Vote Safe

Rethinking Election Security

Emelin Flores, Aruj Jain, Bhavana Chamarthi, Sagar Reddy Patil, Molly Cantillon, Tejas Kaushik

Vote Safe: Rethinking Election Security

Emelin Flores, Aruj Jain, Bhavana Chamarthi, Sagar Reddy Patil, Molly Cantillon, Tejas Kaushik

Governor STEM Scholar

Introduction

The 2016 presidential elections questioned the strength of U.S elections as public attention raised concerns that the voting infrastructure used by states might be suspect, unreliable, or potentially vulnerable to attacks. The ability to vote is the foundation of American democracy and must be protected to ensure the liberties of equality.

The rise in speculation of election security stemmed from evidence of foreign efforts to intrude into state voter registration systems, international attempts to exploit U.S politicians through hack-and-leak operations, and spreading misinformation campaigns through social media sites.

This report intends to give election security enthusiasts information they need to contribute to securing elections and introduce a hand-marked ballot voting machine to address voting security. It sets out to describe current vulnerabilities, assessing existing safeguards and policy choices that are intended to reduce risks of exploiting U.S elections. The assessment used for this report uses New Jersey's election infrastructure as a reference point to assess election security in different states and countries focusing on the legislation, information warfare, and new approaches to secure our digital democracy. In evaluating New Jersey's election infrastructure, the paper reviews the Center of American Progress 2018 report that details and scores the election security in all 50 states, current legislation that addresses election security, and Robert Mueller's report on Russian interference in the 2016 elections. The team built a prototype of a voting machine that promotes automated post-election audits and voter-verified paper audit trails. The voting machine will be discussed in more detail about how it addresses current election security vulnerabilities.

Election security is a prominent issue now as new technology presents new challenges on how to secure it. Protecting election security is a team effort involving local election officials, each state's chief election official, state cybersecurity experts, and the federal government. Together, people can demand that local officials protect the vote and enact more substantial security reforms, push for the Secretary of State and state legislature to pass risk-limiting audits, push for paper ballots and ensure the minimum security requirements. Together, election security can be transparent, reliable, and prepared for any potential attacks.

Background

Assessment of the Center of American Progress (2018) Report

In 2018, the Center for American Progress analyzed and summarized the election security of all 50 states plus the District of Columbia. Cyber-attacks and election interference attempts are becoming more sophisticated and common, so it is important for states to be prepared. The report specifically scored each state based on the way it handles cybersecurity standards for voter registration systems, voter-verified paper ballots, post-election audits that test election results, ballot accounting and reconciliation, return of voted paper absentee ballots, voting machine certification requirements, and pre-election logic and accuracy testing. These are all logistical measures and focus on minimizing error for an election by ensuring that all votes are correct and accounted for. These measures do not exactly prevent any hacking attempts or security vulnerabilities in electronic systems, but serve to make sure states have robust and reliable infrastructure (machines, procedures, officials) in place.

The highest-ranked states in the report (with a score of B, the second-highest possible rating), are Alaska, Colorado, Connecticut, Maryland, Minnesota, New Mexico, New York, North Carolina, Oregon, Rhode Island, and also the District of Columbia. The lowest-ranked states in the report (with a score of F, the lowest possible rating) are Arkansas, Florida, Indiana, Kansas, and Tennessee. New Jersey received a score of D (the second-lowest possible rating), being labeled “Unsatisfactory” for the categories of voter-verified paper audit trail, post-election audits, ballot accounting and reconciliation, and voting machine certification requirements. New Jersey was specifically advised to adopt a paper-based voting system, require post-election audits (those in Colorado serve as a strong example), and strengthen its ballot accounting and reconciliation methods. The latter can be accomplished by having precincts compare the number of ballots gathered to the number of voters that signed into the polling station, and by having counties compare numbers reported by precincts to composite results. In addition, all voting machines currently in use and in the future should be required to follow the U.S. Election Assistance Committee (EAC) Voluntary Voting System Guidelines.

Arkansas, one of the states that received a score of F, does not have paper records for its voting machines and does not require post-election audits. Their score could be improved if they used paper ballots instead of only Direct Recording Electronic voting machines (DREs), and if they executed post-election audits to make sure election results are accurate. Fortunately, the state does have access to the funds that could make this possible. Florida, another state that received a score of F, has the same limitations as Arkansas regarding no paper trail and a lack of auditing. In 2018, Governor Rick Scott requested $2.4 million for cybersecurity improvements to voting systems/software, which would be greatly beneficial if implemented properly (Root et al., 2018, p. 60). The report indicates that many states experience the same vulnerabilities that can be solved in similar manners- chiefly adding a physical paper trail and investing in post-election audits. It is also recommended that all states work with the Department of Homeland Security or National Guard for resources and threat assessment since many states lack the resources to organize secure voting systems on their own.

Alaska, one of the states that received a score of B, was commended by the report for using paper ballots and following best practices for voter registration cybersecurity. They could improve their security by accounting for Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) votes in their post-election audits. Also, their audits currently are based on a fixed number of total ballots rather than a statistically significant number with a margin of victory. A common vulnerability in many of the states with a score of B is that absentee ballots can currently be returned electronically; this should be changed so that absentee ballots can only be submitted in-person or by mail since electronic submittal introduces risk and compromises the audits. Colorado, another state that scored a B, was commended for becoming the first state to require post-election audits, but they also have the vulnerability of absentee votes being submitted electronically.

The report found that all states in the nation have made at least some attempts to improve their voting security; for example, in 2017, Virginia switched to a statewide paper ballot based system and Rhode Island decided to make post-election audits mandatory. Alabama has required election officials that interact with the voter registration system to receive cybersecurity training. New York independently passed a new initiative in 2017 to create helpful resources like an Election Support Center, Election Cyber Security Support Toolkit, and Cyber Risk Vulnerability Assessments (Root et al., 2018, p. 4). These steps are important, but the general state of vote security across the nation is still vulnerable and there are many upgrades that can be made. Regarding general best practices, as mentioned earlier, the investigation advocates for risk-limiting post-election audits and replacing paperless voting with technology that would create a voter-verified paper trail. Having only paper ballots statewide always led to higher scores, but DRE machines that produce voter-verified paper records were also satisfactory. It is the responsibility of each state to strengthen its voting infrastructure, to preserve confidence in and prevent foreign interference with our democratic elections. States must work with the federal government for funding and assistance, and officials of all levels should see that this pressing need is dealt with.

Assessment of Foreign Influence in the United States Election

As technology advances, the most important components of American democracy are becoming vulnerable to outside influences. Over the past years, such influence, in particular Russia, has notably affected the 2016 US presidential election. The security breaches that occurred during 2016 spotlighted an urgent requirement for a well shielded election system. However, in order to build this system, the main components of the security breaches from 2016 must be analyzed -

this includes the effect of Russian Internet hacking communities, the role of social media, and the findings of the Mueller Report.

Through the course of the 2016 election, Russian hackers used online methods to polarize American media, and expose classified, government information. Organized hacking groups were the mastermind behind these attacks, with groups such as "Cozy Bears" (also known as "The Dukes") engaging in 6-year long spying campaigns targeting Washington D.C and the European Union. Other groups such as "Fancy Bear" and "Turla" primarily attacked US military and intelligence agencies. Russian hacking groups have been a known threat to US elections since Obama's campaign, responsible for building and imitating credible websites in attempts to spread false information to American voters. By building automated bots and trolls (accounts programmed to function autonomously in attempts to influence readers), hacking communities grew exponentially and expanded their online presence.

Russian hackers leveraged Facebook's nationwide outreach to proliferate misinformation using the largest social media platform available in America. Facebook was used by Russian hackers to successfully infiltrate into American's emotions by successfully choreographing public, violent demonstrations of American nationalism. When Facebook ads were bought by hacking groups, these ads impacted Google searches and other large platforms across the internet— thus causing a domino effect. The content of such advertisements twisted reality to polarize American voters and create a deep rift between extreme liberals and conservatives. Particularly, these ads acted like catalysts in promoting white-supremist campaigns, as confirmed with the staggering increase in hate crime incidents during 2017. The click-bait nature of the fake ads gained traction with Americans and allowed for troll-websites to earn anywhere between $10,000 - $30,000 in revenue per month (Hess, 2017).

The work of Russian groups during the 2016 US election focused on exposing controversial issues in order to break down the trust of American voters and cause mass disruption. Based on the hacking group's previous focus on racial issues, it is predicted that in 2020, such groups will further invigorate racial tensions on a larger scale. It is worth noting that despite the knowledge of Russia's involvement in previous US elections, the US was not prepared and has not made sufficient efforts to counteract the attacks that occured in the 2016 elections and the attacks that will inevitably occur in 2020.

In order to prevent hacking groups from infiltrating into future US elections, the government and companies with large online presence must work together to monitor and remove false news/ads being spread on their respective platforms. In addition, American voters should take steps to start reporting any suspicious information being spread online. By taking preventative measures, the effectiveness of Russian groups can be eliminated. However, these precautions do not warrant protection from possible newer methods of infiltration that may be presented in the 2020 elections.

The role of social media in the 2016 presidential election provided an edge for Russia to disrupt the US political climate. Foreign involvement emerged through automated Twitter troll bots, which regularly posted anti-Clinton messages on the days leading up to election day. On election day, it was reported that “#WarAgainstDemocrats” was tweeted over 1700 times by a group of these bots (Shane, 2017).

The use of trolls to manipulate users was also seen in Facebook, where bots promoted “DCLeaks” and “WikiLeaks” (websites which exposed classified information about the Clinton campaign). By exploiting the personal information of real Americans, bot accounts seemed to be authentic and went unnoticed by Facebook officials. Through such bots, political ads were successfully promoted to American voters. Infact, the Internet Research Agency reported that in over a four year time span, “In an operation that cost millions of dollars, the Russians studied U.S. political groups, traveled to gather intelligence in several states and developed a network of fake accounts that they used to infect the American electorate” (Abrams, 2019). Furthermore, such ads served to instigate violence, by encouraging opposing groups (such as “Black Lives Matter” and white supremacism) to protest and engage in other forms of public radical expression in close proximity to one another. Unfortunately, Facebook officials were too late in shutting down these propaganda posts, bot accounts, and advertisements because the messages were already shared across the internet.

In addition to being the platform which spread politically-motivated messages, Facebook also shared user’s personal data with third-party vendors like Cambridge Analytica (Detrow, 2018). Cambridge Analytica, a British political consulting firm, used unauthorized information of Facebook user’s data to strategically aid Republican candidates to victory. Although initially involved in aiding Ted Cruz, Cambridge Analytica started to help the Trump campaign once Donald Trump became the GOP nominee. Through non-consensual harvesting of Facebook user’s data, Cambridge Analytica created psychological profiles of American voters. Their research led to mass, personalized advertisements targeted to “persuadables” (swing voters). From Twitter troll bots to Facebook’s lack of secure measures and the involvement of Cambridge Analytica, it was evident that the 2016 election was significantly impacted by foreign entities. A recurring theme throughout Russia’s use of social media to further political agendas, was the breach of user’s personal data in attempts to divide and radicalize American voters. As stated by Daniel R. Coats, the director of US National Intelligence, “Russia’s social media efforts will continue to focus on aggravating social and racial tensions, undermining trust in authorities, and criticizing perceived anti-Russia politicians. Moscow may employ additional influence toolkits—such as spreading disinformation, conducting hack-and leak operations, or manipulating data—in a more targeted fashion to influence US policy, actions, and elections” (Coats, 2018). Moving forward, Russia will adapt to the new political climate and utilize more advanced technology, presumably including ‘deep fakes’ (technology used to morph a person in an existing image/video, replacing someone else's image) and several other unknown means of propaganda using artificial intelligence. Social media corporations, driven by ad revenue, are further compromising the security of user’s data by willingly selling information to create models for targeted advertisements. The Facebook-Cambridge Analytica scandal exemplified how advertising user data-set models were exploited for political gains, which posed an outright danger to US democracy as a whole.

In order to address such issues for the 2020 election, it is imperative that the government, social media companies, and American voters collectively take the proper measures to keep personal data secure. This includes strict regulations enacted on how social media is used for political campaigns. Government and social media companies should collaborate to defend data breaches and should be held liable for the misuse of user's personal data. Using this partnership, they should also advertise and alert citizens by spreading awareness about authentic news sources, political advertisements, and other forms of propaganda. User's should also participate in actively reporting any skeptical information posted online to concerned authorities.

In an assessment of the foreign influences within the 2016 elections, Former Special Counsel for the United States Department of Justice Robert Mueller published a 448-page report on April 18, 2019, detailing how the Russian government influenced American discourse throughout the election campaign and hacked into the servers of political leaders to mobilize the information warfare against America. Mueller's Russian interface findings show that there were two major Russian government efforts; there was the social media propaganda operation and there was the Russian hacking and dumping operations.

The social media propaganda operation was led by the Russian Internet Research Agency, a company engaged in online influence operations on behalf of Russian business and political interests. Russia's social media efforts focus on aggravating social and racial tensions, undermining trust in authorities, and criticizing perceived anti-Russia politicians (Coats, 2018). The social media propaganda operation started through "troll farms," an organized operation of many users who work together in a "factory" to generate online traffic aimed at affecting public opinion, creating fake online accounts that "favored candidate Trump and disparaged candidate Clinton" (Mueller, 2019).

Russian hacking and dumping operations consisted of hacking to gain access to sensitive information from political leaders through social engineering attacks. Russian hacking groups used malicious emails to gain access to the Democratic Congressional Campaign Committee's computer network during the 2016 presidential campaign. In June of 2016, Russian hackers launched DCLeaks.com and posted thousands of stolen documents and emails there to highlight mistrust in U.S political leaders (Abram, 2019). In addition to DCLeaks.com, some of that material was then posted online by the Russians themselves, while another material was eventually posted by WikiLeaks (Prokop, 2019).

Robert Mueller's report verified the initial suspicions of foriegn involvement during the 2016 election. This report highlighted the great lengths that Russian intelligence took to manipulate the political climate within the United States and also expanded on President Trump's involvement throughout this process.

The 2016 election was plagued with errors that, in hindsight, could have been prevented. As described in the Mueller Report, foreign involvement within the US election was the greatest threat to US democracy regardless of its nature. From the unauthorized access of personal data that Cambridge Analytica manipulated, to the security breaches that allowed Russian hacking groups to prevail, the election was ridden with threats. As social media and online platforms grow, US elections are going to be susceptible to newer cyber threats.

To ensure that elections are shielded from dangerous outside influences, Americans, companies, and the government officials must collaborate to create authentic online news sources and actively report any suspicious advertisements/bot accounts activities present throughout the Internet. Ultimately, it all burns down to: creating public awareness, encouraging dialogue and debates, enforcing regulation, and finally continuing to monitor this process using AI… are some of the tools that can save our democracy.

Current Regulations/Legislation for Election Security

In the state of New Jersey, election standards are currently in the process of being changed after New Jersey was declared one of the most vulnerable states to voter hacks. The current election standards involve electronic voting machines that are easily susceptible to voter attacks. NJ then introduced Bill A3991, the New Jersey Election Security Act which was proposed on 5/17/18. This bill proposes to move away from the current electronic ballot system and replace it with a more secure paper ballot system that utilizes optical scanners. This system is said to be more secure and less prone to attacks due to the complexity of the system as well as the simplicity of the paper ballot system. This would greatly affect the NJ voting system as for decades, votes have always been cast electronically, thus the state would be forced to reevaluate its voting infrastructure. All designated voting areas would need to be updated with the proper optical scanning equipment and therefore, putting this program into effect presents many opportunity costs.

Since this bill is very technical and will require effort from all angles to implement, it has unfortunately been held in the NJ committee for almost two years. However, New Jersey is well aware of their lack of security in elections and is still making strides to strengthen voter safety. As mentioned before, New Jersey scored a “D” in the report by the Center for American Progress and according to the federal government, New Jersey is extremely susceptible to both outside influence as well as physical manipulation. The current election standard enforces the use of multiple models of outdated voting machines such as the ES&S AutoMARK, which is also used in 28 other states. New Jersey has vouched to spend $10 million from the federal government to polish and replace these machines throughout the state but only 15 counties have received some of this money.

Our election standard takes the best elements of various secure voting techniques and combines them into one simple process. We decided that the most secure way of counting votes was to indeed have a paper trail system, but since technology has advanced to a significant level, we have decided to pair that concept with the use of Raspberry Pi microcontrollers and the latest sensors. Our system allows every vote to remain completely anonymous as they will be stored on a secure network, however, if any deficiencies do exist, the paper trail system can be referenced as a method of checks and balances. In addition, this system features a hand-marked ballot system that works cohesively with the technical component to assure that each vote is recorded securely. In terms of implementation, this would require a joint effort between the NSA, the Federal Government, and other security agencies to ensure a smooth transition from the traditional voting structure to our more secure standard, but all in all, this standard ensures voter security and sets America on a brighter path towards less manipulable elections.

Proposal Background

Assessment of Open-Source Software or Hardware Developments

America has a variety of ways that they currently conduct their elections. From paper ballots to completely digitized votes, kiosk-style voting machines act as an intermediate, combining both physical and digital verification components. In 2002, the Help America Vote Act established the US Election Assistance Commission (EAC) to mandate the federal guidelines for election infrastructure. These guidelines include the requirement of voter-verified permanent paper ballots and recurrent testing of voting machines to ensure compliance with cybersecurity guidelines. One of the biggest components of the guidelines is that it allows states to self-regulate and individually adapt the mandated guidelines for their voting machines, meaning that states are more inclined to bend the rules in favor of what will save them time and money. This ultimately leads to leniency, manipulation and the development of loopholes in the system.

Brazil and India, two of the most populated countries in the world, rely on voting kiosks entirely. They use the Election Systems & Software's (ES&S) iVotronic kiosk-style voting machine which allows voters to cast their ballot on a touchscreen and confirm their vote with the real-time printed audit log. In this voting configuration, a poll worker uses a device called the personalized electronic ballot (PEB) to enable voting for the next user. These PEBs are used to calculate and store the final vote tallies from all machines. Because this device holds so much power in the outcome, there are a vast number of security concerns on the machine's reliability. According to the recent Security Evaluation of ES&S Voting Machines and Election Management System study done by the University of Pennsylvania, a voter with "a magnet and a properly programmed PDA could gain privileged access to the sensitive functions of the machine". The issue with this is that once an attacker gains access to a PEB, they are not only able to change the votes, but can attack the central Election Management System when the PEB is returned to the election headquarters. In 2017, hackers from DEF CON, one of the world's largest hacker conventions, were able to exploit vulnerabilities in the iVotronic machine and change vote totals. The ease at which these voting machines were hacked is alarming, raising concerns around the world. Due to various security concerns, both Germany and the Netherlands have banned e-voting. For kiosk-style voting machines to be implemented in the US, major revisions would have to occur. This includes changing the structure with how a vote is cast, eliminating the flaws of PEB or PEB entirely, and closer monitoring of the transfer of votes.

A secondary technological solution to voting machines is Scantron style input machines. A Scantron is a device used to convert marks on a paper form into a digital form, most commonly used for multiple-choice and true or false testing. In a voting context, a voter would bubble their chosen candidate on a paper ballot, insert their ballot into a user-friendly optical scanner voting machine, and wait for the machine's verification of accuracy and completeness. The technology behind these optical scan voting machines is called Optical Mark Recognition (OMR) which is a way of using differences in reflectivity to read human-marked data from predefined positions on a form. OMR devices shine a beam of light to compare the contrasting reflectivities at different positions on the page, allowing them to determine what is shaded from what reflects the least amount of light. While there are not many statistics on these machines' accuracy, they rarely make mistakes in detecting the correct selection that the user indicated.

Scantron style input machines are used all around the country, so choosing to implement the scantron process for the purpose of voting could be seamless. The Philippines uses more than 80,000 optical scanners in their elections, the most of any country in the world. The benefits of using optical scanners are that more people would be able to vote simultaneously, manual recounting of ballots is possible, and in the event that a machine breaks, voters can still cast their vote and leave it to be scanned when the machine is fixed. Yet, optical scan voting machines are not completely verifiable and depend on the integrity of the scanner. These machines are not foolproof and mistakes can go undetected if the voter is careless. Additionally, there is no way for the voter to confirm that their vote was tabulated correctly into the final results. In essence, once the voter inserts their ballot and confirms the machine read their mark correctly, there is no way of determining if these results were counted in the final tally. One security enhancement that has been used to prevent this fraud is Scantegrity, an open source election verification technology. Scantegrity provides end to end verifiability of election results using unique confirmation codes to allow a voter to prove to themselves that their ballot is included and unmodified in the final tally.

Overall, the existing flaws in the kiosk-style voting machines outweigh the benefits. On the other hand, the scantron-style input machine seems like a more promising option, with the biggest vulnerabilities in the design already identified and addressed through security enhancements like Scantegrity. Regardless of what technology is used, the general objective for a voting machine is clear: create the perfect balance between security and efficiency.

Solution and Future Work

The proposed robust voting machine is a paper-ballot-scanning system with multiple redundancy checks. The device features a kiosk style user experience with a hand-marked, Scantron-style input with a carbon copy for venue-level auditing. Also, there will be machine-level auditing that stores the original copy of the Scantron paper. The machine allows voters to verify their votes using confirm and cancel indicators. The multiple redundancy checks restrict a voter from voting multiple times. This new voting machine is useful for post-election audits, ballot accounting and reconciliation, and ensuring voter-verified paper audit trail by using a hand-marked process.

Vote Safe, the voting machine proposed, would operate similarly to a Scantron, which is a testing system used in many schools that entails a paper sheet with bubbles that can be filled in by pencil and read by a machine. The machine reads which bubbles are filled in and can determine which answer choice is selected; in this instance, the voting machine will scan the ballot and detect which candidate's bubble has been filled in by the voter. The change to the existing voting experience would be minimal. A voter would enter a voting center checking in as per state code, be given a ballot with a carbon copy paper attached. The carbon copy paper serves as the first set of a paper trail. They would mark their vote on the paper ballot with bubbles next to each candidate's name, hold onto the carbon copy, and feed the actual ballot through the machine. The machine would then display the user's vote to confirm their decision. If the vote is approved, it will be recorded in the voting machine. The original copy will be stored in the device, and the carbon copy will be given to a voter attendant who will store the copy in another location. If the vote is not confirmed, the machine would reject the ballot. The voter will need to seek a new ballot from the voter attendant and restart the process until they verify their vote. This makes for 3 points of redundancy and leaves a 3-point paper trail. A paper trail can be used to verify that the machine registered the intended vote. This will not affect existing voting centers, except for the auditing process. A movement to use such a device will highlight the shortcomings of the current voting process and push awareness for rolling out these types of devices throughout the nation.

In future iterations of Vote Safe, the software should also be made more secure by adding decentralized global counting or having reliable local counting. There should be accessibility features such as a Braille reader, large buttons to confirm or cancel the vote. Automatic scantron filler for disabled citizens, and county-level vote count decentralization.

Overall, Vote Safe is a compromise between electronic and paper voting. Vote Safe's multiple points of redundancy reduce the risk for software and physical vote tampering. There are numerous points of audits and inexpensive to implement. Vote Safe is immune to large scale attacks because it is localized. Finally, the learning curve to use Vote Safe does not require a new skill. It is easy to use and secure. The final design of this voting machine should be handled by the NSA and DHS, given that they are experts in cybersecurity, which is crucial in voting infrastructure.

Assessment of Related Election Security Work

In response to the cyberthreats posed during previous elections, the following is a comprehensive assessment of new election security research and programs, including Google Tools, Election Security Preparedness, Election Infrastructure Security, Cyber Security Campaign Playbook, and The Brennan Center.

Google Jigsaw, a unit within Alphabet, forecasts and confronts emerging threats, creating future-defining research and technology to keep our world safe. Google Jigsaw created Protect Your Election, a free online tool kit to help online users protect election information from digital attacks by helping users stay informed about misinformation and safeguarding their online accounts. Protect Your Election provides tools for individuals running campaigns, candidates themselves, webmasters, news sites, and journalists.

Protect Your Election offers a service that defends news, human rights, and election monitoring sites from DDoS attacks through their Project Shield initiative. Through Google's Advanced Protection Program, you can teach your devices to filter through phishing campaigns, safeguard your data by limiting access to it, block unknown apps, and block fraudulent account access with extra verification. Other resources that Google provides are fact-checking websites or software and other verification tools to make sure the user is receiving accurate information.

The US Election Assistance Commission (EAC) is an independent, bipartisan commission responsible for overseeing various aspects of the election process including the certification of the voting system, maintaining the mail voter registration form and the use of audits. The election officials in EAC have collectively worked to improve the current US election system through various means.

Their Election Security Preparedness program emphasizes the collaboration between all jurisdictions within the US government to spread awareness of how to create a more secure election standard. The EAC provides more resources on maintaining voter security, the importance of using various voting technologies, and cybersecurity training manuals for the general public and government officials. Their initiative heavily focuses on the importance of using audits in elections.

The Cybersecurity and Infrastructure Security Agency (CISA) is a national risk advisor, working with different companies and governments to build secure infrastructure and provide clients with various cybertools to ensure cyber protection. In regards to national election security, CISA started the initiative "#Protect2020", working directly with the US government to manage any risks posed by evolving threats to the current election infrastructure. The goal of

“#Protect2020” is to preserve the physical and cyber security of the current system and restore American’s trust in the voting process.

To address the insecurities of the various state’s standards for voting, CISA will initiate cybersecurity assessments, which include phishing campaign assessments and vulnerability scanning for various jurisdictions. CISA will also work to provide detection and prevention of cyberthreats through extensive malware analysis; in addition, spread awareness about election threats through information sharing programs and homeland security networks. Finally, CISA will present training and career development courses to educate others about this national initiative to secure the election system.

The Belfer Center for Science and International affairs at the Harvard Kennedy School created a Cybersecurity Campaign playbook through their Defending Digital Democracy project to spread digital tools to campaign leaders. The Cybersecurity Campaign playbook details how vulnerable campaign environments can be in the face of digital threats. The playbook continues to inform its audience on how to manage their cyber risk and secure their campaign through preparation and planning.

The content highlighted in Defending Digital Democracy’s playbook highlights managing human risk, internal communications, devices, networks, and incident response planning. The playbook is written by a bipartisan team of experts in cybersecurity, politics, and law to provide simple, actionable ways to counter the growing cyber threats.

The Brennan Center for Justice created an election security resource in response to the 2016 Russian cyberattacks that left U.S voting systems vulnerable. The Brennan Center acknowledges that hackers conducted “research and reconnaissance” against election networks in all 50 states and breaches at least one state registration database while attacking local election boards and infecting the computers at a voting technology company.

The Brennan Center of Justice Election Security resource looks at voting machines and infrastructure, responding to the coronavirus, post-election audits, and how to fund election security. Lastly, the Brennan Center has put together the H.R. 1: Democracy Reform act by highlighting that the act would streamline voter registration, fix campaign funding system, end partisan gerrymandering, update aging voting infrastructure and strengthen ethics rules.

The current election security work is extremely beneficial in spreading awareness about the need for greater measures to be taken for the security of US elections, and is a step in the right direction. Although the 2020 election will inevitably be affected by the coronavirus pandemic - this unforeseen emergency was not mentioned in the planning for the security work listed above. Therefore, it is worth noting that election security work should encompass all types of possible emergencies and provide alternative solutions for those instances. In addition, our current election security work must prioritize more advanced forms of inevitable cyberthreats (including, but not limited to, the malicious usage of artificial intelligence).

Conclusion

Although progress is promised through legislation to improve election security, more technologists and politicians can do to ensure American democracy is not to tamper. Democracy's beauty lies in the ability that people have to demand local officials to protect their votes and enact security reforms. Vote Safe is one iteration of many that can help improve election security across the nation, but it isn't the only solution. It is essential to do more beyond building Vote Safe. Local governments can look at related election security work to protect themselves from social engineering attacks, protect their digital assets by learning to secure their passwords or networks, and distinguish misinformation on the internet. Social media companies must continue to decrease malicious disinformation campaigns. Voting is a constitutional right. It's time for Congress and state governments to make election security a funding and educational necessity.ial, state cybersecurity experts, and the federal government. Together, people can demand that local officials protect the vote and enact more substantial security reforms, push for the Secretary of State and state legislature to pass risk-limiting audits, push for paper ballots and ensure the minimum security requirements. Together, election security can be transparent, reliable, and prepared for any potential attacks.

References

Abrams, A. (2019, April 18). Here's What We Know So Far About Russia's 2016 Meddling. Time. https://www.time.com/5565991/russia-influence-2016-election/

Coats, D., R. (2018). Worldwide threat assessment of the US intelligence community. U.S Intelligence Agency. https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Detrow, S. (2018, March 20). What Did Cambridge Analytica Do During The 2016 Election? Retrieved from https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election

Hess, A. (2017, February 28). How the Trolls Stole Washington. Retrieved from https://www.nytimes.com/2017/02/28/magazine/how-the-trolls-stole-washington.html

Jones, Douglas W., and Barbara Simons. “Election Systems and Software (ES&S) IVotronic.” Verified Voting, 2012, www.verifiedvoting.org/resources/voting-equipment/ess/ivotronic/#fnref-36503-1.

Mueller, R., S. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. U.S. Department of Justice. https://www.justice.gov/storage/report.pdf

Ney, Robert W. “H.R.3295 - 107th Congress (2001-2002): Help America Vote Act of 2002.” Congress.gov, 29 Oct. 2002, www.congress.gov/bill/107th-congress/house-bill/3295.

Prokop, A. (2019, April 18). *The Mueller Report, Explained.* Vox. www.vox.com/2019/4/18/18485602/mueller-report-findings-obstruction-russia-collusion.

Root, D., Kennedy, L., Sozan, M., & Parshall, J. (2018). Election Security in All 50 States. *Center for American Progress*. Retrieved from https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/

Shane, S. (2017, November 1). These Are the Ads Russia Bought on Facebook in 2016. Retrieved from https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html

Shoorbajee, Zaid. "U.S. Voting Machines Are Easily Hackable, DEF CON Report Says." CyberScoop, CyberScoop, 11 Oct. 2017, www.cyberscoop.com/hacker-convention-report-says-u-s-voting-machines-easily-hackable/.