VULNERABILITIES, VARIABILITY, AND REMEDIES: AN ANALYSIS OF
UNITED STATES ELECTORAL SYSTEMS SECURITY

by
Julia Ann Swafford

A thesis submitted to the faculty of The University of Mississippi in partial fulfillment
of the requirements of the Sally McDonnell Barksdale Honors College.

Oxford
May 2018

Approved by

Advisor: Professor Richard Forgette

Reader: Professor Tim Russell

Reader: Professor David Bath
Dedication

I dedicate this thesis to my parents, Carl and Lynne Swafford, who supported me in any venture I had in life. Thank you for raising me to be a great woman, daughter, and citizen. I will never forget the way you led by example how to serve others with your talents. I also dedicate this to idealists everywhere because the world has enough cynicism as is, and remember, it’s only sappy because it’s true.
Acknowledgements

I want to thank my parents and brother for their eternal support and love. My friends who have loved me through and stood by my side through the creation of this project and understood when I simply replied “can’t. thesis.” and took it upon themselves to get me out of the house. My dogs, Rosie, Hoochie, and Prissy, for reminding me of the outside world and giving unlimited cuddles and licks. Lin Manuel Miranda and Jeff Beal for writing the soundtrack to this rage fest of a thesis. And Ben Shapiro for just being the national treasure he is and reminding me to always speak truth to power, even when they don’t want to hear it and that facts don’t care about feelings.
Abstract

Elections in the United States are vulnerable on multiple fronts both physically and in cyberspace. In this paper four main vulnerabilities are discussed: voter rolls, political parties, social media, and voting machines. These four aspects of electioneering are particularly vulnerable due to their age, availability of unprotected data, and ease of misuse. This paper assesses the policy implications of deeming election administration as critical infrastructure by the Department of Homeland Security, and the proposed policy options focused on maintaining decentralization along with necessary upgrades provide adequate security to ensure the United States’ free and fair electoral process.
# Table of Contents

Dedication iii  
Acknowledgements iv  
Abstract v  
Introduction 1  
Chapter 1: History of Foreign Interference in United States Elections 3  
Chapter 2: What Happened In 2016 10  
Chapter 3: National Security Analysis of Electioneering 18  
Chapter 4: Policy Framework and Assumptions 33  
Chapter 5: Policy Recommendation 37  
Chapter 6: Conclusion 51  
Appendix A: Heart of Texas and United Muslims of America Facebook Interaction and Protests 52  
Appendix B: Facebook Ad Preferences Determine Political Affiliation to Tailor Advertising 53
Introduction

"Those who vote decide nothing, those who count the votes decide everything"

-attributed to Joseph Stalin

The 2016 U.S. Presidential election was the culmination of what many security experts felt was on the horizon. A combination of factors including aging voting machines, minimal regulation of social media, and increased utilization of the internet created an election system sufficient to accomplish its purpose of taking votes, but not necessarily to protect itself from manipulation. Electioneering goes beyond the voting machines and consists of cyber, personal, and social components.

This paper identifies vulnerabilities in the United States’ electoral process and elaborate how they are exploited. It is largely based on congressional testimony related to the 2016 election, political journals that provide background on the administrative aspect of election day, and primary sources in order to provide a comprehensive understanding of vulnerabilities and an assessment of security regarding the United States’ electoral process. It focuses primarily on administrative vulnerabilities on Election Day because Election Day has the largest concentration of electoral infrastructure that are likely targets.

Policy solutions are proposed in this paper to address specific security concerns. Many of these solutions utilize available resources. Congressional and state government legislative responsibility regarding elections are also discussed. The information in this paper is current to April 2, 2017.

This paper defines electoral inference in the United States’ electoral process as an unauthorized actor altering items and activities related to Election Day and includes infrastructure such as governmental or private databases containing voter information and
voting machines. Prior condition should act as the baseline for assessment of electoral interference because many states have not adopted best practices for voting machines and other aspects of electioneering.

False information dissemination (a.k.a fake news) will not be the focus of this paper, but will be mentioned as it relates to strategies of foreign and domestic actors and is also discussed as a case study for electoral tampering. It is also a crucial part of the sourcing for this paper, as most of the sources are a result of investigation into the 2016 Presidential election.
Chapter 1: History of Foreign Interference in United States Elections

Foreign nations conducting large scale electoral manipulation campaigns is not a recent phenomenon. In the earliest years of the United States, nations used timely politics in an attempt to affect election outcomes. In what might be the first October surprise in United States history, France’s ambassador to the United States published a decree in 1796 to restrict America’s trade with Europe. The ambassador went on to threaten that France would become an enemy if the United States continued its foreign policies, a reference to the election of John Adams (DeConde, 1958).

The first instance of electoral interference in modern history occurred in the 1940s by British Secret Intelligence Service (SIS). The goal of this interference was to elect politicians, hopefully a President, that were pro-US involvement in World War Two (Usdin, 2017). Prime Minister Winston Churchill oversaw this operation on a global scale, but focused on the United States as Churchill knew there was a slim chance of British victory in World War Two without US involvement or aid.

SIS operated in America with the British Security Corporations (BSC) as a front, and conducted a variety of espionage and propaganda missions. Through the declassification of BSC’s history and operations in 1999, it became known SIS frequently engaged in forgeries, seductions, burglaries, physical surveillance, intercepting and reading letters sent under diplomatic seal, illegally bugging offices, and tapping phones. This went as far as “British intelligence even listened in on a telephone call in June 1940 between President Franklin D. Roosevelt in the White House and his ambassador to Britain, Joseph P. Kennedy Sr. A report on the call was quickly relayed to Churchill, alerting him that the U.S. was making contingency plans in case the U.K. fell to the Nazis” (Usdin, 2017).
Covert influence operations against isolationist candidates were a staple of SIS at this time. Most of the rumor dissemination, a precursor of the fake news of today, occurred in the newspapers through reporters friendly with the government. While Britain openly supported President Franklin D. Roosevelt, they began to utilize their media connections to ensure the Republican candidate would be willing to join the war as well. Leading up to and throughout the Republican convention, BSC published false polls stating three-fifths of GOP delegates supported helping the allies with everything short of war (Usdin, 2017). The Underground Propaganda Committee would approve circulated rumors and disseminate them to friendly reporters stateside.

Nazi Germany also attempted interference in the United States election of 1940. In an attempt to derail the reelection of FDR, they bribed a US newspaper to leak an acquired Polish document framing the President as a warmongering criminal (Farago, 1973). This came to be known as the “October Surprise” of that campaign season. It is unlikely this had any impact due to FDR’s popularity and incumbency.

Some nations choose to take advantage of crises in order to influence an election outcome. One such case was in 1960 in the Kennedy vs. Nixon election. The Soviets originally approached the United States’ Ambassador to the United Nations and multiple time Democratic presidential candidate, Adlai Stevenson II, and offered him propagandic support if he ran in 1960. He declined to run (Taylor, 2017). When John F. Kennedy became the clear Democratic nominee, Soviet Premier Nikita Khrushchev chose to back him instead of the incumbent Vice President Richard Nixon. This was likely due to an embarrassing moment Khrushchev had with Vice President Nixon.
A year prior in 1959, Nixon and Khrushchev shared a series of exchanges, which have become known as the Kitchen Debate. The two men were touring a sample American home meant to display the merits of the western economy in Russia. The exhibitors claimed that anyone in America could afford the home. As Nixon and Khrushchev entered the model kitchen, they began to discuss the merits of capitalism over communism by debating if the typical Russian or American home displayed the values of their respective economic systems using objects in the house as metaphors. Khrushchev walked away from the exchange insulted and belittled by Nixon’s seemingly jovial and dismissive tone.¹

Matters became worse as the election became closer. On May 1, 1960 Russians shot down U2 pilot Francis Gary Powers, who was sentenced to a decade in prison for espionage. In July, the Russians shot down an RB-47H and captured two pilots, John R. McKone and Freeman B. Olmstead. The Soviets chose to imprison the two pilots. The Air Force pilots were released on January 25, 1961, days after Kennedy’s inauguration. Khrushchev commented on the timely releasing of the pilots in his memoir, stating:

My comrades agreed, and we did not release Powers…As it turned out, we’d done the right thing. Kennedy won the election by a majority of only 200,000 or so votes, a negligible margin if you consider the huge population of the United States. The slightest nudge either way would have been decisive (Khrushchev, 234, 1970)

It appears Khrushchev’s motives were not solely to rid his country of spies, but rather to influence the American presidential race’s outcome.

Kennedy and Khrushchev’s acknowledgement of the event’s influence on the election has changed multiple times. While Khrushchev states in his memoir that the Russians “casted

¹ Transcript can be located at https://www.cia.gov/library/readingroom/docs/1959-07-24.pdf
a vote” for President Kennedy, former Soviet Ambassador Oleg Troyanovsky recalls Kennedy stated, “‘I don't think it affected the elections in any way’” (Taylor, 2017).

In the past, foreign governments have communicated with Presidential campaigns. Often, this led to a change in policy or foreign governments abstaining from a course of action. One such case was the election of 1968 during the Vietnam War. President Lyndon Johnson sought to increase the popularity of his administration to boost Vice President Hubert Humphrey’s election prospects. In October, the President announced the cessation of bombing in the War along with renewed peace negotiations. Shortly after, Vice President Humphrey led Richard Nixon by 3 points (Zeitz, 2016). This was shortly undone by the Nixon campaign.

The South Vietnamese government later consulted with the Nixon campaign through Anna Chan Chennault, co-chair of Republican Women for Nixon and confidante of South Vietnamese President Nguyen Van Thieu (Zeitz, 2016). Chennault’s goal was to convince the South Vietnamese that a Nixon Administration was better than a Humphrey or Johnson one. The Nixon campaign quickly realized if they could persuade the South Vietnamese to stay away from peace talks, the three point lead might close.

The conversations between the South Vietnamese and Nixon campaign did not remain a secret. According to historian Josh Zeitz:

Incredibly, Lyndon Johnson and Hubert Humphrey knew of Nixon’s maneuvers. The National Security Agency intercepted cables between Thieu and his ambassador in Washington, D.C. (“[I am] still in contact with the Nixon entourage, which continues to be the favorite despite the uncertainty provoked by the news of an imminent bombing halt,” one communiqué began.) On the basis of these cables, LBJ ordered
the FBI to tap Chennault’s phone; the bureau, in turn, concluded that she “contacted Vietnamese Ambassador Bui Diem and advised him that she had received a message from her boss (not further identified) which her boss wanted her to give personally to the ambassador. She said the message was that the ambassador is to ‘hold on, we are gonna win’ and that her boss also said, ‘Hold on, he understands all of it.”’

Despite the President and Vice President’s views that the communications with the South Vietnamese were treasonous and a violation of the Logan Act\(^2\), President Johnson chose to keep the taps private due to the lack of a smoking gun and they were hesitant to explain to the American people why US intelligence agencies tapped the campaign (Zeitz, 2016). Ultimately, the South Vietnamese pulled away from the negotiating table and Nixon won the election by less than a percentage point.

Some believe a similar use of political maneuvering occurred in the Reagan vs. Carter election in 1980 surrounding the Iranian Hostage Crisis (Lewis, 1991). They cite the release of the hostages twenty minutes after the completion of President Reagan’s inaugural address as evidence Iran preferred a Reagan administration to a Carter one. Several notable individuals including former Iranian President Abulhassan Banisadr and former naval intelligence officer and U.S. National Security Council member Gary Sick stand by the allegations (Lewis, 1991). However, a ten-month investigation by the House of Representatives revealed, “virtually no credible evidence to support the accusations” (Hamilton, 1993).

\(^2\) Passed in 1878. Forbids unauthorized persons from negotiating with foreign governments on behalf of the United States. Last indictment occurred in 1852. 18 US Code § 953
The infiltration of political parties is a tactic foreign governments have used or attempted to use for decades. The methodology seen there is not incredibly different from that of today: propaganda, illegal financial contributions, and front groups were trademarks of active election inference. Two incidents of note have occurred in the past 50 years: the 1984 attempts by the Soviet Union and the 1996 attempt by the Chinese.

Yuri Andropov, the chairman of the K.G.B, directed intelligence operatives to prevent the reelection of President Ronald Reagan by starting rumors and undermining rival groups. Russian defector and former KGB officer Vasili Mitrokhin turned over notes stating Russian intelligence attempted to infiltrate the headquarters of both parties (Osnos, 2017). They also pushed the campaign slogan “Reagan Means War!” to discredit the President as a warmongering leader (Schweizer, 2003).

In February 1997, the FBI announced they unearthed evidence of the Chinese government attempting to illegally donate money to the Democratic National Committee. The FBI received electronic intercepts between Beijing and their US embassy carrying a plan of channeling $2 million to US campaigns. There was disagreement whether the money was targeting congressional or presidential races, and the criticism surrounding the Clinton administration was that the President was willing to do everything for better Chinese/US relations, including overlooking the illegal activity (Harris, 1997). Senators briefed by the FBI stated there was no evidence the plan was carried out, and both the US and Chinese government denied the allegations.

While it seems these actions did not determine electoral outcomes, they were blatant attempts to take advantage of circumstances to shape an outcome. The instances of blatant spying or wiretapping are recent revelations, so it is difficult to take any legal action on them
now. What makes these instances different than what the United States is currently experiencing is public awareness of foul play. In the next chapter, I will introduce a case study of the 2016 election, which will provide information on the current hallmarks of electoral interference.
Chapter 2: What Happened In 2016

The inauguration of President Donald J. Trump occurred under the auspice of a rigged election and a cloud of foreign collusion. The subsequent investigation by the Department of Justice, particularly Special Counsel Robert Mueller, remains an issue the Trump administration handles on a daily basis. This chapter focuses and summarizes what the Department of Justice and Congress confirms as efforts to interfere in the United States’ electoral processes. These efforts include the targeting of state owned voter registration databases, the hacking of the Democratic and Republican National Committees, and the use of social media to direct opposing sides into conflict with one another.

Three hallmarks exist throughout and tie these efforts together: a multimodal strategy governed by a mentality of “try it and see how far you can go,” the use of third parties to maintain deniability or take advantage of the reputation of the distributor (e.g. WikiLeaks), and the goal of discrediting the free and fair American process of elections. This served the purpose of the Kremlin well and led to the embedding of discord between a majority of the American populace. This chapter will focus on the three, confirmable instances mentioned above and display how they embodied the Russian approach.

It appears anyone who attempted to infiltrate voter registrations only did so when there was an obvious vulnerability or weakness. Connie Lawson, President of the National Association of Secretaries of State, testified to the Senate Select Committee on Intelligence (SSCI) as many as twenty states were probed (Russian, 2017). After two instances of unauthorized access, the Intelligence Community began reaching out to the states to provide support.
On August 18, 2016, the Federal Bureau of Investigation issued a nationwide “flash alert” to warn states regarding foreign infiltration of voter registration databases. The flash confirmed the infiltration of two states, later discovered to be Arizona and Illinois (Paganini, 2016). This warning strongly encouraged states to boost their cyber security, perform hygiene checks, and reach out to the FBI and DHS for support. Former FBI Director James Comey confirmed the FBI’s findings September 29th when testifying to the House Judiciary Committee (Oversight, 2016).

It is not known the exact origins of these cyber-attacks on Arizona and Illinois, as the IP addresses from these attacks trace first to the Netherlands, then through Ukraine, and are an otherwise indeterminable origin (Russian, 2017). The Intelligence Community has assessed with high confidence, however, it is almost certain these attacks sourced from Russia or Russian paid actors under the direction of President Vladimir Putin (Assessing, 2017). ODNI and the Secretaries of State confirm there were no election day reported incidents and no hacks on vote tallying equipment or technology.

The strategy of casting a wide net occurs throughout Russian strategy towards elections, but this philosophy is best exemplified in these cyber-attacks on voter rolls. Actors probed over a third of the United States’ voter rolls and spliced them down to two with exploitable vulnerabilities. It does not appear these states were targeted individually, but rather ruled out by elimination. Arizona and Illinois are not as electorally valuable or volatile as Ohio or Florida, so this gives the “phishing expedition” a more exploratory rather than attacking nature. In the Mueller indictment, there is a noted strategy shift once Russian operatives on the ground in Texas are introduced to the concept of “purple states” a.k.a.
states that are historically undecided in elections (U.S. v. INTERNET RESEARCH AGENCY LLC, 2018).

An attack of this kind casts doubt on a crucial part of election day itself. The voter rolls are by definition a list of everyone who is and is not allowed to vote. Voters feel if someone gained access or the ability to add or delete people from these lists, their vote is essentially meaningless. The compromising of a crucial part of election day operations feeds the narrative of a rigged election decided by anyone but the actual voters, which is a sentiment many Americans resonate with.

The most blatantly political move of Russian electoral interference was the hacking and distribution of emails from the Democratic National Committee and Democratic Congressional Campaign Committee. While the counterpart Republican Committee also experienced hacks, the Russians did not obtain much information, target as many individuals within the building, or distribute data as widely (Shelbourne, 2016). It is likely the Russians sought to discredit Secretary Hillary Clinton’s campaign and release information damaging to her legitimacy as a candidate.

In the summer of 2015, hacking group Guccifer 2.0, affiliated with Russian intelligence, gained access to the DNC servers. An FBI agent reported the suspicious activity to the DNC in September of that year, identifying the hacker as Russian operatives. The agent was transferred to a tech-support contractor at the help desk, who made a cursory check of DNC server logs and did not reply to follow-up calls from the FBI agent, allegedly because of a belief that the call might have been a prank (Lipton, 2016). The Russians maintain access of some kind until July of 2016 after multiple releases from WikiLeaks.
The General Staff Main Intelligence Directorate gained access to the DNC in April of 2016 through affiliated hackers Cozy Bear and Fancy Bear. By the end of the month, the DNC’s IT alerted the FBI of suspicious activity and hired a private security firm to investigate (Bump, 2017). Around this time, Russian hackers gained access to the email account of the chairman of the Clinton campaign, John Podesta\(^3\), through a phishing attempt requesting a password change.

The first leaks occurred on July 13\(^{th}\), 2016, when Guccifer 2.0 releases 10,000 names of Democratic donors and a list of quotes from Sarah Palin (Uchill, 2016). Five days later, Guccifer 2.0 leaked 20,000 names of Republican donors and opposition research on President Trump. July 22\(^{nd}\) was arguably the most impactful leak: 20,000 emails released on WikiLeaks from seven DNC officials implying the party’s favoring of Secretary Clinton over Senator Bernie Sanders (Bump, 2017). Following both leaks, DNC Chairwoman Debbie Wasserman Schultz resigned July 24\(^{th}\).

These leaks in particular embodied the hallmarks of the use of third party hackers and distributors. Guccifer, Fuzzy Bear, and Cozy Bear are all affiliated with the Russian government but maintain an ambiguous nationality and allegiance. It appears they are hired and then directed by Russian intelligence to carry out operations. This could be for purposes of deniability or to deflect US intelligence’s efforts to trace the cyber-attacks.

WikiLeaks was the chosen outlet for the July 22\(^{nd}\) email release and Russia maintained a relationship with them throughout 2016. RT, formerly Russia Today, renewed WikiLeaks Founder Julian Assange’s broadcasting contract and is the only Russian media company to do so. Assange frequently appears on the network to denounce the United States.

\(^3\) See pg. 22 for screenshot of email
Russia likely chose WikiLeaks due to “its self-proclaimed reputation for authenticity” (Assessing, 2017). Multiple reports quote officials close to the matter confirming the authenticity and accuracy of the leaked emails.

Foreign content began to grow across social media outlets throughout the summer and fall of 2016. The Russians bought numerous ads from social media outlets with targeted audiences. While social media are cooperating with the Mueller investigation, it is unclear if they are divulging the full expanse of information. This could also be due to the deletion of data related to these ads. It is unclear if this was accidental or purposeful in nature.

The Russians, through the Internet Research Agency (IRA), mainly used Facebook in two ways: ad buys or creation of events and groups. On November 19th, 2017, President Barack Obama asked Facebook CEO Mark Zuckerberg to take the company’s role in fake news and the Russia ad buys seriously. Zuckerberg responded that fake news was indeed an issue, there was no easy solution, and called the ad’s role in the election “crazy” (Entous, 2017). On September 6th, 2017, Facebook admitted selling advertisements to Russian companies seeking to reach the 2016 U.S. election audience and formally begin their cooperation with the Mueller investigation (Entous, 2017).

Facebook has gradually revealed the page’s and ad’s content. Some confirmed instances include a protest in Texas⁴, a Black Lives Matter ad targeted to Ferguson, MO and Baltimore, MA, and a picture of a black female holding a rifle (Dwoskin, 2017). The intent of these ads was to excite polarizing political attitudes. Most of these pages were issue based, a theme that carried over to other social media outlets like Twitter.

---

⁴ See Appendix A
Beginning in the summer of 2015, IRA affiliated Twitter accounts began to praise President Trump much more than any other candidate. Some of these accounts were issue based, like @march_for_trump, others were an attempt to deceive readers they were legitimate news sources. @TEN_GOP, a slight deviation from the real @TNGOP, was a Russian account with hundreds of thousands of followers.

There are select examples of these ads available in public record, but for the large part they remain the property of the individual social media companies or evidence in an ongoing Department of Justice Investigation. New disclosures provided to Congress by digital social media companies indicate that Russian agents during the campaign placed 1,000 videos on YouTube, 131,000 messages on Twitter, and, via 170 accounts, 120,000 items on Instagram (Shane, 2017). The question the Department of Justice is striving to answer is no longer these ad’s existence, but their impact.

While President Trump was the most obvious recipient of Russian support, Senator Bernie Sanders and Dr. Jill Stein also received favorable coverage or advertisements from the Russians. This is because one of the Russian’s goals was not to elect President Trump, but to prevent Secretary Clinton from winning the presidency. The Intelligence Community assesses this was due to, “…[Putin] has publicly blamed her since 2011 for inciting mass protests against his regime in late 2011 and early 2012, and because he holds a grudge for comments he almost certainly saw as disparaging him” (Assessing, 2017). Secretary Clinton was not the only negatively targeted presidential candidate, as Senators Ted Cruz and Marco Rubio were also attacked as the two Republican frontrunners behind President Trump. The

---

5 A large number of ads and their content were released by Special Council Mueller in his indictment of IRA after this was written. They follow the same patterns mentioned throughout this chapter. The indictment can be found at https://www.justice.gov/file/1035477/download
Russian’s favorability towards President Trump arose from a history of stronger Russian relations with states that had and shared business internets in and with Russia (Assessing, 2017).

On February 16th, 2018, Special Counsel Robert Mueller indicted the IRA along with thirteen Russian nationals for engaging in, “…operations to interfere with elections and political processes” (U.S. v. INTERNET RESEARCH AGENCY LLC, 2018). The thirteen Russians either financed, created business fronts, or were employed by IRA. They were charged with one count of conspiracy to defraud the United States, one count of conspiracy to commit wire and bank fraud, and five counts of aggravated identity theft. The actual information contained in the indictment was known for some time, but the indictment served to confirm specifics and prove the claims were legally actionable.

Some legal scholars are predicting the Special Counsel will use the Foreign Agents Registration Act of 1938 to prosecute the individuals listed in the indictment. According to the Department of Justice, it “requires persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities” (FARA, 2018). While this is could be a tool used to prosecute the individuals mentioned in the indictment, there are challenges in suing the IRA under this legislation. Namely, the question of if the social media ads and bots the IRA created were acting in a political or quasi-political nature.

One defense could be a comparison between campaign finance laws governing political vs issues ads. While political ads must carry an endorsement and usually contain
specific names or words\textsuperscript{6}, issue ads are not specifically tied to electioneering. Anyone can purchase an issue ad without disclosing the funder or creator of the content. If the Special Counsel pursues charges under this legislation specifically, they will have to prove the Russians were not creating just issue ads and were endorsing candidates, which makes the ad political by definition.

This indictment likely means the Special Counsel will hand down similar charges against the unnamed co-conspirators frequently mentioned in the original indictment. The investigation is still ongoing, so further counts could be handed down to campaign workers or other Americans or Russian citizens. It mainly crystalizes and summarizes the investigation to this point and allows the DOJ to prosecute the named individuals. What happened in 2016 is becoming clearer as time goes on, and the Mueller indictment is the first step in understanding the scope of Russian action and electoral vulnerabilities in the United States.

The next chapter discusses specific vulnerabilities exploited during the 2016 election. These issues were a concern before the 2016 election, but I will show that the intensity of Russia’s attacks require these problems to have immediate resolution. The evidence in the next chapter mostly consists of Congressional testimony and primary, informative sources.

\textsuperscript{6} Examples include “endorse, vote for, mention of candidate names. Political ads are also required to disclose their funder (campaign or PAC) and the candidate it endorses must approve the message.
Chapter 3: Analysis of Electoral Systems Security

Key Findings

Voting commissions’ reliance on cyber infrastructure along with a lack of consistent administrative and oversight processes create vulnerabilities that actors could exploit to influence electoral outcomes and public opinion in the United States. These vulnerabilities exist in four areas: state owned voter registration databases, political parties, social media, and voting machines. Enemies of the United States likely will continue to seek access to State owned voter registration databases (hereafter referred to as voter rolls) to cause chaos, which causes loss of faith in the United States’ electoral process and government, and to influence the outcome of elections.

Foreign and domestic enemies of the United States are almost certainly going to target political parties, political action committees (PACs), or Super PACs. These databases are easily accessible due to a lack of compliance with Intelligence Community best practices and contain data that can be used to create predictability models in order to identify vulnerable counties and voters in order to influence an electoral outcome.

The exploitation of social media will probably continue to be the most commonly used method of foreign and domestic electoral influence through false information dissemination. Social media is an economical and efficient way to reach a wide audience. Knowledge of how algorithms push a story’s presence in feeds enables an actor to create false accounts and bots to push the story to be in a targeted individual of a certain demographic’s feed.

Security of vote tallying equipment is adequate to ensure reliable counting of votes. The physical security of United States’ voting machines is robust due to the adoption of best
practices such as lack of internet connectivity for the machines, decentralization of elections, and widespread use of audits and paper backups. The age of machines poses a threat to the security of votes and the limited number of voting machine vendors is a vulnerability that could compound as more states seek to purchase new equipment.

The security of the United States electoral process is not sufficient to withhold the effort of foreign and domestic actors seeking to influence the electoral outcome. Russia and other foreign actors’ successes in infiltrating the electoral process including voter rolls, political party databases, along with the deliberate misuse of social media algorithms and other means of communication such as email show current insufficiencies.

It is almost certain Russia took part in the electoral interference of 2016, but IP address traces and investigations lead to third party vendors the Russians possibly contracted out. Back traces often lead to countries like Ukraine or Latvia, but it is doubtful these countries are the source of attacks. Countries that would have interest and ability to carry out the attacks elaborated below include Iran, North Korea, China, and Russia. Domestic actors could also carry out these kinds of attacks, either inspired by other groups or acting as a lone wolf.

**Voter Rolls**

Voter rolls are the most electronically accessible part of Election Day. A voter roll contains the names of all people in a county or precinct who are eligible to vote, along with some basic identifying information such as the last four digits of Social Security numbers and dates of birth, which is concerning to many security officials and is a breach of privacy if accessed illegally (Kopan, 2017). While most of this information is open source and
available to the public, other information stored with one’s voter registration is private and, in some states’ case, the public is notified when it is compromised.

Some states have laws in place that require state governments to notify victims of a breach of personal information once its discovered. According to the Executive Director of the Illinois State Board, the Board notified the Illinois General Assembly of the breach occurring in the 2016 election in accordance with the state’s Personal Information Protection Act (Russian, 2017). This is how the public first came to know of foreign interference in their voter rolls and caused the populous in state’s with a lack of such laws to wonder if they were targeted too.

These voter rolls are not well protected because the information within them is not particularly sensitive. Senator Roy Blunt remarked in the Senate Intelligence Committee (SSCI) on July 21st, 2017 that voter rolls are incredibly accessible and contain mostly public information, which is why they are usually strongly protected (Russian, 2017). The reason people fear actors gaining access to this information illicitly is the combination of this data with other data in models to create useful intelligence.

The hacking of voter rolls accomplishes two common goals for many enemies of the United States. First, it causes chaos and loss of faith in the electoral process. Senator Rubio recalled voters throughout his campaign approaching him to ask “Is my vote going to count? Or do the Russians choose instead?” (Russian, 2017). People become scared when they feel someone outside the voters has control of the election. This drives down turnout and can in extreme instances, sway the outcome of an election.

Second, access to these voter rolls to the point of adding or deleting people creates chaos by forcing poll workers to address these cases individually. Although states are
required to provide a provisional ballot, these still require a great amount of attention. Length of lines along with the appearance of disorganization and lack of integrity become concerns.

The fear regarding access to voter rolls is massive deletions, which cause logistical delays. Indiana Secretary of State Connie Lawson explained in her testimony to SSCI, “the biggest danger is the line to the polls would increase significantly if a large number of folks in each precinct had to do handle that.” While it seems that long lines are typical of an Election Day, if these delays are not organic and are the result of interference, the issue changes face. If these deletions occur, citizens who have the right to vote and are registered to do so may not be allowed or counted, which becomes a breach of constitutional rights.

One could certainly change vote outcomes of an election indirectly by adding or deleting people with certain voting patterns or characteristics. A voter roll also contains information on prior election turnout. That information combined with available, open source information is often used to predict behavior for the upcoming election.

An example of a database that combines voter roll data with third party data is RNC Trust. The Republican National Committee owns and operates it and is accessible for a fee. According to Michael Sullivan, Executive Director of the Tennessee Republican party, it contains variables such as “financial data, election priors, turnout statistics, Amazon purchase history, vehicle and property purchasing history” (Sullivan, 2017). News agencies also use models like these in their polling. According to Chris Stirewalt, digital political editor for Fox News, these data points formulate models that determine likelihood of turnout, issues of critical importance to voters, and take into account factors such as locale and local current events (Stirewalt, 2017).
Using predictability models and prior election results to determine key, winnable counties in elections is common practice among all campaigns. Senator Angus King remarked in a SSCI hearing, “a sophisticated actor could hack an election simply by focusing on particular counties” (Russian, 2017). The fear of access to these voter rolls is someone could selectively choose where to target and change the election outcome indirectly.

By adding or deleting people of a certain background, an outside actor could influence the outcome of an election indirectly. This could occur on a small, precinct level or on the national level through the careful selection of counties in a targeted state (Norden, 2017). Current trends show it is unlikely a single county would be targeted, but rather actors would cast a wide net consisting of multiple electoral manipulation strategies. With about even odds this will continue into the future due to some group’s success with some strategies and the growing scope and capability of these groups.

Lack of a clear target was common among many electoral influence efforts in the 2016 election. Assistant Director of Counterintelligence Division of the FBI, Bill Priestap testified to the SSCI he believed Russian actors sent phishing emails to multiple people in the hopes just one would click on it to allow access (Social, 2017). A similar strategy of casting a wide net to see what was out there is seen through the hacking of non-state entities, like PACs.
Above: the phishing email sent from Russia Clinton campaign Chairman John Podesta received in April, 2016

**Political Parties**

Political parties purchase voter rolls as well as third party vendors’ data such as vehicle purchase history, history on landowning’s, Amazon purchase history, and use other open source tools like Google Analytics to predict voter behavior. Political parties often contract out their data modeling works to marketing analysis companies. Firms hacked in 2015 and 2016 possessed, “modeled data about a voter's likely positions on 46 different issues ranging from ‘how likely it is the individual voted for Obama in 2012’, ‘whether they agree with the Trump foreign policy of ‘America First’” and ‘how likely they are to be concerned with auto manufacturing as an issue’, among others.” (Uchill, 2017)

Once a party creates this database, often with 3000+ variables per person, they use it to form predictive models for counties and states. According to Chris Carr, Political Director at the Republican National Committee, these models and data caches are used to determine where to send grassroots and groundwork workers and to better profile the right people to send to a certain city or county (Carr, 2016). A foreign or domestic actor could not only utilize this data to steal the identity and track patterns of many American citizens, but also identify crucial counties that will likely determine the outcome of an election.
Political parties are also vulnerable due to their close relationship, yet separation from the government. Political parties file as SuperPACs with the IRS and are not subject to additional regulations outside that of a normal PAC. While parties often have internal IT, and it is reliable, vulnerabilities still exist because their standards are defined internally rather than set to meet security levels that would match something similar to the United States Congress.

Political parties appear to have ignored the advice of some officials in the Intelligence Community. One of the more memorable quotes from the 2016 DNC investigation was from Secretary of Homeland Security Jeh Johnson, stating he wishes he would have “slept outside the DNC” for them to take the threat seriously.

Who the parties choose to contract out to is also a cause for concern as these contractors rarely work solely for political means, rather they also conduct market and television research. Although this data is mostly open source and available for purchase, vulnerabilities exist when this data cannot be secured, especially when it is compiled and packaged in the way it currently is to political parties and campaigns.

Social Media

Social media and search engines aim to connect people and make information accessible, but oversight is lax. All social media corporations have terms and conditions, which require a real person to create content for the account. Violation of these terms can result in account suspension or ban, mostly detected by algorithms taking note of frequency of tweets or consistency in large volume out of a location.

All social media platforms present similar mission statements: a combination of community building, enjoyment with people and ideas, and to serve as an accessible platform
for information. Facebook, Alphabet, and Twitter’s general counsels all testified in accordance with these values to the Senate Intelligence Community in November 2017. As of October 2017, social media did not have a formal ban on spreading false information. However, many accounts that engaged in these activities were shut down due to violations of other terms and conditions such as inauthenticity or use of bots (Social, 2017).

This misuse of social media created divisiveness between political factions in the United States. Pages accumulated followers of similar ideals i.e. Heart of Texas on Facebook. The page’s owners published ordinary and non-political content such as Bible verses and other phrases and occasionally published a politically oriented post. This prevented many accounts from earlier detection, as the focus is typically on abnormalities volume that trigger suspicion the account is not authentic.

Often someone would create two, antagonistic groups and Facebook events and publish them once the pages gained a large enough following. Next, the pages would produce posts in order to inspire protests, counter protests, and other gatherings. Facebook conducted an internal audit and was repeatedly asked while testifying in the House and Senate what the goals of these actors were. Colin Stretch, Vice President and General Counsel of Facebook stated, “these foreign actors sought to drive people apart” (Social, 2017).

These ads impact is limited in scope. It appears there is little pattern for how a location was chosen to receive an ad and, if there was, it seems individuals with an inadequate understanding of the United States’ electoral scene made the choice. States that have not changed parties since the 1980s were targeted rather than tossup states and the

---

7 See Appendix A
8 Some exemptions exist including the attempted Florida rallies and ads in Ferguson, MO and Baltimore, MD. Refer to US v. IRA indictment.
actual views these ads and pages received were limited. The goal was to sow discord and to excite both parties’ bases, rather than change a voter’s opinions. Social media ads are also inexpensive compared to other advertisements, especially in unpopulated parts of the country, so actors are not extremely concerned about effectiveness.

Data predictability modeling, such as that used by both political parties, makes it easy to determine which counties can influence an election’s outcome. It does not appear these counties were selected. Chairman Richard Burr of the SSCI pointed out, “Five times more [social media] ads were target at the state of Maryland than of Wisconsin…And Maryland was not up for grabs…the three most heavily targeted states in America: Maryland, Missouri, and New York were all determined by eighteen point margin and two turning to Hillary Clinton” (Social, 2017). It appears these ads were not designed to change opinions, but rather to fire up bases of each political party.

Ben Shapiro is the editor in chief of a conservative, opinion based media outlet named The Daily Wire. While the outlet is prominent, it does not have the household recognition Fox News or MSNBC does. In an episode of his podcast, he noted the Russians had around 150 million engagements in a year on Facebook in the election, while his weekly reach averages approximately 30 million (Shapiro, 2017). While this suggests more people know about the ads through the news rather than through seeing them firsthand. The question then becomes if the ads served their purpose if they were not wide spread.

One reason the distribution was not effective or selective may have to do with cost. It is easy to acquire social media ads for a low cost. For example, the Heart of Texas/United Muslims of America Rally cost approximately $200 in ads (Social, 2017). Ads for less
popular markets often are cheaper to purchase ads in, which could provide explanation for the poor targeting.

**Security of Election Day**

The physical security of voting machines is sufficient to deter cyber manipulation and other types of attacks. The paramount concern of a hacked voting machine is when someone on the outside can manipulate votes. The President-Elect of National Association of Secretaries of State and Secretary of State of Indiana Connie Lawson testified in July of 2017, “We have seen no evidence that vote casting or counting was subject to manipulation in any state or locality…no major cyber security issues were reported on Election Day November 8th” (Russia, 2017). This is largely due to the fact that voting machines are not connected to the internet and the decentralization of the US voting process.

Voting machines are rarely connected to the Internet in accordance with the Department of Homeland Security’s best practices (Norden, 2017, pg. 8). This practice helps defend against remote attacks and, if one were to occur, for it to remain undetected. Most attacks would be localized to a county or state depending on the uniformity of state practices. It would be much easier to hack into a voter registration database or a campaign’s e-mail server.

The Department of Homeland Security on January 6, 2017 designated voting machines as critical infrastructure and defined best practices, provided programing and support, and gave states a FOIA exempt and classified setting to discuss electoral security issues. The Acting Director of the National Protection and Programs Directorate testified to SSC some of these best practices include keeping the voting kiosk and tallying systems disconnected from the internet and having a paper backup trail for the purpose of auditing.
Many states have already adopted these best practices (Russia, 2017). Lack of internet connectivity means someone would have to physically access a part of the machine to insert malware or bad software to create an electoral disturbance or vote change.

Also, the decentralization of the United States voting process strengthens electoral security by limiting the scope of a successful attack. This is a strength as the United States’ presidential election is not one federal election, rather it is thousands of state and county elections. According to the Electoral Assistance Commission, “There are more than 8000 voting jurisdictions with over 100,000 polling places” (EAC, 2014).

If an attack were to be made on the election, it would be limited to a geographic area. These attacks become increasingly difficult as one factors in different types of polling machines.

The most at risk machines are those that lack a paper backup such as Direct recording electronic (DRE) machines, which rarely have an audit system in place. This risk is limited though, due to the decreasing number of operating DRE machines. The combination of the reliability of a paper backup and the electronic aspect of a DRE meet in an optical scan machine. Optical Scan machines are quickly becoming the preferred type of machine. “By the 2004 election, about 35% of the nation’s voters were using optical-scan machines” (Katel, 2006) and as of November 2016, “80% of registered voters made selections on a paper ballot” (Cybersecurity, 2017).
The two most significant vulnerabilities are physical access to the machines and their age. Physical access to machines is the easiest way for a hostile actor to manipulate a voting outcome. The switching of the machine’s memory cards could flip the ballots of a local election, where these individual machines are incredibly important, and infect a machine with virus or malware. Access to these machines is incredibly open, which exposes them to vulnerabilities such as foreign or domestic assets. Recently as this year the “the electronic poll books were stolen from the pickup truck of a poll worker during a ‘grocery run’ shortly before a Congressional special election” (Wallace, 2017).

Lawerence Norden at the Brennan Center for Justice sees this as a significant vulnerability, as most election machines are comparable to early 2000’s computers, which were infected by malware filled floppy disks. The malware in these infected memory cards “could cause…misreporting totals and crashing machines, but on a larger scale” (Norden, 2017, pg. 10)

The physical age of machines makes them susceptible to attack resulting from a lack of software updates to patch exposed vulnerabilities. Some machines are approaching the twenty-year mark, which in most cases is far beyond their expected lifespan. According to the Verified Voting Institute, which interviewed election officials in all 50 states, “Forty-three states will be using machines that were purchased 10 or more years ago. Fourteen states will be using some machines purchased 15 years ago” (Norden, 2015, pg. 9). The age of these machines coupled with the rapid advancement of technology over the past two decades has created the problem of the dated technology and software these voting machines rely on being unavailable.
In some jurisdictions, the machines replacement parts are no longer available. As technology continues to evolve and voting machines’ software does not, more methods for hacking and infiltration are created. For example, California is one of the few states with money left from the Help American Vote Act (HAVA). Yet, “Almost all California jurisdictions are using Windows XP or earlier. We even have jurisdictions that are still on Windows 2000” (Norden, 2015, pg15). This is also the case for most of the country, as the machines were purchased before 2006.

One can learn more from software that is not changing and readily available, like Windows XP and prior. “From a security perspective, old software is riskier, because new methods of attack are constantly being developed, and older software is [more] likely to be vulnerable.” (Norden, 2017, pg. 9). Constant updates occur on new software and operating systems, while out of date ones usually fall to the wayside. The more static something remains, the more someone can learn about it. If hackers can purchase a computer with Windows 2000, then they have access to what is installed in a voting machine and can learn from the primary source how to best hack these voting machines.

**Security Outlook**

If all remains constant, it is probable vote count manipulation will occur in the next six years. This manipulation will most likely be indirect through tampering with voter rolls or
other internet accessible components of Election Day. Targeted social media attacks will continue as the norm among these actors, followed by state and other electoral databases, and human infiltration of voting machines through malware as the least likely, but worst case scenario.

Foreign and domestic actors will continue to attempt electoral interference through the use of social media. While a great number of accounts with this purpose will become deactivated due to heightened public interest, corporate awareness, and legislative intent, actors will easily navigate these obstacles. As social media platforms adopt a hawkish stance against these actors, they will become increasingly active on sites with lesser restrictions or those that are less developed such as 4chan, Reddit, and Twitter.

Although the intent of foreign actors in the US election is unclear, we can assess it was an attempt to see what was “out there” and how much information they could obtain by the broad scope and variety of technique. All foreign actors in the 2016 election were widely unsuccessful in their attempts to manipulate vote count, but the campaign of disruption and chaos the Russians engaged in using social media and voter rolls was a success. The audience of many of these attempts including phishing emails also suggests this was more of an attempt to see how far they could get without detection rather than a full hearted attempt to change an electoral outcome.

In the next chapters, I will propose an assumption basis that shapes the subsequent policy recommendations. The roles of state governments and the federal government are crucial in identifying who bears the legislative and policy implementation burden. Russia attacked both state and federal elements of Election Day, so it is crucial the solution involves

---

9 Although Twitter is a part of the “Big 3” social media companies, they have the least amount of restriction as to verification of accounts, which is why they are included in this list.
all the components of electioneering. This framework aims to establish a solid ground based on responsibility and Constitutional jurisdiction to inform the best, legal policy solutions.
Chapter 4: Policy Framework and Assumptions

Before legislators begin to shape policy specifics, they must first decide how the state and federal governments will cooperate with one another within existing election laws. While the state typically makes election laws and policies, as Election Day becomes an issue of national security, the federal government might have increased purview. This chapter aims to discuss three policy frameworks which will provide a basis for the later policy recommendations.

The paramount question for many of these legislators is who has the power to enforce electioneering policy: states or the federal government? There are merits to either approach. A federal approach would likely have a supervising agency regulating election standards once Congress passed laws giving these agencies the right to do so. Once an agency came to a conclusion of standards or best practices, states would be obligated to meet them. While the cost of most electioneering reforms are low compared to the disastrous effects of electioneering failure, many states have little to no funds to operate with\(^{10}\), and required federal reform often comes in the form of unfunded mandates or grants, which take time to apply for and receive.

The benefits of such an approach include conformity among electioneering practitioners and massive federal infrastructure for support. It is often difficult to address issues in individual voting precincts because there is a great amount of background information and briefing required to establish a foundation before the problem is diagnosable. Creating consistency in practice allows for less intermediaries between the

\(^{10}\) States also typically include election upgrades in their budget, but it is lower on the priority list than most funding requests. Most machines were purchased shortly after the passing of HAVA in 2002 and have not been upgraded since. See the Verified Voting Center map in chapter 3
person running the election in a given precinct and the national security or IT expert. It also allows for people to become incredibly specialized in election security and maintain consistent oversight.

DHS would likely be the lead oversight agency for election security. Upon its creation in 2002, it was tasked with protecting the nation’s critical infrastructure from physical and cyber threats (DHS, 2017). DHS gained authority over electioneering equipment when it was designated critical infrastructure on January 6, 2017. While they have chosen to frame their role with this designation differently than described above, the mainly federal oversight mentioned above remains a possibility if the program is successful and expands or further threats necessitate more DHS involvement.

Many legislators and election officials feel that since any election, even the presidential, occurs at the state level, states should take the lead on ensuring their security. States could have intelligence agencies brief them on current vulnerabilities or address them with internal checks and address them using existing resources at the discretion of the Secretary of State, General Assembly, or Governor. All states have the ability to perform cyber hygiene checks using off-the-shelf diagnostic tools like Norton or McAfee or the funds to contract out to a private security firm. States can also address vulnerabilities like open access to voter rolls and voting machines or lack of paper audits with simple policy changes or further training, so the use of federal resources is not completely mandated.

There are numerous benefits to this approach including cost saving factors along with the elimination of the perception of federal oversight. Also, as mentioned previously in this paper, the decentralization of US electioneering is one of its strongest assets. Allowing states to individually come up with solutions creates further diversity for actors continuing to attack
our election infrastructure. States also do have methods to conference and discuss with one another, such as national boards of Secretaries of States or Governors, so groupthink is avoidable and innovative solution making and sharing is possible.

The pitfalls to this approach include the fact that many states\textsuperscript{11} do not have available Help America Vote Act (HAVA) funds or money in the state budget to purchase and utilize these tools (Norden, 2017). The lack of communication with the federal government also could create a gap in intelligence, as there is a weak connection between states experiencing security issues and a sort of fusion center. While it is doubtful an attack on multiple states would occur without the IC knowing, these gaps in communication could damper the speed in which a response is formed.

The ideal policy solution embodies the merits of both alternatives: the diversity of a state led solution with the resources of a federally led solution. This argument operates from the premise that some level of federal involvement in necessary due to the threat to national security tied to electoral security and any threat to national security falls within the purview of the IC. Both parties’ involvement is crucial in order to best secure elections while addressing individual issues.

In order for DHS involvement to be successful and accepted by policy makers, it is essential election officials do not feel DHS is overreaching and going outside their role as a federal agency. The principle of each state running their election is crucial to the free and fair American electoral process and essential to its identity. Infringement with this could create tension between the agencies and election officials and policymakers.

\textsuperscript{11} These states are Arkansas, Connecticut, Idaho, Illinois, Kentucky, Louisiana, Massachusetts, Michigan, Mississippi, Nebraska, Nevada, New Mexico, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, Utah, Vermont, Washington state, and West Virginia
Federal support of the states is an ideal blend of these two policy philosophies. It gives states the chance to assess independently what they need or take full advantage of DHS resources and formulate a plan in cooperation. It also alleviates the financial burden of pursuing many of these security checks or upgrades. DHS can also act in this role as a sounding board for states to form solutions or a place to synthesize nationwide issues multiple states experience.

The next chapter discusses individual policy solutions that embody this approach. It also elaborates on DHS’s designation of election systems as critical infrastructure and elaborate on the most valuable resources available to states from this designation. Finally, it discusses the role of non-state actors (e.g. Social media) in the election and resources available to them.
Chapter 5: Policy Recommendation

This chapter contains policy recommendations to address the vulnerabilities highlighted previously in the paper. Two of these recommendations include utilizing DHS resources available to owners of critical infrastructure. DHS’s designation of election systems as critical infrastructure in January of 2017 left many states confused as to the role the federal government would have in elections. The aim of the following section is to explain critical infrastructure as it applies to states and the private sector.

What is Critical Infrastructure?

The US PATRIOT Act of 2001 defines critical infrastructure as, “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters” (USA Patriot Act of 2001, 2018). There are sixteen subsets of critical infrastructure. Election systems fall under the sector of Government facilities, which also includes the subsets of National Monuments and Icons, and Education Facilities.

Once a sector is assigned to a piece of critical infrastructure, it is assigned a sector specific agency (SSA). DHS is the SSA for election systems. The SSA is supposed to govern and help the sector self-organize to meet its legal requirements for protection. The SSA is “responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all hazards environment” (Starting Point, 2017). There is an option for other agencies to become co-SSA’s in order to fulfill a substantial knowledge gap. The US Elections Assistance Commission has petitioned to become the co-SSA, but it is not currently designated as such.
Critical infrastructure also provides further organization beyond the SSA and co-SSA. In particular, it established two committees: Sector Coordinating Councils (SSC) and Government Coordinating Councils (GCC). The SSCs is perhaps the most valuable, as it is a self-organized body consisting of infrastructure owners and their representatives. It will likely consist of, “representatives from federal, state, and local government; election system vendors; and other stakeholders impacted by the critical infrastructure designation” (Starting Point, 2017). They coordinate policy with the GCC and also serve as a communication conduit between various parties, in this case, individual states. The GCC is similarly organized in order to facilitate cross governmental communication regarding election matters.

The designation of critical infrastructure is intended to provide clear and strong lines of communication between stakeholders and the SSA. Part of this includes designating Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). Both are formal communication channels, but ISACs are distinguished in that they are exclusive to critical infrastructure owners\(^\text{12}\) and it provides an appropriate setting for discussing classified information (Starting Point, 2017). ISACs are classified as Protected Critical Infrastructure Information (PCII) under the Critical Infrastructure Information Act, so they are not subject to laws such as the Freedom of Information Act (FOIA) or similar state counterparts.

All of the above is completely voluntary and the DHS role is entirely limited to support. This is a theme throughout the services provided through the critical infrastructure

\(^{12}\) ISAOs are available to a much broader group including small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc.
designation. The next section will discuss the resources and programming available to owners of critical infrastructure, along with resources specific to states and other subsectors.

**What Resources Are Available to Critical Infrastructure Owners?**

Numerous resources and programs are available to critical infrastructure owners, and many of these are made specifically for state, local, tribal, and tribal (SLTT) owners in the election systems subsector. Most of this program consists of cyber assessments, tests, hygiene, and consulting for future individual organizations. There are also multiple opt-in warning systems and remote tests available to critical infrastructure owners, many with near immediate response time (DHS, 2017). The designation mainly gives critical infrastructure owners direct lines of communication with DHS cyber security experts and election infrastructure owners across the country. Later in this paper, I will make recommendations for specific programs for election infrastructure owners and private sector operators.\(^{13}\)

These programs greatly improve cyber security as DHS provides a central location and communication hub for intelligence and information. If many states are experiencing similar issues, there is an effective, reliable, and secure place to discuss solutions. All the programs are no cost and SLTTs receive priority over private sector actors.

Two resources in the DHS election infrastructure catalog are exclusively available to election infrastructure owners in SLTT governments: cybersecurity advisors (CSA) and incident response, recovery, and cyber threat hunting. CSA’s are individuals with expertise in a region and they stay on cite to conduct preparedness meetings, assessments, coordinate with federal and local entities, and address incidents as they occur. These individuals are available locally, so SLTTs can form relationships with them.

\(^{13}\) The full catalog of services can be found at [https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf](https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf)
Incident response consists of a team assessing a situation on cite or remotely to assess gravity of the situation, review the security of core devices and technology, and mitigate future response to create solutions (DHS, 2017). The team generates a report within 30-60 days consisting of background, scope, findings, security best practices, and relevant conclusions. The goal of this program is to manage the potential incident in a way that reduces risk, harm, recovery time, and costs.

**Recommendations for Voter Roll and Electronic Poll Book Owners**

These recommendations are tailored for SLTT owners of voter rolls. Most of these recommendations take advantage of existing, low cost resources and suggest opportunities for further funding. This is due to the limited reserve of HAVA funds states still have and the fact most election day activity is federally stipulated. Congressional action will be discussed later in the paper.

The most effective action election infrastructure owners can take is increasing their own threat awareness. While this solution sounds simple, it is incredibly complex due to the constant change and update of voter rolls from multiple sources. These rolls are also centralized at the state, so one roll can be updated hundreds of times a day.

While the costs of risk assessments could be between $25,000 and $50,000, DHS now provides resources through its critical infrastructure designation to owners of voter rolls. In particular, a cyber infrastructure study, phishing campaign assessment, cyber resilience review, vulnerability scan, and communication with the local cyber security advisor can provide a thorough risk assessment. These programs can provide reports in as little as a week and require only a 48 hour lead time to schedule (DHS, 2017). All of these programs are opt-in only, so states and localities must consult the DHS catalog to find the content and
instructions for initiating service. These services only cover cyber audits, but the cybersecurity advisor can serve as a liaison between the SLTT and other risk assessment providers.

Upgrading and replacing these databases is also crucial for electoral security. The Brennan Center for Justice estimates that 41 states are using voter registration databases that were initially created at least a decade ago (Norden, 2017). Sadly, most states have exhausted the HAVA funds that originally create the databases. If states require further funding for risk assessment, upgrading IT and software, or purchasing new voting machines, they can apply for grants through EAC or DHS to provide these upgrades.

**Congressional Responsibility to Voter Roll Owners**

Congress’s main control over electoral security comes from funding and amending previous legislation. DHS’s designation of electoral systems as critical infrastructure addresses the need for new policy creation. Rather, Congress could work within its existing framework to support the states and agencies assisting them. This is more politically feasible due to the general dislike of federal involvement in elections, election consultants’ concerns over changing election administration policy, and hyper partisan political environment.

HAVA created the provision which mandated states to create central voter rolls. Prior to the enactment of HAVA, these rolls were maintained on the jurisdictional level and managed independently of one another. One of the strongest aspects of US election administration is its decentralized nature, and this could increase the security of voter rolls. Congress could repeal the provision of HAVA that requires state centralized and owned voter rolls. This would give states the option to maintain their databases as is or diversify. This
increases security because it adds another facet to our multi-dimensioned election administration and addresses the unique needs of each state.

It is likely states will maintain their central databases, but to avoid confusions and poor policy transition, Congress could mandate a switchover day or Governors could urge their state legislatures to vote on legislation deciding who owns their database. This allows for states to address their problems in a way suited for their needs.

Fully funding the EAC is crucial to providing states the much-needed electoral support. This funding provides grants necessary for upgrades and risk assessments, both of which are essential to strengthening electoral security. Congress could fund most of the needed updates to electoral software and machines through a combination of these and DHS grants.

To address the issue of machines without audit systems, Congress could stipulate the grants must fund machines with a paper backup or some other form of audit. Congress could also mandate routine audits of federal elections in order to ensure accurate electoral counting and address discrepancies as they arise. This provides an additional layer of security to the highest caliber of elections and ensures best practices for subsequent midterm and local elections.

**Recommendations to Political Parties and Third Party Political Organizations**

One notable aspect of US elections is the extensive involvement of third parties, namely those outside of the federal, state, and local government. Russian efforts reached think tanks, political parties, and research groups. This interference made the public realize how much information these groups held onto and how valuable it truly was, whereas prior to this, these political organization’s existence was rarely questions or thought about. Political
organizations now have an obligation to increase their security because the 2016 election made the world realize how integral they are to our elections.

Political organizations are also able to partake in the resources available to SLTTs through DHS’s critical infrastructure designation. However, an SLTT must recognize them as an affiliated third party or they must unilaterally pursue action. If they contact DHS independently, they will not be given priority the SLTT governments are given and will likely be placed on a waiting list.

It is in the interest of both the Republic and Democratic National Committees to work with their state level offices to conduct a thorough cybersecurity check using DHS resources. State level parties could reach out to the localities they are affiliated with and have strong relationships with and request the SLTT have DHS conduct an External Dependencies Management Assessment, which assess risks from the third parties SLTTs use. The state and local level parties from there can form a beneficial relationship with DHS if they choose to pursue further cyber or security assessments.

The congressional and national committees will likely have to use a similar method as the state level offices to receive priority, but could be better served by contacting DHS as an independent organization. This allows for the committees to address their specific needs and inadequacies in an appropriate setting if a national security incident like that of 2016 were to occur again. A majority of DHS resources offered to election system owners are offered to third parties like political parties, they will just likely wait longer than SLTTs. For this reason, it is also recommendation political organizations work with private security firms and hire more IT security personnel.
Some political committee’s leadership may not be comfortable using DHS resources or prefer to contract independently for faster service. Private security firms are a valuable tool for ensuring security and are likely more able to maintain routine cyber maintenance and checks while filling in gaps from DHS cyber security checks to address more specific concerns. Internal IT is also crucial to upgrading security. While an internal IT cybersecurity staffer may not be necessary for every gradation of political parties, it is recommended the National Committees have one for their internal IT needs and potentially one available for their state offices. The role could also be fulfilled by the same individual depending on budget.

Recommendations to Social Media Corporations

Social media ad buys are of particular interest to lawmakers as they a minimally regulated form of political advertisement where the rights of private corporations and public interest meet. Social media corporations are extensively protected from government regulation of their activities as private business. However, Congress is taking legislative initiative to regulate these corporations and their ad distribution. It is in the interest of corporations to avoid this regulation, as it is likely to create future accountability issues and sets a precedent of government interference in tech businesses with large amounts of data caches. Social media companies could self-regulate by enforcing their current terms of service more strongly, updating them to clarify language surrounding political advertisement, and increase the presence of community policing.

Most social media corporations have terms of service and condition that a client must agree to before opening an account. They are relatively uniform in stature: a real person must own and operate the account, no pornographic or violent content without proper designation,
and the condition that violation of any of the terms is grounds for immediate account shutdown without notice. These terms and conditions must be strongly enforced to reduce the risk of foreign ad buys related to US elections. Facebook, Twitter, and Alphabet all testified the ads purchased relating to the 2016 cycle were in violation of a term or condition of service in some way, so the means for these companies to police themselves are already in place.

Terms of service can always be updated to add clarifying language or sections regarding specific instances or cases. An example of this is LinkedIn updating their terms of service in the mid 2010s to remove legal sex workers from advertising on their platform in response to increased use of the platform as advertisement for escort businesses. Social media corporations could update their terms of service to lay out explicit parameters regarding political advertisement, particularly advertisements from abroad in the US. This update is not only a strong means of enforcement, but also advisable from a public relations standpoint, as it shows affirmative action and explicitly names and sets forth an agenda for foreign purchased political advertisement.

Community policing is also a recommended initiative for social media corporations. While many social media outlets, such as Facebook, have already invested heavily in creating more algorithms to determine fake accounts from real ones, humans are particularly acute at recognizing advertisement and knowing it as clickbait or legitimate reading material. Social media companies could offer incentives, financial or otherwise, to encourage policing of content.

While it would not be wise for all users to have this power, it is possible to test and select users diverse in location, background, demographic, political affiliation, and socio-
economic status to become community regulators. These individuals could be tasked with reporting “fake news” or suspicious advertisement and pages to Facebook. The regulators’ reports could have priority status over general user’s reported content. Since these individuals are previously vetted and could be compensated from successful reporting, there is mutual incentive between the social media organizations and the reporters.

An example of an outlet that has similar policing is Reddit. Reddit is a forum outlet where users ask and respond to various questions. Select members apply and are granted the title of “Reddiquite keepers”. These individuals are in charge of reporting slanderous, offensive, vulgar, or otherwise inappropriate content to Reddit. They are compensated for doing so at an undisclosed amount. The outlet despite its laissez faire approach remains an outlet known for its civil discourse and exchange of ideas and information.

Social media organizations must also be careful to avoid censorship in the cracking down on fake news and foreign advertisement. Multiple outlets are currently experiencing censorship lawsuits and others face accusations of censorship. Current, Google via YouTube is undergoing a lawsuit from Prager U, a conservative education and media outlet with an entirely online presence. Their argument sources from the premise that since Google codes the algorithms that deletes or lowers visibility of their content, they are liable for censorship. The confusion lies in how much Google can blame a computer for censorship or does the responsibility fall on the programmer that coded it?

By creating an algorithm that chooses not to show post in a chronologic order, social media companies have made themselves liable to lawsuits and accusations of censoring particular content creators. These algorithms make social media companies gatekeepers of

---

14 See Appendix B
what information one can receive, rather than the of the platform which sought to break up the monopoly of mainstream media. Currently, about two thirds of Americans receive their news from Facebook (Shearer & Gottfried, 2017). If social media cites are going to have news on their website, they must remain the minimally regulated, public forums they are to keep their Section 230 protections rather than become a publisher by implementing algorithms.

According to US Code 230, “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider (Telecommunications Act, 1996). The question becomes when social media outlets create algorithms that influence traffic to certain outlets along political lines, do they keep these protections or do they become publishers and speakers of content?

An analogous comparison is telecommunication outlets like ATT and Verizon and how they handle their service. Neither of these companies have people monitoring what is said over a line and censoring content they do not approve of. So they are not liable to the illegal things someone might say under Section 230.

Since social media platforms are now beginning to respond to pressures from Congress by continuing to police information, they are now opening themselves up to more lawsuits for crimes like slander and copyright infringement. They cannot continue to police what people publish online because their actions make them complicit if they do not do their job fully and leave someone victim to slander or unauthorized use of a stolen image. To maintain Section 230 protections, social media must return to the platform it once was and either refine their algorithms or get rid of them altogether.
While the social media ads appear to be largely ineffective as demonstrated earlier in the paper, social media corporations do have an obligation as information sharing outlets to protect First Amendment Rights, but they also are private corporations that have a right to run their business how they please as long as it is done legally. They must learn to balance these obligations while protecting the integrity of their outlet from fake news and advertisement.

**Recommendations to Upgrade Voting Machine and Election Day Security**

Although much of the above paper paints a weak and vulnerable electoral system, the US’s electoral systems are far from helpless. The decentralization of our elections combined with diversity in voting machine types make our election day incredibly difficult to manipulate. The antiquity of most of America’s voting machines is a paramount concern, and addressing it addresses many of the root problems. Congress and the states jointly carry the burden of addressing these vulnerabilities through funding and implementation of best practices.

First and foremost, states must go about purchasing new voting machines and equipment. Particularly, states relying heavily on DRE machines must purchase a form of machine with a paper backup or voter verified ballot, such as Optical Scan machines or implementing vote by mail. For all practical purposes, given the current state of voting technology, this means that a voting system should provide a paper record that the voter has reviewed or filled out before casting her ballot on the electronic machine. According to the Brennan Center estimates, “in 2016, at least 80 percent of registered voters made selections on a paper ballot or voted on an electronic machine that produced a paper trail” (Norden, 2017). This unchangeable record provides an important security redundancy that
should act as a deterrent to cyberattacks and should provide voters with more confidence that their votes have been counted accurately.

The Brennan Center also estimates the machine replacement alone could cost between $130 million and $400 million (Norden, 2017). While this is certainly not the full extent of funding needed and does not include expenses like training and costs incurred over the lifetime of the machine, it provides a baseline on what Congress and states can expect as adequate funding. EAC and DHS grants can bear some of this burden, but Congress needs to free up money in the budget to fund these grants fully and create new ones.

The elimination of multiple agencies and endowments in the President’s FY18 budget provides more than adequate funding for new voting machines. Congress would be well served by freeing up these funds because covering a fraction of these costs would go a long way in persuading states to upgrade their systems.

Congress or the EAC must stipulate with the receipt of new funding comes mandates and expectations. First, that the states adopt best security practices as they are currently able. Second, it must keep the vendors and machine types relatively diverse across the nation. Finally, states must conduct routine audits.

States are currently aware of best security practices and the EAC needs to ensure states are adequately implementing the best practices a state can afford. More funding can be pursued to fill in gaps or states can utilize the free DHS resources from the critical infrastructure designation. Ensuring diversity in voting machine vendor and type maintains the current strengths of the US electoral systems. The fear is if multiple states begin to purchase new equipment and decide their needs are suited for a singular type of machine
from a single manufacturer, enemies of the US can more easily disrupt more voting machines with a smaller time and resource investment.

Of course, these new machines that provide a paper backup are not of much aid if the states do not conduct audits. Currently, only twenty-six states require post elections audits (Norden, 2017). These post-election audits serve a dual purpose of potentially catching attacks and rebuilding voter confidence in elections. Even though most of these audits only utilize a sample of votes, their implementation will likely restore voter’s faith in US elections, which was greatly degraded by Russia’s efforts in the 2016 election.
Chapter 6: Conclusion

The United States is not defenseless against electoral interference. Decentralization along with a new, heightened public interest make it possible to address vulnerabilities in the electoral process and find innovative solutions. However, if solutions are not implemented quickly, it is likely the US could have a vote outcome changed in the next six years.

History proves that different nation-states are likely going to continually interfere in one another’s elections, but what made the 2016 Presidential election so special was a focus not on directly changing votes, but deepening divides between Americans. Russia’s goal was not to change a vote outcome this time, it was to create animosity and turmoil between Americans and push people closer to ideological tribalism.

They accomplished this while investigating how far they could penetrate American electoral systems. This hacking provided more than information. As reports of these hacks became public, it forced Americans to doubt if something as crucial to our identity as a free and fair electoral process is even occurring anymore. Inauguration Day occurring under the auspice of a rigged election sowed seeds of doubt and division that will likely bear fruit of further division and a breakdown of partisan, civilized discussion.

While there are solutions immediate solutions that address pertinent national security issues such as fully funding agencies that assist and secure elections like DHS and the EAC, replacing old voting machines, enabling states to get rid of centralized voter rolls, and protecting information on social media and political parties through internal policy changes partially address the problem, the United States must come to terms with the damage Russia did and how to go about rebuilding trust in government and the electoral process.
Appendix A: Heart of Texas and United Muslims of America Facebook Interaction and Protests

Source: SSCI Hearing on Russian Interference in the 2016 Election
Appendix B: Facebook Ad Preferences Determine Political Affiliation to Tailor Advertising

Source: Facebook of Julia Swafford

How to find your marked political preference: Facebook>Settings>Ads>Your Information>Your Categories
Works Cited

Assessing Russian Activities and Intentions in Recent US Elections. (2017, January 06).
Retrieved February 21, 2018, from


Carr, C., personal communication, May 2016

London : Greenwood Press.

https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf


Russia Investigative Task Force Open Hearing with Social Media Companies: Hearings Before the Select Committee on Intelligence, House, 115th Cong. 1 (2017).


https://soundcloud.com/benshapiroshow/ep409


Sullivan, M., personal communication, September 2017


U.S. v. INTERNET RESEARCH AGENCY LLC, (D.C. Cir. 2018)
