complicated. Unfortunately, not all paper trails are created equal. When it comes to elections, "paper" can mean three things: paper ballots filled out ("marked") by hand, paper ballots marked by a machine (a "ballot-marking device"), or a paper receipt of some kind printed by an electronic voting machine.[27]

And it will be up to states to determine which type of paper ballot works for them. Wallach's suggestion is to ensure that hand-marked paper ballots should be human-readable and auditable by humans. With this form of the voting system, "voters must be able to detect errors on machine-marked paper ballots and have the opportunity to correct them, as they can with the hand-marked ballot,"[28] and this would be a step towards a much more secure election. There has been confusion around the use of hand-marked paper ballots since the 2000 election. Its aftermath inspired Congress to pass a law that included $3.9 billion to assist election precincts across the country replace old systems with new technology.

Table 2.3: Hand-Marked Paper Ballots

Advantages:	Disadvantages:
The Brennan Center describes paper ballots by stating, "Paper ballots create tangible, tamper-evident and auditable records of how each voter voted."[29]	Post-election auditing problems will be presented because of human error. Conducting manual auditing of the election can differ with accuracy and effectiveness because auditors or outside observers might argue against the validity of the audit. Although many say against using the computerized ballot because of the possible insecurities, "we must be careful to remember that even the most basic tasks performed by humans can and do introduce error into the process."[30]
Paper ballots typically have good usability because they are not as prone to error as electronic voting systems. In addition, many individuals deal with paper for thousands of years; therefore, "with paper, there are fewer opportunities for failures due to unclear instructions, indirect mappings between actions and candidates, inappropriate configuration."[31]	Tedious and lengthy counting process. In addition, states such as Michigan have laws that prohibit the opening of the ballots until election day, while Colorado allows for the ballots to be opened on the day that they are received. Therefore, it will take Michigan longer to verify their votes while Colorado will not face a similar challenge.

Fastest method because voting should take a reasonable amount of time, and voters should not spend their days in long lines waiting for the available machines. Paper ballots make voting efficient, and "when the efficiency of a system is inadequate, lines at the polls can quickly reach unreasonable lengths,"[32] causing some individuals to leave without casting their votes.	It does not meet the accessibility requirements enforced by the Help America Vote Act (HAVA). Therefore, voters with disabilities might face challenges with this voting method.
	It is significantly difficult to make changes because voters will request a new ballot to make changes. It may be harder for voters who participate in the vote-by-mail elections.
	It can become costly because paying individuals to count the ballots will cost more than the one-time expenditure of purchasing a machine.

The Optical Scan System is used to scan devices that scan paper ballots. With this form of the voting system, voters mark their ballots either scanned at the precinct or taken to a central scan location to be counted. Older versions of the optical scan systems used infrared (IR) technologies to scan ballots with timing marks on the edges. The new version of the optical scan uses digital scanning technology to scan each ballot collected during the voting process. The optical scan system,

> [I]ncludes both mark sense and digital image scanners in which voters mark paper ballots that are subsequently tabulated by scanning devices. On most optical scan ballots voters indicate their selections by filling in an oval, completing an arrow, or filling in a box. Ballots may be either scanned on hand-fed optical scan tabulators in the polling place or vote center (Precinct Count) or collected in a ballot box to be scanned at a central location (Central Count.) High-capacity batch-fed optical scan tabulators are used in some jurisdictions to handle larger volumes of central count ballots. Optical scan voting systems can scan, and tabulate ballots marked by hand or those marked by a ballot marking device…[33]

This type of voting system was first introduced in the 1960s and has been used in various jurisdictions.

Table 3.1: The Optical Scan System

Advantages:	**Disadvantages:**
Timely count of the votes due to the Central Count Scanner. They are typically used at locations that receive a bulk amount of absentee or mail-in ballots.	Lack of opportunity to fix voting errors with the central count scanners.
Opportunity to fix voting errors with the use of precinct scanners.	While central count scanners can have advantages, transporting votes to a central location can delay the election.[34]
It is known to be the "robust and secure election technology that is widely used with risk-limiting audits based on a robust, well-maintained, physical audit trail."[35]	Optical scanners are not equally accessible to all voters.

A **Hybrid Voting Systems** is a touchscreen voting machine that provides voters with a paper copy of their selection, giving them the ability to verify their choice before submitting their ballot. Currently, available hybrid systems include the Election Systems & Software ExpressVote and ExpressVote XL, Image Cast Evolution, and Hart InterCivic Verity hybrid voting solution. Texas has certified two hybrid systems: the Hart InterCivic Inc. and Election Systems & Software. The Election Systems & Software ExpressVote hybrid voting system "uses touch-screen technology that produces a paper record for tabulation…, handles the entire marking process, eliminating unclear marks and the need for interpretation of the voter's mark."[36] While some jurisdictions favor this new form of voting system, implementing these systems has advantages and disadvantages.

Table 4.1: Hybrid Voting Systems

Advantages:	Disadvantages:
Accessible for voters across the country. It does meet the requirements for voters with disabilities as well.	Vulnerable to cyber-attacks that can impact the election.
Provides a paper trail for voters to be able to verify their selections.	Potential for fraud because these systems can "AutoCast," meaning that the voter can cast their vote without checking for their selections.
Is available at all locations and to all voters.	Even with the paper trail, voters might not pay enough attention or decide to continue without reviewing.
	The Verity voting system has access to scanning barcode capabilities, which can be dangerous since those barcodes can be programmed to change votes.
	While touchscreen devices might be suitable for usability, they might be susceptible to denial-of-service attacks or malware can be installed.

While America has implemented various forms of voting systems, the question remains of which method will efficiently and effectively protect the American democracy. Experts state that America is headed to a time to implement voting systems that combine automation and traditional paper ballots. Charles Stewart, the MIT Election Lab director, advises that "So I can imagine that in 2024 we would no longer be seeing paperless DREs...You need paper to conduct post-election audits. Several states are moving in that direction. Colorado was a real pioneer, and other states will be moving that way."[37] There will be a time when states and counties will begin leaning towards the hybrid voting system, such as DREs with VVPAT and paper ballots. In March 2020, Lucas Ropek, a writer for govtech, wrote that "only six states now have communities that deploy DREs without VVPAT, while a majority deploy a combination of paper ballots and DREs with VVPATs,"[38] and this might change by the next election. Experts express hope that these states will transition to the system that a majority of states are using.

POSSIBLE DISRUPTIONS TO ELECTRONIC VOTING SYSTEMS

Electronic voting systems are also vulnerable to cyberattacks or potential disruption and need to be well secured to avoid being hacked. Attackers can exploit these vulnerabilities to damage or tamper with elections, including vote counts at voting precincts. Election officials need to study and understand the potential disruption to electoral infrastructure and establish the necessary measures to prepare for attacks. Some of the possible attacks include Advanced Persistent Threats, Denial-of-Service, Malware, and more.

Advanced Persistent Threats

Advanced Persistent Threats (APT) is a group that is supported and directed by nation-states to cause disruptions to others. Like many other cybercriminals, APT groups steal information, interrupt operations, and/or destroy infrastructure worldwide. They tend to "pursue their objectives over months or years…they adapt to cyber defenses and frequently retarget the same victim."[39] In October 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) began warning individuals and officials of possible attacks from Iranian APT actors who would attempt to influence and interfere with the presidential elections. To disrupt the 2020 presidential election, the APT actors started creating fictitious websites and practiced domain spoofing[40]. With the obtained information, they disseminated voter registration information and provided misinformation about voter fraud, ballot fraud, and more. According to CISA and FBI, "[the] APT actors have historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks,

structured query language (SQL) injections attacks, spear-phishing campaigns, website defacements, and disinformation campaigns."[41]

APT actors are the most dangerous cybersecurity attack groups because they are the most experienced, advanced, and financially secure. Because nation-states sponsor them, they have the resources to carry out undetectable attacks. They are typically motivated by political or economic gain because they target vital businesses, government entities, and more. Some APT groups turn to espionage routes such as human information, social engineering, etc., to gain access. Once they enter the systems, networks, or structures, they remain there until they obtain the needed information.

Denial-of-service (DoS) Attack

A Denial-of-service (DoS) Attack prevents a computer system from functioning correctly or normally. It tends to disrupt or slow down access to computers or networks. A DoS Attack "can exploit a known vulnerability in a specific application or operating system, or it can attack features (or weaknesses) in specific protocols or services."[42] Attackers attempt a DoS intending to crash electronic systems by taking the approach offline or sending multiple requests to overwhelm the machines. With a DoS, attackers use a single system to conduct the attacks. However, when the attacks come from many different devices, this becomes a distributed denial-of-service attack.

DoS can be used with electronic voting systems to prevent voters from casting their votes, disrupt vote counting or election auditing by stopping officials from accessing e-poll books, voting systems, or auditing systems. If this type of attack is launched against jurisdictions, its disruption can lead to civilians losing confidence in the elections' integrity altogether. When

targeting select locations or systems, DoS can alter the election outcome as well. If voting systems are taken offline, this will disrupt elections, and voters will not participate in one of the most important roles they were assigned as citizens of the nation.

Malware Attack

Malware, also known as malicious code, is software designed by attackers for some malicious intent. Malware "can be designed to cause damage to a system, such as by deleting all files, or it can be designed to create a backdoor in the system to grant access to unauthorized individuals."[43] It includes Trojan horses, ransomware, spyware, worms, and viruses. Malware is known to be one of the biggest dangers to electronic voting because it can be used to damage voting systems. It can be launched at any point during the process of a vote, beginning with the software used to cast ballots and end with the software used to record and tabulate votes.

This dangerous attack is installed so that the system's authorized users may not be aware of it. Malware attacks are also known to,

> [P]revent voting by compromising or disrupting e-poll books or by disabling vote-casting systems. It can prevent correct tallying by altering or destroying electronic records or by causing the software to miscount electronic ballots or physical ballots (e.g., in instances where optical scanners are used in the vote tabulation process). Malware can also be used to disrupt auditing software[44]

Individuals cannot easily detect malware because it can be installed on the systems when software updates are performed. It can be installed through removable media such as ballot definition files and by exploiting software code errors in the network systems. This attack can also be deployed through physical access by accessing locations that do not have maximum security.

In his course Security Digital Democracy, J. Alex Halderman, a professor of computer science and engineering at the University of Michigan, summoned individuals to,

> [T]hink of malware in the context of voting…there are a few problems with voting online if you have malware on your computer…one problem is that if this malware is stealing personal information, some of the information it could steal might be, say, your username and password for logging in and voting. That could then be used by scammers somewhere else to cast a vote on your behalf or to change your vote if the internet voting system allows that.[45]

Social Engineering (SE)

Cybercriminals tend to advance their skills for every opportunity by finding new ways to gain unauthorized access to information, networks, or systems. They have attempted different attack methods such as DoS, DDoS, and malware to successfully obtain the information or achieve their goals. One of the most dangerous attacks they have turned to is social engineering (SE), which Webroot defines as "the art of manipulating people, so they give up confidential information."[46] SE is the type of attack that requires social skills to acquire or compromise information about an entity or its computer networks. To obtain such information, attackers pretend to be someone that the individual trusts, typically a contractor or IT Specialist.

One of the most common types of social engineering is phishing, where attackers use email or malicious websites to solicit personal information by pretending to be trustworthy organizations or individuals. Phishing is the most dangerous cyber threat because it influences peoples' decisions while forcing them to disclose sensitive information. During the 2020 presidential elections, FBI and CISA warned voters of "Cybercriminals and malicious foreign actors [who] are leveraging spoofed domains and email accounts to disseminate false information; gather valid usernames, passwords, and email addresses; collect personally

identifiable information; and spread malware, leading to further compromises and potential financial losses."[47] The emails discourage voters from casting votes for one particular candidate, and they were threatened if they did not follow the instructions. In this instance, attackers used intimidation and authority to influence the voters into choosing one candidate over the other.

Concerning electronic voting systems, attackers "may obtain sensitive information such as usernames or passwords by pretending to be a trustworthy entity in an electronic communication…individuals with site access (e.g., employees or contractors) might physically access a system"[48] to compromise the election. For instance, if election workers or voting system specialists are not well trained, they may provide sensitive information to an attacker who pretends to be their co-worker or IT assistant who needs access to the voting systems. If the information is provided to the attacker, they would gain access to the electronic voting systems and make any changes.

THE HUMAN FACTOR

Wm. Arthur Conklin, Ph.D., a professor at the University of Houston in the College of Technology, once proclaimed that the greatest threat to information or cybersecurity is the user, us, the people. Humans are becoming one of the most significant vulnerabilities when it comes to cybersecurity and protecting sensitive data. One of the reasons is that humans find it easy to trust, leading to authorizing attackers to access sensitive data. It is essential to explore why humans are the leading factor to the cyberattacks against elections and the strongest vulnerability to information security. Cybercriminals target humans because they are quick to trust and do not question the motives behind peoples' actions. Instead of targeting computer systems, networks, and infrastructures, cybercriminals are shifting their focus on individuals, "their roles within an organization, the data to which they had access, and their likelihood to 'click here"[49] as a way to gain unauthorized access to information. Cybercriminals and their supporters have found that humans will be the most successful path to access organizations and commit cyber fraud or theft after trying various attacking methods. According to the 2020 Verizon Data Breach Investigation Report, social engineering attacks such as phishing remain at the top of data breaches. The report shows that during phishing attacks, "Over 80% of breaches within Hacking involve Brute force or the use of lost or stolen credentials."[50]

Social Engineering

The previous pages discuss the concept of social engineering (SE) and how it works concerning cybersecurity, and the impact on elections and electoral infrastructure. Historically, this attacking method took place either face-to-face or through a phone call. However, SE is now also practiced through emails, social media, and other online platforms. The various forms of

social engineering include Phishing, Vishing, Impersonation, Tailgating, Dumpster diving, Baiting, Shoulder surfing, and now Smishing.

Phishing: phishing is recognized as one of the most successful forms of social engineering, which has caused damage in many of the data breaches experienced. With this method, the attacker sends an email to the user in an attempt to "entice unwary recipients to click on a deceptive link, giving hackers access to their information or a network."[51] The email typically includes familiar images, links, or sent from a spoofed email address that the user can recognize and trust.

Typical phishing contains the following, "We have noticed suspicious activity on your account. To protect your privacy, we will suspend your account unless you are able to log in and validate your credentials. Click here to change your password and prevent it from being locked out."[52] Due to the email's urgency, individuals are not provided with the time to verify the email or the sender and would perform the actions requested by the email.

Vishing: In one day, individuals receive multiple phone calls from different phone numbers about their social security numbers, credit cards, car extended warranty, and more. Attackers use phone systems to trick users into providing their information and personal information. One of the most popular vishing ploys comes from an organization claiming to be "credit services," which lower one's credit card rates. These calls come from phone numbers similar to the users or containing an identical first six digits.

Impersonation: Type of social engineering where the attacker is posing as someone else to convince an authorized individual to provide them with sensitive information. In this instance,

the attacker would pretend to be an IT specialist or a repair technician who needs access to passwords or a server room.

Tailgating: SE practice where an unauthorized individual follows behind another person with credentials to access a location. For instance, an attacker can track an employee while entering their office building or sensitive room, making themselves look like they work at a particular site. While employees may find opening the door for others convenient and a courtesy, it is believed to be a dangerous practice; therefore, cybersecurity experts would encourage employees to authenticate themselves and access their credentials. Implementing security guards or mantraps is a great way to solve this problem.

Dumpster diving: While throwing away paper in the trash or recycling might be healthy for our environment, it can also be dangerous to cybersecurity if not done correctly. Dumpster divers live with a mission of searching through trash bins and recycling containers to obtain documents that individuals discard. They operate intending to potentially find valuable information such as names, phone numbers, and essential individuals in organizations. Smaller opportunities would include finding envelopes with pre-approved credit cards to sign up on behalf of the person. Instead of throwing away documents, the best way to prevent dumpster diving is by shredding documents.

Shoulder surfing: this is one of the "common attacks against password or PIN entry"[53] for locations that do not practice strong security tactics. With shoulder surfing, attackers can look over one's shoulder to obtain the information that they need. The goal is to gain unauthorized entry to intelligence by observing the individual and typically takes place in office environments. The types of information obtained through shoulder surfing include username and password, PIN

for cards, etc. Screen filters and repositioning of monitors is a recommended solution for shoulder surfing.

Smishing: Cybercriminals use the new form of attack called Smishing to try and obtain information from individuals. Now that technology is expanding, and many individuals rely on mobile phones, attackers also shift their attention to stealing data. Smishing is a form of attack where the attacker sends SMS or text messages containing links, webpages, email addresses, or phone numbers to users.

During the 2016 elections, there was an attack at the Democratic National Committee (DNC) which led to a compromise of critical information that many say could have influenced the election results. An FBI Special Agent warned that hackers had compromised a "computer system belonging to the D.N.C. Federal Investigators had named these hackers "the Dukes," a cyberespionage team linked to the Russian government." [54]The attackers sent a phishing email to Hillary Clinton's campaign chairman, John Podesta, who was masked to imitate Google, informing him that a user attempted to access his account. The email that he received contained a link with a website where Podesta could change his password. He decided to forward the email to one of the campaign help desk assistants to verify its legitimacy. According to CNN, "The [help desk] staffer replies with a typo – instead of typing 'this is an illegitimate email,' the staffer types 'This is a legitimate email'"[55] granting Podesta a confirmation to proceed with changing his password and allowing the attackers access to his emails which was then used to gain access to many other email addresses and contact information. This shows how miscommunication among individuals caused one of the biggest election security concerns. Because of this attack,

officials will continue to worry about attacks on elections and how this can be prevented or contained.

Insider Threat

When we think about cyber threats and attacks, we often think about outsiders or anonymous cybercriminals who sit behind their computers miles away thinking about ways or individuals to target. With humans being one of the biggest threats to information and infrastructure security, it is not difficult to imagine that those among us every day can also be the biggest threat. Former and current employees who have access to the most valuable information about companies or networks and systems are also likely to commit or assist with cybercrimes.

"An insider threat occurs when a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data, intentionally misuses that access in a manner to commit a cybercrime."[56]

Election security has been one of the most discussed topics, and officials have been trying to find ways to defend against attacks on electoral infrastructure. However, many are focused on outsiders, which causes them to neglect one of the most dangerous threats, insider threats. Some of these individuals can include election day workers, election judges, board members, County technicians, and other personnel involved in securing the elections.

Misinformation (Rumor Control)

The 2016 Russian interference in the American election has left many voters posing questions such as "how secure is my vote?", "How secure is my voter information?" and "will my vote be counted?" These are examples of questions voters are struggling with and are

constantly trying to understand whether their votes will be hacked. While tampering with votes has been one of the most critical threats to elections, misinformation is now something that officials need to worry about based on the recent 2020 elections. At the federal and state level, the American government needs to assure its citizens that voting systems and their votes are secure and not manipulated. They have to ensure that this is the case because "While Americans may not always agree on politics, we can all agree that election security must be a national priority moving forward to protect each of us and the democratic process we all hold dear."[57]

To warn and educate voters about misinformation related to election security, the Department of Homeland Security's Cybersecurity Infrastructure Security Agency created a rumor control report where voters can learn to distinguish between rumors and the reality of information read online. Misinformation can weaken the public trust in the election process and democracy, causing a more significant threat to the elections. The Rumor Control is,

> [D]esigned to debunk common misinformation and disinformation narratives and themes that relate broadly to the security of election infrastructure and related processes…this resource addresses election security rumors by describing common and generally applicable protective processes, security measures, and legal requirements designed to protect against or detect large-scale security issues related to election infrastructure and processes.[58]

Misinformation on elections and electoral infrastructure can be one of the biggest threats because attackers use it to manipulate individuals and persuade their voting decisions. While we might be concerned about the security of voting machines, we also need to be concerned about the influence of misinformation on voters. An interview was conducted with Bernhard, a Research Engineer at VotingWorks. When asked about the most prominent concern regarding elections and election security, Bernhard responded by stating,

> What are we supposed to do when the election is not convincing to people? How can we change that? This topic is fairly new, and I am worried that the field will go dormant again. The problems we thought we were fixing are not the problems that we are worrying about now—a lot of misinformation and angry people. The community is tearing itself apart; stakeholders have fallen prey to misinformation and have joined that route as well. We need to fix this.[59]

Not only should we worry about securing electoral infrastructure, but we also need to begin worrying about how misinformation can also be a threat to our democracy. We need to discover and understand how to prevent such a threat from potentially impacting our elections' security and the voting systems we use.

Ballot Design

When voters receive their ballots, they are also provided with instructions to assist them throughout the process. However, the question remains, how many of these voters read the instructions? Are the ballots helpful or confusing for voters? These are among the few questions that one can ask regarding voting systems or methods used. After discussing the various voting machines or systems used around the country, we need to discuss the ballots' design and the layouts provided while also attempting to understand if they help voters. How the ballot is designed and how the computer is set up can impact the way individuals vote. If there are little or too many instructions, voters are more likely to be confused. According to the Center for Civic Design,

> A ballot is a form that represents perhaps the most important interaction between a government and its citizens. Thousands of votes are lost in elections every year because of poorly designed ballots. And yet, avoiding these design issues is not difficult or expensive.[60]

Some of their suggestions for better ballots include: using lowercase letters instead of capital letters, avoiding centered texts, aligning the text on one side (preferably on the left), increasing

the font size to ensure that everyone can read the information, using clear and simple language, including illustrations of the instructions, using icons for information instead of including the political party emblems, highlighting the most important information and leaving out the unnecessary information.[61]

COVID-19 and Human Behavior

The 2020 presidential election was a record-breaking election due to the number of voters that decided to cast their votes and participate in democracy. This election took place during the ongoing COVID-19 pandemic, which was supposed to impact voting; however, it did just the opposite. Voting officials around the United States were forced to begin implementing voting techniques that can provide protection both for voters and workers. Not only did they worry about protecting the electoral infrastructure from potential attacks, but they also had to worry about whether individuals will be able to practice their right to vote without contracting the virus. Even though some voters experienced phishing attempts from attackers, everyone was alerted about these incidents allowing for better preparations.

According to statistics collected, over 40% of voters voted by mail during the 2020 elections, caused by the pandemic and the people's willingness to impact. This natural disaster was unexpected, and the government needs to plan on improving election security and establishing ways to prepare for natural disasters. Due to the concerns that were reported in the 2020 election about ballot security and the COVID-19 pandemic, the government would need "to upgrade existing voting sites to improve cybersecurity and create new "pop-up" sites (locations not typically used for voting) to help ensure social distancing"[62] as well as implement voting systems that would allow for voters to be able to participate during natural disasters safely. To

better prepare, the government needs to modernize electoral infrastructure and address “the challenges of election security and voting in the midst of a global pandemic”[63] through HAVA and The Coronavirus Aid, Relief, and Economic Security Act (CARES).

HIGH-LEVEL POLICIES

Help America Vote Act of 2002

Because States were using punch cards and lever voting machines, the government saw the potential of this becoming a problem; therefore, they decided to pass the Help America Vote Act (HAVA) of 2002. This act is one of the most relevant voting security policies. It was presented due to the controversies surrounding the 2000 Presidential Election. One of the HAVA sections highlights the framework that advises states to implement a centralized and digital voting system. This Act was passed to mandate changes to every part of the administration of elections and voting systems. H.R. 3295 section of this law highlights the primary purposes, which include,

> To establish a program to provide funds to States to replace punch-card voting systems, to establish the Election Assistance Commission to assist in the administration of Federal elections and to otherwise provide assistance with the administration of certain Federal election laws and programs, to establish minimum election administration standards for States and units of local government with responsibility for the administration of Federal elections, and for other purposes.[64]

The United States Congress approved The Help America Vote Act to better voting systems and enforced reforms for improving the voting process as a whole. This was one of Congress's first attempts to enhance voting equipment to better secure the digital infrastructure and elections. Not only were funds provided to states for updating equipment, but the Election Assistance Commission was also created and tasked with testing and certifying the voting equipment while communicating with jurisdictions to ensure election security.

SAFE Act

The problems we face regarding election security can be divided into internal and external threats and vulnerabilities. An example of an external threat includes the 2016 elections

when Russian actors attempted to exploit a vulnerability and gain access to voter registration systems causing a significant cybersecurity breach. Even though interference or manipulation of elections was not confirmed, those actors could influence the election. After this incident, many became concerned about the future of elections and the possibility of others using a similar structure to interfere with elections. The internal vulnerability that individuals were concerned about includes outdated voting systems, uneducated voting staff, and more.

The Securing America's Federal Elections (SAFE) Act was initially introduced in 2017 due to the events in 2016. This act was modified various times to meet the standard and restrain from violating the rights of states. The bill's purpose was "[to] protect elections for public office by providing financial support and enhanced security for the infrastructure used to carry out such elections, and for other purposes."[65] The SAFE Act was passed in 2019 in the House of Representatives (House) to protect American elections by,

> [P]roviding funding for states to replace outdated and vulnerable voting equipment, mandate paper ballot voting systems, risk-limiting post-election audits and contains strict cybersecurity requirements for election technology vendors and voting systems.[66]

This law also ensures that local and state officials have the necessary resources to replace the older voting systems with machines that provide a voter-verified paper audit trail ballot system. It also provides grants to hire IT Specialists, provide cybersecurity training, conduct risk assessments, and other essential needs to secure the electoral infrastructure properly.

The For the People Act

Another policy passed in the House in 2019 is the For the People Act, which House Democratic introduced to improve the current federal standards regarding voting. According to the Brennan Center for Justice, the law would be "making it easier for voters to cast a ballot and

harder for lawmakers to gerrymander, by transforming how campaigns are funded to amplify voices of ordinary Americans, and by bolstering elections security and government ethics.[67]"

The For the People Act aims to improve access by requiring that voter registration systems be updated, canceling the limited hours, and other barriers. This law establishes automatic voter registration across the nation while ensuring that those with felonies have their rights restored. It also increases voting by mail and early voting with a focus on modernizing the voting systems. Another goal is to ensure security-enhancing federal support for secure electoral infrastructure, recommend using paper ballots or systems with the voter-verified paper ballot, and enforcing election vendors to be federally certified vendors with certified voting equipment.

Both the SAFE Act and the For the People Act call for election officials to implement user-friendly voting systems while also providing voters methods to verify their votes. According to 2018 records, 85% of the public called for electronic voting systems that print a ballot's paper backup.[68]

CASE STUDY: THE STATE OF TEXAS

Texas is a state in the southern region of the United States and among one of the largest states with a population of approximately 29,145,505 based on 2020 estimates.[69] The capital city is Austin and is governed by Republican Greg Abbott. Known as the "Lone Star State," Texas is represented in the Senate by Republicans John Cornyn and Ted Cruz. Texas has approximately 16,955,519 registered voters as of November 2020 and 8,745 precincts as of November 2018.[70] It consists of 254 counties, with Ruth R. Highs as its Secretary of State and Keith Ingram as the Director of Elections. The Lone Star State praises itself as having the "security of our elections [being the]top priority for the State of Texas."[71]

According to VerifiedVoting, 12.5% of registered voters are living in jurisdictions using Hand Marked Paper Ballots for most voters, 67.1% of registered voters are living in jurisdictions using Ballot Marking Devices for all voters, and 20.4% are living in jurisdictions using Direct Recording Electronic (DRE) systems for all voters.[72]

Texas Cybersecurity Act

After the 2016 elections, many institutions and states began thinking about enforcing cybersecurity and protecting elections everywhere. In 2017, Texas passed a law, House Bill (HB) 8-Texas Cybersecurity Act which "provides specific measures to protect sensitive and confidential data and maintain cyberattack readiness" while the House Bill (HB) 9, the Texas Cybercrime Act "updates the Texas Penal Code to recognize several new types of cybercrime and their punishments."[73] These laws were passed to combat cybercrime and expand officials' roles to protect essential data that they are responsible for. Texas demonstrated its interest in

fighting against cyberattacks by holding security officials accountable and teaching everyone the importance of cybersecurity in expanding technology use.

I chose to conduct a case study on three counties in the State of Texas with the hope of collecting lessons learned from our recent national elections, understanding problems or threats associated with the types of voting equipment currently used in these jurisdictions, and exploring the allocation of resources to secure the electoral infrastructure. To collect lessons learned from our recent national elections, I decided to canvass officials who safeguard our electoral infrastructure. I interviewed officials from Bexar, Cameron, and Harris counties (who chose to remain anonymous) with the hope of understanding how secure their voting systems are and whether they have the necessary resources to provide the best security for the voting machines.

Bexar County

With San Antonio as the county seat, Bexar County is the fourth most populated county in Texas and the most populated in the United States. This county's election department is led by Elections Administrator Jacquelyn F. Callanen, a non-partisan candidate appointed by the election commission, including county judge, clerk, and more. Like other counties, "The Bexar County Elections Department is responsible for voter registration activities and election operations throughout Bexar County. This includes 712 voting precincts, 53 political subdivisions, 20 Independent School Districts, 29 Cities, 3 Military Installations (including Lackland AFB, Fort Sam Houston, and Randolph Air Force Base), and over 1,181,842 registered voters."[74]

I interviewed a Bexar County official who answered questions regarding election security and voting systems used in the County. During my interview with the County official, I was able

to ask questions about the voting processes and procedures. The state mandates EAC certification, where the EAC conducts the testing and certification of the voting machines. I was also informed that the State of Texas requires its certificate, and, in this process, Bexar County elections officials would invite companies to come and test the voting equipment.

When thinking about election security, we need to start thinking about the voting systems, which hold the destiny of elections in the United States. Before 2016, many counties around the country used aged voting systems such as lever machines and DREs. For 17 years, Bexar County used Direct-Recording Electronic (DRE) as its voting system and did not plan on adopting a new one for as long as they did not experience any problems. In November 2019, Bexar County finally decided to upgrade its voting system to what they now call blended or hybrid, similar to DRE with VVPAT. This new voting system combines optical scanners, ballot marking devices, or DREs to complete the process. The new system is called ExpressVote, which is a paper-based ExpressVote Universal Voting System that "uses touch-screen technology that produces a paper record for tabulation. As a marker, the ExpressVote handles the entire marking process, eliminating unclear marks and the need for interpretations of the voter's mark [some of the security features include] physical and system access controls, verifiable paper record, audit logs, proprietary flash drives, system application controls, encryption, hash validation, and digital signatures."[75]

Figure 1.1 **ExpressVote Universal Voting System**

76

This County's preparing process differs from the other counties because Bexar County services the three military bases. The elections administrator would meet once a week with the staff to brief all the critical functions that need to be completed before elections. Their preparation period begins six months before the election, when equipment testing, and voter registration systems are initially inspected. Forty-five days before the election, they have to follow federal mandates, which require the County elections department to send all the military ballots to the bases, including around the globe. Failure to do such on time would result in the County covering the ballots' delivery and returning costs.

After the events surrounding the 2016 elections, many election officials were determined to make changes before the 2020 national election. For Bexar County, everything went according to plan except for two events that impacted the elections worldwide. Something different for

officials at Bexar County was the COVID-19 pandemic and misinformation. Even with all this, one official was very proud of their team and proclaimed,

> I am unbelievably proud of my team and how well we worked in November…CISA made us essential workers which means that we spent over 90 hours in the office together…[we witnessed] the most voters, mail-in ballots, the governor extended early voting which helped. The County paid for all election officials to test for COVID-19…spent about half-million dollars to ensure everyone is protected.[77]

The official alleges that in 2016, the Texas Secretary of State's (SOS) system was hacked, which Texas admitted. However, the then-Secretary of State denied that the state was a victim of the Russian hacks asking the DHS to make corrections of the list they published. However, this did not stop Bexar County from making changes to its systems. Since then, they have written protocols to protect them if another situation arises with the SOS system getting hacked. They have backup plans for such cases and want to ensure that nothing disrupts elections. For this official, 2016 taught them a lesson which they reassure by stating,

> "Should something happen, we will still be able to get election results. Before 2016, we never thought of this. The climate [has] changed a little bit [it has changed a lot actually]…the one thing we have learned from 2016, we go and work very closely with the emergency operations center. Work hand-in-hand with them and see if we can remediate anything from the back-end."[78]

Even after following the proper measures of protecting the electoral infrastructure, Bexar County experienced an unexpected problem during the 2020 national elections that left voters confused and contributed to misinformation spreading across the jurisdiction. With the new blended or hybrid system, the voter must put the ballot in the tabulator; however, no one was aware that those boxes could only hold 2000 ballots. Election workers at the precincts were under the assumption that the tabulator was jammed when they could not push through ballots which caused the County to have to switch the boxes after every 2000 votes. Voters began thinking that

the tabulators were not working, and misinformation circulated the County, and voters started walking away to return to their homes. The official explained that "everybody focused on hardware and software. No one informed us of the number of ballots held by the tabulator. The solution was to change the tabulators causing problems with…misinformation spreading."[79] The County's election administrator was forced to bring extra technical experts from other departments to change the tabulators because the office only had five information technology specialists with 45 sites. The official did this to avoid breaching of votes and stated that this would be the method that will be used moving forward. The Bexar County official acknowledged that early voting helped their County tremendously because most voters did not have to go to some centers, which helped with the ballots' size and allowed some locations not to change their tabulators.

The official I spoke with agreed that Bexar County is well-equipped to secure the voting systems and voter information from cyberattacks. Not only do they have vendors come in once a year to inspect voting systems, but they also provide technical support, which includes the loading and testing. The systems are encrypted using federally certified encryption methods and those certified by the State of Texas. The official also feels strongly about their ability to secure voting systems because Bexar County uses electronic pollbooks, which the official believes to be the future; they have their databases and uses virtual private networks. They assign a password to all the staff or systems individually. According to the official, Bexar County has checks and balances to keep them ready to secure the electoral infrastructure.

Cameron County

Cameron County is located in the southernmost part of Texas, with Brownsville as the county seat. This County has approximately 218,910 registered voters with about 102 precincts.[80] According to the County official, "the elections administrator…serves as the Voter Registrar [and] is responsible for the department's daily functions and coordination of all electoral functions on behalf of the County."[81]

Cameron County uses hand-marked paper ballots with ballot marking devices for accessibility and an optical scanner for tabulation. They follow a precinct count voting system where the ballots are tabulated at the polling location. The County uses two backup methods for voting counts and results to avoid problems, including utilizing a USB drive and an internal record. The presiding judge brings the copy of the counts to the central location, and if an issue arises, an individual is sent to collect a copy of the USB drive and machines.

For Cameron County, the preparation for elections is a year-round duty. The planning process begins six months before the elections. The electronic pollbooks are not available online until a month before early voting begins. The voting equipment testing begins roughly one week before the election to verify that all the voting systems are operating well. While conducting the machines' testing, they are all secured at a specific location and not connected to the internet for security purposes. During my interview with one of the County officials, I asked about the steps they follow to test equipment before elections. The official explained that there is ongoing security surveillance of the County IT system. they would get equipment back online and verify the machine's state before making sure that nothing has changed. Then, they would invite the public to view the process where they would bring their systems online using virtual private

networks and run programs for security patches and installation along with performing the logic and accuracy test.[82] To better protect voter information, the County has decided to use virtual private networks (VPN), file transfer protocol for transferring files over the internet, physical security at the warehouse with the equipment, and assigned administrative rights and user controls. While they do not use encryption on their office systems, they encrypt data transferred to locations with no additional security layer.

After 2016, there were significant concerns regarding the security of Cameron County elections and voting systems. While laws were passed to upgrade voting systems, Cameron County could not switch to electronic voting systems. The official explained that they have been interested in implementing a hybrid voting system; however, they are not interested in using the direct recording electronic system. For this County, funding from the state and grant money from two outside entities allowed for better security of their voting equipment. The difference that they witnessed between the 2016 and 2020 elections was a significant increase in cybersecurity training and awareness. Cameron County established a process for reporting suspicious incidents or emails related to elections or voting systems. They have also noticed better communication between federal, state, and local officials. According to the County official, "with the [cybersecurity] training, we all started speaking the same language and understand each other."[83] The events that impacted the 2016 national elections provided a foundation for better security and relationship between the governments, allowing them to prepare for the protection of future elections.

When asked about the 2020 elections and if the County experienced any problems with the elections or voting systems, the Cameron County official responded by stating, "Every

election offers its challenges. COVID-19 was a challenge for us, and the machines did not have any problems. Using the paper-based system, covid did not have as much impact."[84] Like Bexar and Harris counties, the main problem that Cameron County experienced during the 2020 presidential election was misinformation and voters, which is becoming one of the most significant vulnerabilities to the election. Cameron County official explained that they want to address the issue of misinformation,

> [We will] try our best to make sure that information [that we share with the public] is legitimate. After 2020, misinformation is becoming a danger to our elections and we need to provide additional training [to the public and staff] to recognize it. The awareness of the threat has increased since 2016. The more information we have, the better we can protect ourselves and our democracy.[85]

I recommended the rumor control report established by the department of homeland security's CISA to the County official and suggested that they share this with their staff and the Cameron County voters.

When asked if Cameron County is well equipped to secure voting systems and protect voter information from cyberattacks, the official responded, "yes, we have gotten better. In the past, some information that should have been protected was released for sale. The County has changed the procedures to ensure that the data is protected and only those who need access have it. Controlled access to data."[86] Even with the necessary measures in place, individuals will continue to worry about democracy and electoral infrastructure security. With the current technological advancement, it is up to government officials to implement the proper security protocols and ensure that all the jurisdictions have the equipment needed to secure voting systems and voter information from cybercriminals.

Harris County

Harris County is the largest county in Texas, with an estimated population of over 4,713,325.[87] The County's election department is under the leadership of County Judge Lina Hidalgo and elections administrator Isabel Longoria. According to VerifiedVoting, Harris County had over 2,480,522 registered voters as of November 2020, with an estimate of 1,012 precincts.[88]

I interviewed Michael Winn, the Harris County Chief Deputy Administration, who has over 25 years of experience working in the government. He has worked in Bexar, Travis, and Harris Counties in the elections department and is on the Election Assistance Commission Board of Advisors. He was involved in implementing the Countywide voting centers in both the Harris and Travis counties, ensuring that voters can vote anywhere and eliminating the rules that voters can only vote in their precincts. Harris County officials have been working to ensure that they have the most updated voting equipment. However, Harris County did not begin thinking about making a transition until the 1990s. However, around 1998, Harris County officials and community leaders decided to select a new voting system to replace their punch-card machines. In 2001, they implemented the Hart InterCivic eSlate electronic voting system. The transition made Harris County a metropolitan area in the whole County to implement the electronic voting system.[89] Harris County continued using its DRE voting system until the 2020 presidential election and was prepared to update its electoral infrastructure, which will be used in the May 2021 election.

When preparing for elections, the County follows three preparing windows, which include 45, 60, and 90 days before elections. During these periods, they conduct hash code

testing to verify whether the code matches a hash code that was previously taken. If they do not, they choose to replace the system due to the possibility of the system being tampered with. They also perform the logic and accuracy testing where the machines are programmed with known values, and if the device does not have the same number of values, this would be problematic, and it would be quarantined. Forty-five days before the elections are known as the lockdown period where the system is air gapped. During the preparation period, the County involves its partners to check that their information such as addresses, contact and more is correct, including schools, political parties, and polling places. This process, known as entity proofing, is vital because they need to ensure that the public's information is correct.

During the interview, I asked Mr. Winn how the County deals with equipment security. He explained that "if there are updates, we do communicate with vendors…we do get the updates and when completed, there is a file, a record that shows that there has been an update and it outlines the details of it including dates and times. Record is sent to the state [Secretary of State}, and they have a version of the last update."[90] They also use encryption to protect their systems along with voter information. To backup votes or results, Harris County automatically performs audits during tabulation, and a paper copy of the ballots is saved. After the elections, all the machines used to conduct the elections would be taken to a central location and held for 22 months, along with a physical copy of the ballot. During the 2020 election, the County used only direct recording electronic for in-person voting and hand-marked paper ballots with optical scanners for absentee ballots; however, they bought the Hart InterCivic Inc. Verity Voting System, a hybrid voting system implemented and will use it in May 2021 election. This new voting machine is different for Harris County because it allows voters to verify their selections

before submitting their ballot. The county has also implemented the paper ballot, which they did not have for in-person voting before.

When I asked Mr. Winn how the 2020 presidential elections differed from 2016, he responded, saying that "there was more communication between CISA, DHS, FBI. Continuation efforts to make sure that County officials become a part of the decision-making of elections. The government was keeping information to themselves; part was to avoid vulnerability. In 2020, there was the inclusion of all officials."[91] While 2016 may have been one of the most horrifying years for the United States and its elections, it has brought awareness to not only the security of elections, but it has highlighted the issues that the different government entities were facing that could have led to the events that compromised important information. According to Mr. Winn, Harris County has a team of information technology (IT) specialists who provide the election officials updated on their voting equipment status and any critical information they need to know daily. The County also ensures that education and training are provided for every employee and encourages them to become certified in election security. They also have a program such as the automatic shutdown of programs when the computers experience inactivity, mitigating insider threat.

With Harris County being Texas's largest county, many individuals assume that they have all the necessary tools and are well equipped to secure elections and electoral infrastructure; however, when posed with the question of whether Harris County is well equipped to protect the voting systems and voter information from cyberattacks, the official's response was no different from the others, "nothing is guaranteed, our County does a good job of making sure that we stay current and make sure we have the best system in place. We just purchased a new voting system

that will be used for the first time in May 2021,"[92] referring to the DRE with VVPAT that will be used in the May 2021 Texas elections.

FINDINGS

While various mechanisms are being used to secure voting systems from cyber threats and attacks, no solution can guarantee complete security for electoral infrastructure.

Different jurisdictions are still conducting elections using older voting systems that are prone to vulnerabilities and cyberattacks. Using old voting equipment brings an increase in the possibility of those systems failing or becoming exposed. When the public becomes aware of the potential vulnerabilities associated with older voting systems and their elected officials not taking the proper measures to secure or upgrade the systems, it will cause trust issues. Even after 2016, Harris County continued using the old voting system, which they used for 17 years, proving some jurisdictions need to upgrade their systems and ensure better security.

The various types of governments need to communicate and collaborate better with one another when preparing for elections. Lack of communication played a factor in the events that took place in the 2016 Russian hack.

Funding that is provided to states might not be enough to implement new voting systems. HAVA's budget to the states is insufficient to purchase entirely new voting systems and offer election workers training.

Smaller jurisdictions are likely to fall victims to cyber threats and attackers if they are not provided the necessary resources to secure their voting systems. Therefore, there needs to be

equal distribution of resources between all the jurisdictions to ensure that they are all equipped to secure the elections.

Education has been one of the missing links when it comes to cybersecurity or election security. While 2016 brought awareness to the possibilities of elections being attacked, it also highlighted the lack of knowledge that those in charge of our democracy have, which increases the chance of exploitation by attackers. As a result, the State of Texas has decided to take the initiative to educate its staff, officials, and the public about the election and information security. Project V.O.T.E, Voters of Tomorrow through Education, "is a program designed to help students become knowledgeable, responsible voters."[93] It also provides them with additional resources about the election, voting systems, and more.

There needs to be better preparation for natural disasters, and officials need to study how this can impact elections, voting systems, and voters. In response to the COVID-19, Harris County implemented the S.A.F.E Initiative, where the County commits to ensuring that voters exercise their rights without worrying about health risks. Two of the counties I interviewed have implemented the curbside voting system for those who cannot enter the polling locations. However, for counties such as Cameron County, where they use paper ballots, it will be difficult for voters with disabilities to participate because they have to seek additional assistance. In addition, the voting system used would require that those with disabilities depend on others which could discourage some voters.

When interviewing the County officials, they all had one common goal, assuring me that all is well within their County elections department. They provided me with an "Our County did a good job" statement and expressed how proud they are of handling election problems or taking

care of their voting systems. Those officials provided me with good information and a great understanding of whether their jurisdiction is equipped to secure voting systems or not. However, they have left me with one question, is it possible to fully secure voting systems without possible interference or threats from cybercriminals?

There is a new problem more prominent than what was anticipated and might be one of the most dangerous threats to election security, and that is **misinformation**. Throughout my interview and research process, I discovered that one of the most recent impacts on the election is the misinformation fed to the public about elections, voting systems, and the security surrounding their democracy. Some of the officials' problems have to deal with system security and losing the public's trust.

While implementing various electronic voting systems has been a success for some states, paper ballots might be the most secure voting system backup plan, ensuring public trust for the elections, security, and election officials administering them.

RECOMMENDATIONS

Funding: The United States Congress needs to increase the funding provided to upgrade voting systems through the Help America Vote Act or provide financing to increase voting systems' security every four years. This law was passed to provide funding to improve digital democracy; therefore, Congress should invest more money into voting systems. They need to provide a constant and steady stream of funding to states to invest in their electoral infrastructure. Matt Bernhard advised that "it is ridiculous to be charged more for voting machines while cell phones cost way less. The market should shift from for-profit companies so that the jurisdiction can pay less and invest more in their staff. We need to focus on the annual funding for elections and not just when federal elections are happening,"[94] which is something that many do not think about. Congress needs to budget funds that can be used to secure voting machines and ensure a safer democracy.

Education: Cybersecurity Education is a critical need for election security, and action needs to be taken. Congress needs to invest in educating the individuals that are responsible for taking care of the electoral infrastructure. The National Science Foundation needs to create a grant dedicated to training students interested in studying cybersecurity, focusing on election security, or securing voting systems. Colleges and universities need to establish a curriculum that focuses on the "growing organizational management and information technology needs of the election community"[95] and collaborate with government entities to ensure that these students are staffed upon graduation. While the State of Texas has implemented training and the necessary tools needed by its staff to remain cyber aware, they also need to invest in educating cybersecurity students who safeguard our elections and machines in the future. The Texas Secretary of State

implemented project V.O.T.E which provides voters with the ability to learn about the election, which is available to the public and children. While this is helpful, more needs to be done to educate them about election security and recognize cyber threats.

Voting Machines: One of the most critical parts of the election process is the voting system. Attackers are beginning to target voting machines to compromise elections, and steps need to be taken to safeguard against these attacks. During his testimony before Congress and the Texas Senate Select Committee on Election Security, Dan Wallach, a professor in the Rice University Department of Computer Science, offers recommendations on securing voting machines from attacks. To mitigate against the cyber threats, "First and foremost, we can require computer backups and run drills to make sure we can rapidly recover from corruption. We must certainly establish baseline computer security standards for network firewalls, intrusion detection systems, and other "good hygiene" practices, along with state resources to help our counties adopt such practices."[96] Additionally, counties use the air gap method and disconnect their systems from the internet. The federal, state, and local governments need to establish a timeline for which voting machines can be used and replaced.

Counties would have to choose between using the hybrid voting system for all voters or turn to paper ballots with better accessibility for voters with disabilities. Not only will they do this, but they also need to encrypt all the data on their systems using an advanced encryption method. In addition, systems need to be patched when the security updates become available, and penetration testers need to be hired to test the voting machines before and after each use.

> Before the State spends precious resources on replacement technology, it must establish standards for new equipment and backend data systems, including voter registration databases, that are both protective and practical. Standards must come before any money

> is spent on new systems. At a minimum, new voting systems must include the capacity for paper auditing. Separating hardware from software, such that replacing or updating one does not require replacing or updating the other, also would have substantial cost and security benefits relative to the current market for voting equipment.[97]

Communication: Better communication needs to be established between the federal, state, local governments, and other partners in securing democracy in the United States. During my interview with the County officials from Texas, I was informed that communication between the federal, state, and local governments improved tremendously between the 2016 and 2020 elections. While this may be the case, the government needs to communicate with the public and provide them with the necessary tools to understand election security. According to the Texas Secretary of State (SOS), "Most Texas counties participate in the Elections Infrastructure Information Sharing and Analysis Center (EL-ISAC) to ensure that the elections community is effectively sharing relevant information to safeguarding our elections and being aware of potential cyber threats."[98] This is important because it provides a collaborative environment and better communication. The Department of Homeland Security needs to establish a committee that will support the EAC in ensuring that counties receive all the critical communication regarding elections and electoral infrastructure.

Resource Distribution: Jurisdictions must be provided with the necessary resources to secure elections and voting systems. While the size of counties varies by population, it is still crucial that they are equally given the proper resources to protect the critical American infrastructure. The Help Americans Vote Act provides states with the funds needed to update their voting systems and improve their management of elections altogether. For example, Texas was provided with $23.3 million and a match of over $1.1 million. These funds were used to enhance

election security as well as the voting machines. During the interview process, all the election officials assured me that their counties were given adequate resources to secure their voting infrastructure. However, smaller jurisdictions must be well taken care of and provided with the training. While cybercriminals have been focused on targeting voting systems, they will also be looking to target vulnerable jurisdictions, typically the smaller jurisdictions that are constantly ignored. Therefore, ensuring that all the resources are equally distributed or jurisdictions have sufficient resources is critical and will provide a better, more secure election.

Misinformation: While the focus has been on securing electoral infrastructure, the 2020 elections presented us with a new problem, misinformation. The Texas Secretary of State reported that they had created communication with several social media corporations and law enforcement to remove incorrect information shared on those sites regarding the elections.[99] And they have provided their email where voters can report those incidents. Jurisdictions also need to share CISA's Rumer Control report with the public to provide them with additional resources to combat misinformation. To deal with this problem, all government entities will need to work in tandem to provide the public with the resources required to educate them and recognize misinformation about elections and voting machines. States need to create databases where voters can report inaccurate and misleading information or receive threats regarding their votes.

CONCLUSION

Let us turn back to the research question that guided this thesis: How prepared are county officials to defend against cyber threats to electoral infrastructure? To answer this question, this thesis analyzed the various types of voting systems used in three counties in Texas, high-level policies regarding voting technology. Finally, it looked at whether all jurisdictions are well equipped and prepared to secure elections, voting systems and prevent interference from cybercriminals.

Looking at the technical vulnerabilities, the currently used voting systems are vulnerable to manipulation. Election security experts have recommended that the Direct Recording Electronics be updated by adding a paper trail or replacing a different voting system, including paper ballots. Voting technologies are at risk of being hacked, and attackers have started to improve their skills to accomplish their goals of tampering with the American elections. Not only are there multiple threats to voting systems, but officials also need to begin worrying about the human factor and provide proper training for those in charge of administering the elections. Misinformation also contributes to the loss of public trust in the government, election security, and democracy. Protecting the voting systems and educating the public about election security is critical and can provide a safer election.

While many states in the United States have followed the HAVA funds to update their voting technology, some remain with unknown decisions about what they plan to do. For Bexar, Cameron, and Harris counties in Texas, election security is a critical need, and they have been working to ensure that they are successful in protecting their electoral infrastructure. Even though they implemented different voting systems, these three counties have shown that they are

willing to stay up to date with the growing need for better election security. The state of Texas has established different programs that will be used to train their election departments and educate the public about cybersecurity. With the various steps being taken to advance, more work still needs to be done. Cameron County's use of paper ballots is a safe way to administer elections; however, more work needs to be done to accommodate voters with disabilities. Better alternatives need to be provided for those who need assistance. Even though the election officials assured me that all counties are equipped to secure voting systems and elections, they need to ensure that they use the funds provided to them and update their voting technology.

Regarding the high-level policies, the United States Congress passed laws that push for better voting systems while replacing the aged ones used in jurisdictions around the country. They passed the Help America Vote and For the People Acts which provided funding for states to modernize their voting technology, pushing for better election security and protect voter information. While these laws were passed as the foundation for improving the safety of elections in the United States, the funds provided are not enough for long-term security. There need to be more funds provided before each election that jurisdictions can use to improve elections' security and ensure that attackers cannot interfere with the elections.

There have been attempts to interfere with elections in countries around the world. However, the American elections have become the primary target by nation-state actors, and they are finding new ways to influence the elections. As a nation, the United States needs to plan ways to stop cybercriminals from attacking their elections. The Russian interference with the 2016 presidential election left the American public with questions regarding the future of their digital democracy, and officials have made it their duty to ensure that the elections are secured.

There need to be security measures to safeguard the election, voter information, voting systems, and training for everyone. The events that took place in 2016 brought awareness to the issue of election security. Thus, the United States needs to focus on improving its practices and replacing obsolete and insecure systems, implementing security procedures that can defeat attacks in the future head-on.[100] While it is not possible to fully secure elections or voting systems, there will need to be a collaboration between voters, governments, industry professionals, and academia to build a safer democracy. Each of these systems plays an essential role in ensuring that the elections are not influenced or tampered with; therefore, they all need to ensure that elections are protected.

WORKS CITED

[1] Wallach, D. S. (2018, March 13). *Post-hearing Letter* [PDF]. Houston:

[2] National Academies of Sciences, Engineering, and Medicine. 2018. Securing the Vote: Protecting American Democracy. Washington, DC: The National Academies Press.

[3] Abrams, Abigail. “Here's What We Know So Far About Russia's 2016 Meddling.” Time. Time, April 18, 2019.

[4] Felsenthal, E. (2020, April 09). Front line workers tell their own stories in the new issue of time. Retrieved April 11, 2021.

[5] Fischer, Eric A. “Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues.” epic.org, November 4, 2003.

[6] Roos, Dave. “How Americans Have Voted Through History: From Voices to Screens.” History.com. A&E Television Networks, April 13, 2020.

[7] Halderman, J. Alex. “Securing Digital Democracy.” Coursera, 2009.

[8] Roos, 2

[9] Halderman, 2

[10] Roos, 3

[11] Halderman, 3

[12] Halderman, 4

[13] Halderman, 5

[14] Roos, 4

[15] Norden, Lawrence, and Andrea Cordova McCadney. “Voting Machines at Risk: Where We Stand Today.” Brennan Center for Justice, March 5, 2019.

[16] Long, Colleen. “Cybersecurity Officials Start Focusing on the 2020 Elections.” AP NEWS. Associated Press, November 8, 2018.

[17] Norden, 2

[18] Ney, Robert W. “Text - H.R.3295 - 107th Congress (2001-2002): Help America Vote Act of 2002.” Congress.gov, October 29, 2002.

[19] National Election Defense Coalition. “WHY E-VOTING SYSTEMS PUT DEMOCRACY AT RISK.” National Election Defense Coalition. Accessed April 11, 2021.

[20] VerifiedVoting. “Voting Equipment.” Verified Voting. Accessed April 30, 2021.

[21] Wallach, Dan S. “On the Security of Ballot Marking Devices.” Arxiv.org, 12 Dec. 2019.

[22] Wallach, 2

[23] “The Dangers of Ballot Marking Devices.” National Election Defense Coalition. Accessed April 30, 2021.

[24] VerifiedVoting. “Voting Equipment.” Verified Voting. Accessed April 11, 2021.

[25] Fischer, 2

[26] Gambhir, Raj Karan, and Jack Karsten. “Why Paper Is Considered State-of-the-Art Voting Technology.” Brookings. Brookings, August 14, 2019.

[27] Wallach, Dan S. “Commentary: Bill Promises Better Election Security. Let's Be Sure to Get It Right.” Statesman. Austin American-Statesman, March 25, 2019.

[28] Wallach, 2

[29] Brennan Center For Justice, Common Cause, National Election Defense Coalition, and Vorifiedvoting. “Securing the Nation’s Voting Machines.” verifiedvoting.org, 2018.

[30] Goggin, Stephen N, Michael D Byrne, and Juan E Gilbert. “Post-Election Auditing: Effects of Procedure and Ballot Type on Manual Counting Accuracy, Efficiency, and Auditor Satisfaction and Confidence.” Liebertpub, 2012.

[31] Byrne, Michael D, Kristen K Greene, and Sarah P Everett. “Usability of Voting Systems: Baseline Data for Paper, Punch Cards, and Lever Machines.” Houston: chil.rice.edu, 2007.

[32] Everett, Sarah P, Michael D Byrne, and Kristen K Greene. “MEASURING THE USABILITY OF PAPER BALLOTS: EFFICIENCY, EFFECTIVENESS, AND SATISFACTION.” Houston: chil.rice.edu, 2006.

[33] VerifiedVoting, 2

[34] Hubler, Katy Owens. Voting Equipment, August 20, 2018.

[35] Bernhard, Matthew, Kartikeya Kandula, Jeremy Wink, and J. Alex Halderman. “UnclearBallot: Automated Ballot Image Manipulation.” E-Vote-ID'19, 2019.

[36] Election Systems & Software. “ExpressVote.” Election Systems & Software, December 15, 2020.

[37] Ropek, Lucas. “America's Love Affair with Paperless Voting Is Over. Here's Why.” Government Technology State & Local Articles - e.Republic, 2020.

[38] Ropek, 2

[39] FireEye. “Advanced Persistent Threat Groups (APT Groups).” FireEye. Accessed April 11, 2021.

[40] CISA and FBI. “Alert (AA20-296B).” Cybersecurity and Infrastructure Security Agency CISA, October 22, 2020.

[41] Ibid

[42] Conklin, Wm Arthur, Gregory B. White, Chuck Cothren, Roger Davis, and Dwayne Williams. *Principles of Computer Security: CompTIA Security+ and beyond, (Exam SY0-501)*. New York: McGraw-Hill Education, 2018.

[43] Conklin, 2

[44] National Academies of Sciences, Engineering, and Medicine 2018. Securing the Vote: Protecting American Democracy. Washington, DC: The National Academies Press.

[45] Halderman, 6

[46] Webroot. “What Is Social Engineering? Examples And.” Webroot. Accessed April 12, 2021.

[47] Day, Brittany. “FBI: The 2020 Presidential Election Is Under Attack by Email Scammers.” FBI: The 2020 Presidential Election Is Under Attack by Email S., October 19, 2020.

[48] Day, 2

[49] Proofpoint. “The Human Factor Report.” Proofpoint, 2019.

[50] Verizon. “2020 Verizon Data Breach Investigations Report,” 2020.

[51] Lipton, Eric, David E. Sanger, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New York Times. The New York Times, December 13, 2016.

[52] Gibson, Darril. *Comptia Security+: Get Certified Get Ahead*. Virginia Beach, VA: Ycda, LLC, 2017.

[53] Frankland, Richard, Denise Demirel, Jurlind Budurushi, and Melanie Volkamer. "Side-Channels and EVoting Machine Security Identifying Vulnerabilities and Defining Requirements." IEEE, October 17, 2011.

[54] Lipton, Eric, David E. Sanger, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New York Times. The New York Times, December 13, 2016.

[55] "2016 Presidential Campaign Hacking Fast Facts." CNN. Cable News Network, October 28, 2020.

[56] CISA

[57] Schmdit, Wayne. "Misinformation, Not Vote Tampering, Is Our Most Critical Election Threat." SIW, November 2, 2020.

[58] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. "#Protect2020 Rumor vs. Reality." Cybersecurity and Infrastructure Security Agency CISA, 2020.

[59] Interview with Matthew Bernhard, PhD, 2021

[60] Center for Civic Design. "Vol. 1 Designing Usable Ballots." Center for civic design. Accessed April 12, 2021.

[61] Center for Civic Design, 2

[62] Verizon. "Funding Safe and Secure Elections During the COVID-19 Pandemic." Government Technology State & Local Articles - e.Republic, August 5, 2020.

[63] Verizon, 2

[64] Ney 2

[65] Lofgren, Zoe. "Text - H.R.2722 - 116th Congress (2019-2020): SAFE Act." Congress.gov, June 28, 2019.

[66] Lofgren, 2

[67] Lau, Tim, and Daniel I Weiner. "Historic Bill to Strengthen Democracy Introduced in Congress." Brennan Center for Justice, January 3, 2019.

[68] Pew Research Center. "Views of Election Policy Proposals." Pew Research Center - U.S. Politics & Policy. Pew Research Center, October 29, 2018.

[69] US Census Bureau

[70] Verifiedvoting, 3

[71] DIR. "Elections Cybersecurity Guide." Texas Department of Information Resources, n.d.

[72] Verifiedvoting, 4

[73] Benton, Jackie. "Cyberdefense for Texas State Government." Texas Controller of Public Accounts, March 2019.

[74] Bexar County. "Bexar County Elections Department." Bexar County Elections Department | Bexar County, TX - Official Website. Accessed April 12, 2021.

[75] Election Systems&Software. "ExpressVote." Election Systems & Software, December 15, 2020.

[76] Election Systems&Software, 2

[77] Interview with Bexar County official, 2021

[78] Ibid

[79] Ibid

[80] Verifiedvoting, 5

[81] Cameron County. “About Us.” Cameron County. Accessed April 12, 2021.

[82] Interview with Cameron County Official, 2021

[83] Ibid

[84] Ibid

[85] Ibid

[86] Ibid

[87] Census.gov, 2019

[88] Verifiedvoting, 6

[89] Harris County. “Harris Votes - Voting Information.” Home - Election Division. Accessed April 12, 2021.

[90] Interview Michael Winn, Harris County Official, 2021

[91] Ibid

[92] Ibid

[93] Texas Secretary of State. “Welcome to Project V.O.T.E.” Project V.O.T.E. Accessed April 12, 2021.

[94] Interview with Matthew Bernhard, PhD, 2021

[95] Ibid

[96] Wallach, Dan S. “Before the Texas Senate Select Committee on Election Security.” Houston: cs.rice.edu, February 21, 2018.

[97] Wallach, D. S. (2018, March 13). *Post-hearing Letter* [PDF]. Houston:

[98] Texas Secretary of State. “Welcome to Project V.O.T.E.” Project V.O.T.E. Accessed April 12, 2021.

[99] Ibid

[100] Wallach, Dan S. “Before the House Committee on Space, Science & Technology Hearing, ‘Protecting the 2016 Elections from Cyber and Voting Machine Attacks.’” Houston: cs.rice.edu, September 13, 2016.