



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**IN THE LINE OF FIRE: SAFEGUARDING AMERICA'S
ELECTION SECURITY**

by

Laura A. Hughes

March 2021

Thesis Advisor:
Second Reader:

Rodrigo Nieto-Gomez
Shannon A. Brown

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE March 2021	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE IN THE LINE OF FIRE: SAFEGUARDING AMERICA'S ELECTION SECURITY			5. FUNDING NUMBERS	
6. AUTHOR(S) Laura A. Hughes				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The U.S. electoral system and democracy are under continued attack by foreign adversaries and political extremists intent on manipulating U.S. elections. Election officials and homeland security stakeholders must search for alternative methods to help strengthen the resiliency of the system. The question then becomes: How can red teaming and systems thinking be applied to reinforce the integrity of the U.S. electoral system? The goal is to analyze the system in its entirety to ensure the system in place can support a free and fair election and withstand an attack from an adversary. This research studies how the rapid implementation of universal mail-in voting created the opportunity for political activists to cast doubt on the validity of the election results. By applying systems thinking to the implementation of mail-in voting, election officials would have identified the additional challenges in advance and employed security protocols and alternative options to mitigate potential threats. To test security protocols in place, stakeholders should employ red teaming vulnerability probes. The vulnerability probes will assist in determining how effective the protocols are and if alternatives need to be established. Stakeholders should consider employing the use of systems thinking and red teaming to identify vulnerabilities and reinforce the integrity of the U.S. electoral system.				
14. SUBJECT TERMS election integrity, election security, red teaming, systems thinking, U.S. Secret Service, DHS, Department of Defense, U.S. electoral system, voting machines, voter registration databases, election management bodies, CISA, vulnerabilities, technology, election infrastructure, voter confidence, democracy, voter fraud, election day, cyber attacks, poll workers, voting systems, security plan, advance work, resilient and secure			15. NUMBER OF PAGES 127	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**IN THE LINE OF FIRE: SAFEGUARDING AMERICA'S ELECTION
SECURITY**

Laura A. Hughes
Senior Special Agent, U.S. Secret Service, Department of Homeland Security
BA, University of North Carolina at Charlotte, 1998

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2021**

Approved by: Rodrigo Nieto-Gomez
Advisor

Shannon A. Brown
Second Reader

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The U.S. electoral system and democracy are under continued attack by foreign adversaries and political extremists intent on manipulating U.S. elections. Election officials and homeland security stakeholders must search for alternative methods to help strengthen the resiliency of the system. The question then becomes: How can red teaming and systems thinking be applied to reinforce the integrity of the U.S. electoral system? The goal is to analyze the system in its entirety to ensure the system in place can support a free and fair election and withstand an attack from an adversary. This research studies how the rapid implementation of universal mail-in voting created the opportunity for political activists to cast doubt on the validity of the election results. By applying systems thinking to the implementation of mail-in voting, election officials would have identified the additional challenges in advance and employed security protocols and alternative options to mitigate potential threats. To test security protocols in place, stakeholders should employ red teaming vulnerability probes. The vulnerability probes will assist in determining how effective the protocols are and if alternatives need to be established. Stakeholders should consider employing the use of systems thinking and red teaming to identify vulnerabilities and reinforce the integrity of the U.S. electoral system.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	RESEARCH QUESTION	1
B.	PROBLEM STATEMENT	1
C.	LITERATURE REVIEW	5
1.	Technology in U.S. Election Infrastructure.....	5
2.	Election Management Bodies.....	7
D.	RESEARCH DESIGN	10
II.	U.S. ELECTION SYSTEM (2000–2020)	15
A.	2000 ELECTION	15
1.	The Help Act and the Election Commission.....	18
2.	Voting Technology	19
3.	Voter Identification, Databases, and Provisional Voting.....	20
4.	Recounts and Lawsuits	22
B.	2016 PRESIDENTIAL ELECTION	24
1.	Social Media and Fake News	24
2.	Vulnerability of Election Infrastructure.....	27
C.	CREATION OF A CYBER AGENCY TO PROTECT THE U.S. ELECTION SYSTEM.....	29
D.	2020 ELECTION	33
III.	U.S. ELECTORAL SYSTEM.....	39
A.	PRIMARIES AND CAUCUSES	41
B.	NATIONAL CONVENTION	44
C.	ELECTION DAY.....	47
D.	CERTIFYING ELECTIONS.....	52
E.	ELECTORAL COLLEGE.....	56
F.	JOINT SESSION OF CONGRESS CERTIFICATION	58
IV.	APPLYING SYSTEMS THINKING AND RED TEAMING TO THE U.S. ELECTORAL SYSTEM.....	65
A.	CHAIN OF CUSTODY PROCEDURES FOR MAIL-IN BALLOTS.....	65
1.	Voter Registration and Distribution of Universal Mail-In Ballots.....	66
2.	Casting Mail-In Ballots.....	67
B.	RETURNING MAIL-IN BALLOTS	71

1.	Ballot Drop Boxes	72
2.	United States Postal Service	74
C.	STORAGE OF BALLOTS.....	78
D.	ELECTION RESULTS	81
V.	CONCLUSIONS AND RECOMMENDATIONS.....	87
A.	RECOMMENDATIONS.....	88
1.	Conducting After-Action Reports through the Use of Systems Thinking.....	89
2.	Executing Red Team Attacks on Non-Cyber Election Infrastructure.....	91
B.	CONCLUSION	92
	LIST OF REFERENCES	93
	INITIAL DISTRIBUTION LIST	107

LIST OF FIGURES

Figure 1.	Broward County Judge Reviews Punch Card Ballot in Florida Recount.	16
Figure 2.	The U.S. Electoral Process.....	40
Figure 3.	Primary and Caucus Flow Chart	42
Figure 4.	National Conventions Flow Chart.	45
Figure 5.	General Election Voting Flow Chart.	51
Figure 6.	Certifying Elections Flow Chart	52
Figure 7.	Electoral College Flow Chart.....	57
Figure 8.	Joint Sessions of Congress Flow Chart.....	60
Figure 9.	The U.S. Electoral Process Flow Chart	62
Figure 10.	Systems Thinking Mapping of the Implementation of Mail-In Voting.....	84

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DMV	Department of Motor Vehicles
DNC	Democratic National Committee
FBI	Federal Bureau of Investigation
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
PEI	perception of electoral integrity
PROSeS	process design, resource investment, service output, service outcomes, and stakeholder satisfaction
USB	Universal Serial Bus

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The U.S. Electoral System and democracy continue to be under attack by foreign adversaries and political extremists who intend to manipulate U.S. elections. Despite the diligent work of election stakeholders, vulnerabilities within the current system continue to provide adversaries a vehicle to disrupt U.S. elections. The recent 2016 and 2020 U.S. presidential elections saw foreign adversaries attempt to gain access to election infrastructure, initiate disinformation campaigns, and saw high-ranking U.S. officials challenge mail-in voting's validity. While the electoral system attacks did not alter the election's outcome, they succeeded in creating doubt in the system's integrity. Election officials and homeland security stakeholders must continue to search for alternative methods to help strengthen the system's resiliency.

This thesis analyzes the current electoral process from start to finish to gain perspective on the current system's resiliency. Specifically, it examines the process of mail-in voting to include voter identification procedures, the chain of custody, and security protocols. The thesis focuses on how election officials and stakeholders can strengthen the system and prevent future vulnerabilities caused by recent changes. While the current linear method used by election officials effectively solves the problem at hand, it fails to recognize how the solution can inadvertently cause additional vulnerabilities in other system components. Which leads to the question: *How can red teaming and systems thinking be applied to reinforce the integrity of the U.S. electoral system?* This thesis explores the potential use of systems thinking to evaluate the system and use a red teaming method to test the system. This project draws on data from academic literature, legislative testimony, and government reports, and examines the rapid implementation of mail-in voting in the 2020 U.S. elections as a case study.

The thesis compares how the U.S. Secret Service methodology is akin to systems thinking and has successfully ensured the safety of the world's highest leaders. The Secret Service and the Department of Defense have tested protocols in place through the method

of red teaming.¹ The complexity of the U.S. electoral system makes it a perfect candidate for systems thinking. Systems thinking provides a framework to analyze how altering one element of the system can have a lasting effect on the system as a whole.² The method examines three components within the system: the elements, the interconnections, and the purpose.³ An examination of the electoral system affords election officials the ability to identify the pitfalls or advantages of future changes to the system before implementation. By mapping out the mail-in voting process, officials would have recognized that relaxing security and chain of custody protocols, last-minute changes to election laws, and poor communication could lead the public to question the system's integrity.

Red teaming challenges an organization's assumptions by imagining a system from an adversary's perspective, thinking outside the box, and perpetuating an attack on the system to identify vulnerabilities.⁴ To understand the threat, U.S. election officials must understand the enemy's culture and skillset and how they factor into planning an attack. The Cybersecurity and Infrastructure Security Agency already recognizes its effectiveness in securing electronic voting infrastructure. Following the 2016 election, the creation of tabletop exercises helped state and local election officials mitigate an attack on their voting systems.⁵ The tabletop exercises could help test the durability of security protocols for all designated election critical infrastructure. While the agency made great strides in securing electronic infrastructure, the focus must shift to ensuring critical physical infrastructure has sufficient security protocols. Election officials and government agencies have been one step behind this nation's adversaries in identifying vulnerabilities within the U.S. electoral system. Red teaming may be the answer to solving this problem.

¹ Micah Zenko, *Red Team: How to Succeed By Thinking Like The Enemy* (New York: Basic Books, 2015), 116.

² Donella H. Meadows, *Thinking in Systems: A Primer* (White River Junction, VT: Chelsea Green Publishing, 2008), 17.

³ Meadows, 11.

⁴ University of Foreign Military and Cultural Studies et al., *The Red Team Handbook*, v. 9 (Fort Leavenworth, KS: University of Foreign Military and Cultural Studies, 2018), 69–72, https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf.

⁵ Vijay D'Souza and Rebecca Gambler, *Election Security: DHS Plans Are Urgently Needed to Address Identified Challenges before the 2020 Elections*, GAO-20-267 (Washington, DC: Government Accountability Office, 2020), 16–17, <https://www.gao.gov/assets/710/704314.pdf>.

Over the last decade, foreign adversaries and high-ranking elected officials have tested the U.S. electoral system and exposed vulnerabilities within the system that need addressing to preserve its integrity. The recent implementation of universal mail-in voting provided the perfect case study to test the application of systems thinking and red teaming. Therefore, based on the case study findings, this thesis recommends two proposals for inserting after-action reports in which systems thinking methodologies are utilized for the final analysis and the use of vulnerability probes to test the resiliency of election infrastructure. The recommendations can identify current and future vulnerabilities within the electoral system and provide the opportunity to test solutions before implementation. The proposals will require buy-in from election stakeholders and additional funding to obtain the personnel qualified to perform the task. While election officials must consider the challenges to implementing the recommendations, they must also consider the importance of maintaining a secure and resilient electoral system.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would first like to thank my thesis committee, Rodrigo Nieto-Gomez and Shannon Brown, who spent many hours talking through my ideas, providing feedback and guidance, and challenging me to push myself outside my comfort zone. I am grateful for their knowledge and support throughout this journey.

Second, I would like to thank my cohort members for always supporting me through this process. While our adventure through this program did not exactly go as planned, I would not have succeeded in completing this program without their friendship and encouragement.

I would especially like to thank my husband, Glen, for always believing in me and for being my rock. I could not have completed this process without your unwavering support. From the extra responsibilities you took on, your willingness to be my second pair of eyes, and your pep talks, all of which made this process possible for me. Georgia, Charlotte, and Lila, I hope I have shown you that you are never too old to learn and can do anything you set your mind too. To my parents, David and Billie, thank you for instilling in me the importance of learning. Your encouragement, not only throughout this process but also throughout my life, has been a driving force in my success.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

How can red teaming and systems thinking be applied to reinforce the integrity of the U.S. electoral system?

B. PROBLEM STATEMENT

On the evening of November 7, 2000, the nation held its breath as the Presidential Election was coming to a close that night.¹ As the Electoral College's majority numbers trickled in, it soon became obvious no clear winner would be declared that night. When Americans awoke the next morning, they learned that Florida's 25 electoral votes, hampered by hand recounts, machine recounts, absentee ballots, and outdated punch-card technology, were thwarting anyone from declaring victory.² This situation should have served as an early warning siren to states, and it was about to be deafening.

Federal, state, and local governments have been trying to rectify flaws in the U.S. voting system for more than two decades since the 2000 election came down to the State of Florida. Due to the slim margin of votes in favor of George W. Bush, a recount was conducted per Florida law.³ The results of this recount raised the question of why Florida was still using this outdated punch-card technology that forced many states to re-evaluate their voting machines and processes.

The American Civil Liberties Union filed lawsuits against five states, including Florida, for using outmoded punch-card machines, which it claimed violated individuals' equal protection rights.⁴ Consequently, Congress passed the Help America Vote Act of

¹ Ron Elving, "The Florida Recount of 2000: A Nightmare That Goes on Haunting," National Public Radio, November 12, 2018, <https://www.npr.org/2018/11/12/666812854/the-florida-recount-of-2000-a-nightmare-that-goes-on-haunting>.

² Elving.

³ Richard L. Hasen, *The Voting Wars: From Florida 2000 to the Next Election Meltdown* (New Haven, CT: Yale University Press, 2012), 3–4.

⁴ Daniel P. Tokaji, "The New Vote Denial: Where Election Reform Meets the Voting Rights," *South Carolina Law Review* 57, no. 4 (Summer 2006): 689–734.

2002, which provided funding for states to replace their outdated voting systems with new touchscreen computers.⁵ However, by 2006, only 38% of states had adopted such new technology.⁶

While replacing outdated voting machines with new technology was a step in the right direction, it failed to address election system deficiencies, such as inaccurate voter registration databases, partisan involvement in post-election audits, and poorly trained poll workers.⁷ The beginning of the new millennium saw the emergence of some novel election concerns, as well as the recurrence of some more familiar problems, such as partisan bias. First, in 2004, the Ohio secretary of state faced election abuse allegations from Democrats because he had been the former head of President Bush's re-election campaign in Ohio.⁸

Additionally, in 2008, the Minnesota Senate race was brought into question when Democrats requested a recount to include over 1,000 absentee votes, which had initially been dismissed by local election judges.⁹

Then came the 2016 election, which opened the proverbial Pandora's box of technological problems, and exposed new weaknesses, such as foreign interference in U.S. elections.¹⁰

The following May, then Deputy Attorney General Rosenstein appointed Robert Mueller special counsel to the Department of Justice's inquiry into Russian interference in

⁵ "The Help America Vote Act of 2002," Department of Justice, August 6, 2015, <https://www.justice.gov/crt/help-america-vote-act-2002>.

⁶ Nelson W. Polsby et al., *Presidential Elections: Strategies and Structures of American Politics*, 13th ed. (Lanham, MD: Rowan & Littlefield, 2011), 206.

⁷ Hasen, *The Voting Wars*.

⁸ Bruce E. Cain, Todd Donovan, and Caroline J. Tolbert, *Democracy in the States: Experiments in Election Reform* (Washington, DC: Brookings Institute Press, 2008), 5.

⁹ Jay Weiner, *This Is Not Florida: How Al Franken Won the Minnesota Senate Race* (Minneapolis: University of Minnesota Press, 2010), xviii.

¹⁰ Katie Bo Williams, "DHS Designates Election Systems as 'Critical Infrastructure,'" The Hill, January 6, 2017, <https://thehill.com/policy/national-security/313132-dhs-designates-election-systems-as-critical-infrastructure>.

the 2016 U.S. presidential election.¹¹ The subsequent report revealed that voter registration databases in the 2016 elections had been successfully infiltrated by Russian intelligence organizations or their proxies.¹²

Although no evidence of tampering with voter registration databases or voting machines was found, the existing voting infrastructure was deemed vulnerable to attacks from foreign adversaries.¹³ As the 2020 election rapidly approached, Americans were understandably anxious about the integrity and security of the U.S. election infrastructure; voter fraud and foreign interference ranked among their top concerns.¹⁴ Meanwhile, the Cybersecurity and Infrastructure Security Agency (CISA) under Department of Homeland Security (DHS) have taken the lead in collaborating with state and local agencies to improve election security.¹⁵

CISA has made great strides in forging stronger relationships with local, state, and territorial election officials and created best practices for cybersecurity and intelligence sharing all the while failing to look within the DHS family for an affiliate agency to collaborate on election vulnerabilities.

One potential electoral institution partner, the U.S. Secret Service, has successfully employed a 360-degree security approach to protecting the president of the United States and other high-ranking officials since 1902. The Secret Service analyzes each component of a venue or facility and determines how one area may affect the whole, where the threat may come from, and how to mitigate it.

¹¹ Rod J. Rosenstein, *Appointment of Special Counsel to Investigate Russian Interference with the 2016 Presidential Election and Related Manners* (Washington, DC: Office of the Deputy Attorney General, 2017), <https://www.justice.gov/opa/press-release/file/967231/download>.

¹² “The Mueller Report Exposed Weaknesses in U.S. Democratic Institutions that H.R. 1 Would Address,” Brennan Center for Justice, July 10, 2019, <https://www.brennancenter.org/our-work/research-reports/mueller-report-exposed-weaknesses-us-democratic-institutions-hr-1-would>.

¹³ Brennan Center for Justice.

¹⁴ Thad Hall, J. Quin Monson, and Kelly D. Patterson, “Poll Workers and the Vitality of Democracy: An Early Assessment,” *PS: Political Science & Politics* 40, no. 4 (October 2007): 647–54, <https://doi.org/10.1017/S104909650707103X>.

¹⁵ Vijay D’Souza and Rebecca Gambler, *Election Security: DHS Plans Are Urgently Needed to Address Identified Challenges before the 2020 Elections*, GAO-20-267 (Washington, DC: Government Accountability Office, 2020), 2, <https://www.gao.gov/assets/710/704314.pdf>.

Such a methodology could be effective at revealing vulnerabilities and plotting solutions for the U.S. electoral system. Moreover, CISA and the Secret Service have both used red teaming to combat threats, though the agency's employment of the method has been confined to the cybersecurity realm.¹⁶ In fact, the agency has even assisted other DHS agencies with cyber penetration efforts on their networks.¹⁷

It would be a logical next step for CISA and election institutions to consider partnering with the Secret Service in adopting a red-teaming methodology for the electoral system. CISA would be playing the blue team's role by defending its "virtual ground" based on its current best practices. In contrast, Secret Service teams that work in both cyber and site protection fields attempt to penetrate and socially engineer their way into the voting systems and election storage facilities. Additionally, the data gleaned from the virtual exercises could then be passed on to the local or state governments, much like the cybersecurity agency releases warning bulletins to national corporations on matters of software vulnerabilities and malware.

To have faith in the U.S. election system, the agencies assisting in the security of elections must have institutional trust. While CISA is a relatively new federal agency, the Secret Service was established in 1865 and entrusted with safeguarding U.S. currency. The Secret Service upholds its personnel to the motto of "worthy of trust and confidence." The Secret Service dual mission has successfully protected the U.S. financial system and hundreds of world leaders over the last 150 years.

Moreover, federal, state, local, and territorial governments would then approach election security as the Secret Service approaches security advances for the officials they protect; a 360-degree ring of protection that starts long before citizens cast their ballots on election day.

¹⁶ Sean Michael Kerner, "DHS Using Red Team Approach to Identify Cyber-Security Issues," eWeek, August 13, 2018, <https://www.eweek.com/security/dhs-using-red-team-approach-to-improve-national-cyber-security>.

¹⁷ "DHS Teams Hunt for Weaknesses in Federal Cyber Networks," Federal News Network, July 11, 2012, <https://federalnewsnetwork.com/all-news/2012/07/dhs-teams-hunt-for-weaknesses-in-federal-cyber-networks/>.

C. LITERATURE REVIEW

This literature review addresses the current state of security and resilience of the U.S. election system and methods implemented since 2000 to secure them. The first section focuses on cited vulnerabilities to election system technology. The second addresses how election management bodies are created and what effect they have on election security.

1. Technology in U.S. Election Infrastructure

Some studies already analyzed how voting machines are vulnerable to hackers and foreign state actors. A group of election subject matter experts and industry professionals co-wrote *DEF CON 27: Voting Machine Hacking Village*, a report detailing current electronic voting machines' vulnerability to attacks.¹⁸

During the experiments, computer scientists had access over three days to 100 voting machines currently used in U.S. elections, and participants used the tools in their possession to alter votes and infiltrate the voting machines, some of which had been identified as vulnerable over a decade ago.¹⁹

This study also raised concerns over the supply chain for voting machine components, many of which are manufactured overseas in countries often accused of election interference. For example, Alexa Corse concurs with the 2019 Voting Village findings that voting machines are particularly susceptible to hacking because many contain components from China and Russia, adversaries of the United States.²⁰

To drive home her point, Corse references a study conducted by a risk-management company called Interos, which explored the risk of using international components in U.S.

¹⁸ Matt Blaze et al., *DEF CON 27: Voting Machine Hacking Village* (Furlong, PA: Voting Village, 2019), 2, <https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf>.

¹⁹ Blaze et al., 2.

²⁰ Alexa Corse, "Voting-Machine Parts Made by Foreign Suppliers Stir Security Concerns," *Wall Street Journal*, December 16, 2019, <https://www.wsj.com/articles/voting-machine-parts-made-by-foreign-suppliers-stir-security-concerns-11576494003>.

voting machines. Interos recommends that voting machine vendors scrutinize parts supplied by foreign companies.²¹

Various methods can be used to conduct an attack on electronic voting machines. Computer scientist Alex Halderman has published a series of studies since 2006 on the vulnerabilities of election systems and applied threat models to identify potential attackers.²² According to him, malicious code on memory cards or USB devices, which contain software for ballot design and procedures for tallying votes, might be a mode of attack.²³

Independently funded research by Shackelford et al. analyzed national case studies to assist the U.S. electoral system in creating best practices for combating cyber-attacks.²⁴ While this study recognizes the same vulnerabilities to the voting machines that Halderman identified, it draws attention to five key areas within the electoral system susceptible to hacking: pre-election rhetoric, poll books, electronic voting machines, machine tabulation, and post-election dissemination of information.²⁵

Some experts on election integrity have traced the decline of the integrity of U.S. elections. One such group of experts—Pippa Norris, Alessandro Nai, and Max Grompling—conducted a quantitative study called the Election Integrity Project to evaluate election integrity worldwide. The Project surveyed U.S.-based political scientists to measure their regions' election security. On the perception of electoral integrity (PEI) scale, where a score of one is the least secure and 100 is the most secure, the United States scored 64.²⁶

²¹ Corse.

²² J. Alex Halderman, *Testimony: Russian Interference in the 2016 Elections* (Washington, DC: Senate Select Committee on Intelligence, 2017), 2. <https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf>.

²³ Halderman, 4.

²⁴ Scott Shackelford et al., “Making Democracy Harder to Hack,” *University of Michigan Journal of Law Reform* 50 (2017): 629–68.

²⁵ Shackelford et al., 636.

²⁶ Pippa Norris, Alessandro Nai, and Max Grompling, “The Electoral Integrity Project EIP,” Harvard Dataverse, December 15, 2016, <https://doi.org/10.7910/DVN/YXUV3W>.

The project identified hacking by an adversary as a top challenge within the current election system. In a solo project, Norris studied the hacking of voter registration databases and its effect on election integrity, including the Illinois and Arizona voter registration databases that cyber criminals accessed in a 2016 attempt to obtain voter records.²⁷ Norris's study revealed it would take only a few hacks on registration databases or voting machines to cast doubt on election results among voters.²⁸

While voter registration databases, voting machines, and their components are vulnerable to attacks, assessments conducted by CISA's Department of National Cybersecurity Assessments and Technical Team revealed that any time information technology is used to support critical infrastructure, it becomes vulnerable. Moreover, all systems are equally vulnerable.²⁹

2. Election Management Bodies

Election management bodies play a major role in the U.S. electoral system and are vulnerable to manipulation based on their election responsibilities, from organizing, to monitoring, to certifying elections. While plenty of literature is available on voting technology, little scholarly work has addressed election management.

Toby James, a subject matter expert on election management, explored the strengths and vulnerabilities of international election authorities.³⁰ He focused on five key components with election management: process design, resource investment, service output, service outcomes, and stakeholder satisfaction (PROSeS).³¹

²⁷ Pippa Norris, *Why American Elections Are Flawed (and How to Fix Them)* (New York: Cornell University Press, 2017), 15.

²⁸ Norris, 16.

²⁹ Office of Inspector General, *Progress Made, but Additional Efforts Are Needed to Secure the Election Infrastructure* (Washington, DC: Department of Homeland Security, 2019), 3, <https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf>.

³⁰ Toby James, *Comparative Electoral Management: Performance, Networks and Instruments* (London: Routledge, 2019), 3–17, <https://doi.org/10.4324/9781315545172>.

³¹ James, 61.

Within the PROSeS framework, the five elements comprise variables for evaluation. For example, process design comprises the variables of public participation, probity and impartiality, and accountability.³² James's framework helped to identify the strengths and weaknesses of both the U.K. and Canadian systems, whose electoral management structures diverge. By gaining this knowledge, the two countries could create policies to improve their electoral management bodies.³³

Holly Ann Garnett, who also measured multiple variables, argues that the capacity of election management is an indicator of electoral integrity. Garnett defines capacity as "the ability to perform functions and achieve . . . goals."³⁴

Garnett explores whether the quality of content on election websites correlates with high election integrity. This cross-national study from 2012 to 2014 analyzed the websites of 99 international election management bodies by measuring 20 variables and quantifying the results on a Mokken scale of one through three, where three reflects the greatest capacity.³⁵ On the Mokken scale, the United States scored between 1.50 and 1.9.³⁶ Garnett's study, the first of its kind, revealed the significance of the capacity of election management bodies. The higher the confidence in the election official, the more assured the voter is in the electoral process.

Some scholars would argue that poll workers are a key factor in determining the integrity of an election system because having the power to deny someone the right to vote can affect voter confidence in U.S. elections.

³² James, 62–63.

³³ James, 84–85.

³⁴ Holly Ann Garnett, "Evaluating Electoral Management Body Capacity," *International Political Science Review* 40, no. 3 (2019): 335–53.

³⁵ Garnett, 340.

³⁶ Garnett, 342.

Atkeson et al. revealed how vital poll workers are to maintaining election security. This study analyzed whether poll workers discriminated against minority voters in requesting identification.³⁷

The study surveyed New Mexico poll workers and voters and analyzed whether voter identification laws were administered.³⁸ It revealed that poll workers who support voter identification laws are more likely to request a form of identification from a voter therefore demonstrating a lack of consistency amongst poll workers does exist.³⁹

Burden et al. analyzed what transpires at the polling station by reviewing the incident logs that contain voter complaints.⁴⁰ This analysis of 66,000 incident from four different elections in Wisconsin suggested that voters experienced few problems when voting.⁴¹

Self-reporting by elections officials has many advantages although respondents may sometimes be too embarrassed to report mistakes or even social biases. This study revealed that election administrators needed to focus on how the polling location was organized in an effort to prevent such incidents.

In a similar study, Sara Rinfret, Christina Barsky, and Samuel Scott conducted a telephone survey comprising eight questions regarding the voter's experience and confidence in election administrators in Missoula, Montana.⁴² The researchers utilized a five-point scale to index the results, which revealed voters in Missoula had high confidence in their election officials.⁴³ These studies highlight the impact election administrators can

³⁷ Lonna Rae Atkeson et al., "Who Asks for Voter Identification? Explaining Poll-Worker Discretion," *Journal of Politics* 76, no. 4 (2014): 944–57, <https://doi.org/10.1017/s0022381614000528>.

³⁸ Atkeson et al., 944.

³⁹ Atkeson et al., 947–948.

⁴⁰ Barry C. Burden et al., "What Happens at the Polling Place: Using Administrative Data to Look Inside Elections," *Public Administration Review* 77, no. 3 (2017): 354–64.

⁴¹ Burden et al., 354–355.

⁴² Sara Rinfret, Christina Barsley, and Scott Samuel, "Public Perceptions, Elections, Administration, and the Role of Street Level Bureaucrats," *Public Administration Quarterly* 42, no. 4 (December 2018): 493–515.

⁴³ Rinfret, Barsley, and Samuel, 501–502.

have on the U.S. electoral system. The more confident voters are in the official who oversees their polling location, the greater the trust in the overall system.

Some experts have attempted to explore the correlation between election integrity and voters' confidence in the accuracy of their votes, such as the study conducted by R. Michael Alvarez, Thad E. Hall, and Morgan H. Llewellyn on the 2004 election.⁴⁴ In a poll of 2,793 randomly selected voters, researchers found that 11% lacked confidence in the accuracy of their vote, and the higher the confidence in the election system, the more likely registered voters are to vote.⁴⁵

For example, the Pew Research Center conducted a survey of 9,451 adults to determine whether they believed their vote was recorded and counted accurately in the 2018 midterm election.⁴⁶ The study revealed 80% had confidence that their local election administration counted the votes accurately, and 70% were confident in accuracy nationwide.⁴⁷ These studies provide greater insight into voters' confidence in the U.S. election system.

While numerous studies have explored the various components of the electoral system and their impact on election security, no study has evaluated how each component interacts with the others, which ultimately can affect the overall system. As a result, this thesis examines how a systems thinking approach and red teaming can be applied to improve election security by analyzing each of the components, their interactions, and finally, the vulnerabilities and how to fix them.

D. RESEARCH DESIGN

The U.S. electoral system is a complex, decentralized system made up of numerous election administrations, laws, and technologies and influenced by political partisanship.

⁴⁴ R. Michael Alvarez, Thad E. Hall, and Morgan H. Llewellyn, "Are Americans Confident Their Ballots Are Counted?," *Journal of Politics* 70, no. 3 (July 2008): 754–66.

⁴⁵ Alvarez, Hall, and Llewellyn, 758.

⁴⁶ Pew Research Center, *Public Expects Gridlock, Deeper Divisions with Changed Political Landscape* (Washington, DC: Pew Research Center, 2018), 1, <https://www.people-press.org/2018/11/15/public-expects-gridlock-deeper-divisions-with-changed-political-landscape/>.

⁴⁷ Pew Research Center, 1.

Researchers and government officials have often overlooked the interconnection of the system's components and neglected testing their resilience. This thesis studies how the Secret Service conducts security advances through a system's thinking approach and tests its process often utilized by the Department of Defense (DOD), a concept known as "red teaming" and how it can be applied to election security.

Systems thinking provides a framework to analyze how altering one element of the system can have a lasting effect on the system as a whole.⁴⁸ The systems thinking approach examines three components within a system; the elements, the interconnections, and the purpose.⁴⁹ Through this approach, government officials can determine the purpose of the U.S. electoral system and integrate a feedback loop to determine how a change to one component depends on another.

The U.S. Secret Service methodology is akin to systems thinking by revealing how the agency approaches security advances, how effective this method has been at protecting the United States' highest leaders, and how it may be used to modify the U.S. electoral system. For the Secret Service to accomplish its mission of ensuring the world's highest leaders' safety, it must understand the impact each component of an advance has on the other. When conducting advances, the Secret Service relies on various components within the agency, such as the motorcade section and counter-sniper section, to assess their area of expertise for vulnerabilities.⁵⁰ Once the vulnerabilities have been identified, the various components converge to devise a security plan. By discussing each section's security plan, the advance can determine how each plan may affect the others. For continuity, meetings involving agents from each subsection are held at the end of the day to review the overall security plan.

⁴⁸ Donella H. Meadows, *Thinking in Systems: A Primer* (White River Junction, VT: Chelsea Green Publishing, 2008), 17.

⁴⁹ Meadows, 11.

⁵⁰ "The Protective Mission," Secret Service, accessed July 3, 2020, <https://www.secretservice.gov/protection/#who>.

After major security events, the Secret Service conducts after-action reports to determine the executed security plan's effectiveness.⁵¹ Even if an event is successful, the Secret Service sees the benefit of breaking down the security plan piece by piece to identify if any holes were exposed on game day or if plans should be altered in the future to increase security. The Secret Service assesses if the appropriate amount of staffing was utilized, communication effectiveness with law enforcement partners, and security ingress and egress areas. Problems and recommendations are documented in the after-action report and available to the agents who will hand the next major event.

Red teaming challenges an organization's assumptions by imagining a system from an adversary's perspective, thinking outside the box, and perpetuating an attack on the system to identify vulnerabilities.⁵² The DOD and Secret Service commonly use physical and analytical red teaming to train and prepare for and respond to worst-case scenarios. The DOD has been using the concept of red teaming since the Cold War.⁵³ It often utilizes the method to test strategy plans for upcoming missions, the effectiveness of the latest technology, and security for military installations all over the world.⁵⁴ The Secret Service has embraced the concept of red teaming and conducted several tabletop exercises, simulations, and vulnerability probes to assess security plans for its various protective missions.⁵⁵ To understand the threat truly, U.S. election officials must understand the enemy's culture and skill set and how they factor into planning an attack.

A study completed by the Defense Science Board in 2003 revealed, "We believe red teaming is especially important now... Aggressive red teams challenge emerging

⁵¹ Department of Homeland Security Office of Inspector General, *United States Secret Service After-Action Review of Inaugural Security (Redacted)* (Washington, DC: Department of Homeland Security, 2009), 7, https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIGr_10-04_Oct09.pdf.

⁵² University of Foreign Military and Cultural Studies et al., *The Red Team Handbook*, v. 9 (Fort Leavenworth, KS: University of Foreign Military and Cultural Studies, 2018), 69–72, https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf.

⁵³ Micah Zenko, *Red Team: How to Succeed By Thinking Like the Enemy* (New York: Basic Books, 2015), 26.

⁵⁴ Zenko, xxi.

⁵⁵ Edward Connors, *Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement* (Alexandria, VA: Institute for Law & Justice, 2007), 65.

operational concepts in order to discover weaknesses before read adversaries do. Red teaming also tempers the complacency that often follows success.”⁵⁶ For the last decade, foreign adversaries have tested the U.S. electoral system in hopes of identifying gaps that can be exploited to their benefit. Election officials and government agencies have been one step behind this nation’s adversaries in identifying vulnerabilities within the U.S. electoral system. Red teaming may be the answer to solving this problem.

Step one involves identifying the challenges facing the U.S. electoral system from the 2000 election to the recent 2020 election. This thesis highlights the policies implemented to improve the system, the government’s designation of the system as critical infrastructure, and the establishment of greater federal oversight.

Step two explains the U.S. electoral system from start to finish. Election stakeholders must understand how the framers envisioned the electoral process, from its implementation, and how it evolved and became more complex over time. To reinforce the system’s resiliency, election officials, legislatures, and government agencies must have a complete understanding of each step along the way.

Step three demonstrates how systems thinking and red teaming can be applied to specific components within the U.S. electoral system. States began implementing universal mail-in voting as an alternative to in-person voting to protect Americans during a global pandemic. Many states’ rapid implementation failed to recognize how this change would directly impact other components within the system. Mapping out a systems thinking diagram could help election officials identify how the potential change may inadvertently prove to do more harm than good. Lastly, thinking like this nation’s adversaries through red teaming will help election officials identify future vulnerabilities and determine how resilient the U.S. electoral system will be during an attack. It would afford election officials the time they need to establish protocols on how to mitigate the damage if an attack were to happen, because right now, this country is always one step behind.

⁵⁶ Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Defense Science Board Task Force on The Role and Status of DOD Red Teaming Activities* (Washington, DC: Department of Defense, 2003), Memorandum for Chairman, Defense Science Board, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a430100.pdf>.

The thesis's final step is to synthesize the information gleaned from the study and apply it to current election vulnerabilities. Demonstrate how the Cyber agency and the DHS can study how other agencies and the military have successfully applied the methodology of systems thinking and red teaming to its missions; and how it can help identify potential election security vulnerabilities. The results of this thesis highlight a set of recommendations to reinforce the resiliency and security of the U.S. electoral system.

II. U.S. ELECTION SYSTEM (2000–2020)

Electoral integrity first showed signs of cracking in the 2000 presidential election, which led the public to question electoral security. Since then, the United States has experienced the creation of the Help America Vote Act and the Election Assistance, funding to upgrade voting machines but not uniformity, an uptick in legal challenges to election results, and foreign interference through hacking and disinformation campaigns. These challenges have only diminished voter confidence. This chapter analyzes the aforementioned vulnerabilities that have arisen since the 2000 U.S. Presidential election to the 2016 Presidential election.

A. 2000 ELECTION

The fate of the U.S. Presidential election rested entirely on Florida. With the election too close to call, Florida law required that the votes be run through the same tabulation machines once again to determine whether the machines had caused an error.⁵⁷ Unsatisfied with the machine recount, presidential nominee Al Gore requested a hand recount in a few Democratic-leaning counties (Figure 1).⁵⁸ Over the next 36 days, America learned how flawed its election system was, made manifest in outdated voting machines and poorly designed ballots, to weak election laws and partisan election officials, to the questionable validity of absentee votes.⁵⁹

⁵⁷ Hasen, *The Voting Wars*, 12.

⁵⁸ Hasen, 12.

⁵⁹ Hasen, 11–40.



Figure 1. Broward County Judge Reviews Punch Card Ballot in Florida Recount.⁶⁰

One of the many questions that arose in Florida involved the use of outdated voting machines, chiefly punch-card machines.⁶¹ Of the different machines used in Florida, the punch-card machine, which represented 20% of all machines nationwide, proved unreliable and scored the worst in vote accuracy.⁶² A punch card machine utilized a metal pin to punch a hole next to the name of the candidate of their choosing, which produced a hanging chad.⁶³ The ballot design, called the butterfly ballot, only exacerbated the problems with the machines in Florida, and Democrats argued the design led voters to select the unintended candidate by mistake.⁶⁴ The ballot design was heavily scrutinized in Palm Beach County, where the election supervisor had placed the candidates' names on both sides of the holes to assist the elderly in navigating the vast number of candidates.⁶⁵ The

⁶⁰ Elving, "The Florida Recount of 2000."

⁶¹ Hasen, *The Voting Wars*, 12.

⁶² Hasen, 15.

⁶³ Enrico Spolaore and Phillip Garner, "Why Chads? Determinants of Voting Equipment Use in the United States," *Public Choice* 123 (February 1, 2005): 363–92, <https://doi.org/10.1007/s11127-005-7167-0>.

⁶⁴ Hasen, *The Voting Wars*, 16.

⁶⁵ Hasen, 16.

ballot design combined with the machine's inaccuracy led to confusion among voters and incorrect votes.⁶⁶

Ballot design and voting machines were not the only controversy in Florida, so were the laws governing the recount. Florida election laws failed to provide clear and concise guidelines for determining the intent of a vote or conducting a recount.⁶⁷ Florida election laws dictate it is left up to the Chief Election Official, Secretary of State, to interpret and certify election results.⁶⁸ Democrats were particularly concerned over how the Republican Secretary interpretation of absentee ballot laws in Florida would benefit George W. Bush.⁶⁹ For ballots to count, Florida law states the ballots must contain an election date postmark.⁷⁰ The Secretary read the law to state that as long as the ballots encompassed a foreign postmark and were received within the 10-day allotment period, the votes should be counted.⁷¹

Furthering the problem was the fact that the Secretary of State was the co-chair of Presidential nominee Bush in Florida.⁷² The perceived conflict of interest and imprecise laws lead both parties to file lawsuits following the election.⁷³ The Gore campaign opted to request a manual recount to protect voters from outdated voting machines' flaws.⁷⁴ A recount in several counties sought to decipher voter's intent on ballots initially disqualified due to mechanical error. Republicans filed a lawsuit and went before the Florida Supreme Court who ruled in favor of the Democrats. Once again, the Bush campaign shared their dismay by appealing to the U.S. Supreme Court. The case went before the Supreme Court,

⁶⁶ Hasen, 16.

⁶⁷ Hasen, 20.

⁶⁸ Fla. Stat. § 101.5614(5) (2000).

⁶⁹ Hasen, *The Voting Wars*, 26.

⁷⁰ Fla. Admin § 1S.2.013(7) (1984).

⁷¹ Hasen, *The Voting Wars*, 26.

⁷² Hasen, 26.

⁷³ Hasen, 11–40.

⁷⁴ Hasen, 21.

which ruled in favor of Bush, which ended the Florida recount.⁷⁵ While Americans were relieved finally to have an official President, it highlighted many flaws in the U.S. electoral system.

1. The Help Act and the Election Commission

In the wake of the 2000 election, Congress passed election reform through the Help America Vote Act of 2002.⁷⁶ Congress sought assistance from state and local governments to determine the area's most in need of funding to improve election administration.⁷⁷ The Help Act appropriated federal funding for upgraded voting machines, the creation of statewide voter registration databases, education for poll workers, and provisional voting were key components to the Help Act.⁷⁸

Prior to the Help Act, the Federal Election Commission's Office of Election Administration provided federal election administration assistance.⁷⁹ Federal Election Administrative oversight was housed under the Federal Election Commission with the primary duties to provide information to the public, conduct research, and create guidelines for voting systems.⁸⁰ The 2000 election caused legislators to re-evaluate the role of the Feds.⁸¹ Congress saw the need for an independent bi-partisan agency to oversee the distribution of federal funding to the states, testing of voting machines, conducting research, and creating administrative guidelines outlined in the Help Act.⁸² Under the

⁷⁵ *Britannica* s.v. "Bush v. Gore, summary, decision, significance, & facts," accessed September 19, 2020, <https://www.britannica.com/event/Bush-v-Gore>.

⁷⁶ Arthur L. Burris and Eric Fischer, *The Help America Vote Act and Election Administration: Overview of 2016* (Washington, DC, Congressional Research Service, 2016), 1.

⁷⁷ Burris and Fischer, 3.

⁷⁸ Daniel Palazzolo et al., "Election Reform after HAVA: Voter Verification in Congress and the States," *Publius: The Journal of Federalism* 38, no. 3 (January 1, 2008): 515–37, <https://doi.org/10.1093/publius/pjn013>.

⁷⁹ Burris and Fischer, *The Help America Vote Act and Election Administration*, 2.

⁸⁰ Burris and Fischer, 2.

⁸¹ Burris and Fischer, 1.

⁸² Burris and Fischer, 1.

passage of the Help Act, the Election Assistance Commission would take over the primary responsibilities held by the previous federal election administrators.⁸³

2. Voting Technology

The Election Commission would provide the funding the states needed to upgrade election technology.⁸⁴ States first had to qualify for assistance from the Help Act and agree to replace the outdated voting infrastructure before November 2004 to receive funding or request an extension until 2006.⁸⁵ The new infrastructure would afford voters the ability to verify and change their vote prior to submitting.⁸⁶ Under Title III of the Help Act, the voting system needed to be handicapped accessible, provide a paper copy of each ballot cast, and provide alternative languages.⁸⁷ Nevertheless, the Help Act failed to standardize what type of voting machines should be purchased, which thus allowed each state the authority to purchase whatever electronic voting machine it deemed appropriate.⁸⁸ The quick fix led to states purchasing machines without doing their due diligence to verify the security procedures in place for the machines.⁸⁹ The idea of votes being stored on the computer's memory was concerning for some state election officials.⁹⁰ In an effort to calm fears, the Commission offered states the ability to have the voting infrastructure tested and certified.⁹¹

⁸³ Election Assistance Commission, *History of the National Clearinghouse on Election Administration* (Washington, DC: Election Assistance Commission, 2019), 1.

⁸⁴ Department of Justice, "The Help America Vote Act of 2002."

⁸⁵ Margot Adams, "The Voting Technology Problem," Stanford Law School, January 16, 2018, <https://pacscenter.stanford.edu/publication/the-voting-technology-problem/>.

⁸⁶ Department of Justice, "The Help America Vote Act of 2002."

⁸⁷ "Help America Vote Act," U.S. Election Assistance Commission, accessed May 13, 2020, https://www.eac.gov/about_the_eac/help_america_vote_act.aspx.

⁸⁸ Adams, "The Voting Technology Problem."

⁸⁹ Adams.

⁹⁰ Burris and Fischer, *The Help America Vote Act and Election Administration*, 12.

⁹¹ Burris and Fischer, 3.

While the Help Act provided much needed funding to upgrade voting systems, delayed funding, lack of faith in the security of new systems, and lack of mandatory testing ultimately contributed to minor changes.⁹²

3. Voter Identification, Databases, and Provisional Voting

The 2000 election highlighted flaws with Florida's voter registration database. Unfortunately, for Florida, and the third party company they utilized for removal, they inadvertently removed 2,000 individuals who had been mislabeled.⁹³ This error led to legally registered voters being denied the right to vote due a clerical error.⁹⁴ This error resulted in lawsuits and the creation of independent studies to determine what recommendations should be made towards election reform for voter registration databases.⁹⁵

The Carter-Ford Commission, a bi-partisan commission, recommended that voters produce a form of government identification or equivalent when registering and casting a vote on Election Day.⁹⁶ It seemed the public agreed with the Carter Commission; a Gallup poll taken in 2016 suggested that 80% of surveyed Americans were in favor of presenting a form of identification at polling locations.⁹⁷ The Help Act did not include a requirement to provide government identification at the time of voting, but it did enact the requirement to provide a valid id or proof of residency when registering to vote via mail in a new district.⁹⁸

⁹² Adams, "The Voting Technology Problem."

⁹³ Ari Berman, "How the 2000 Election in Florida Led to a New Wave of Voter Disenfranchisement," July 28, 2015, <https://www.thenation.com/article/archive/how-the-2000-election-in-florida-led-to-a-new-wave-of-voter-disenfranchisement/>.

⁹⁴ Hasen, *The Voting Wars*, 28.

⁹⁵ Eric A. Fischer, R. Sam Garrett, and L. Paige Whitaker, *State Voter Identification Requirements: Analysis, Legal Issues, and Policy Considerations* (Washington, DC: Congressional Research Service, 2016), 43.

⁹⁶ Fischer, Garrett, and Whitaker, 2.

⁹⁷ Justin McCarthy, "Four in Five Americans Support Voter ID Laws, Early Voting," Gallup, August 22, 2016, <https://news.gallup.com/poll/194741/four-five-americans-support-voter-laws-early-voting.aspx>.

⁹⁸ Fischer, Garrett, and Whitaker, *State Voter Identification Requirements*, 2.

Prior to the Help Act, states had the ability to house voter registration data in the mechanism of their choosing. In an effort to streamline voter registration information, the Help Act requires each state to create and maintain a computerized electronic database of registered voters.⁹⁹ This requirement will increase the security of the information, make it readily accessible to election officials and poll workers, and provide the ability to link to the state's Department of Motor Vehicle and social security offices to verify the accuracy of the information.¹⁰⁰ The Help Act offered guidance to states on building the database but did not provide any formal requirements for the states to meet.¹⁰¹

While the Help Act made improvements to voter registration and databases, the lack of uniformity among states on verifying voters' identity has led to misinterpretations of the law by poll workers, which led to some voters being turned away on election day.¹⁰² States themselves set the laws regarding what identification is needed to register to vote, cast a ballot, or vote via mail-in or absentee ballot.¹⁰³

In an attempt to prevent voters from being denied their right to vote due to an error within a voter registration database, the Help Act required election officials to allow the individual to cast a provisional ballot.¹⁰⁴ If voters arrive at a polling location and their name is absent from the pollbook, or the address does not match the address on the voter's ID, then the voter will be allowed to cast a provisional ballot. Once election officials verify a registered voter did indeed cast the provisional ballot, it is added to the official count.¹⁰⁵ Voters and candidates are worried that provisional ballots are not being counted during elections. The Election Commission reported that from 2006 to 2016, 31% of provisional

⁹⁹ Burris and Fischer, *The Help America Vote Act and Election Administration*, 2.

¹⁰⁰ Help America Vote Act, Public Law 107-252, *U.S. Statutes at Large* 1666 (2002): 1, <https://www.congress.gov/107/plaws/publ252/PLAW-107publ252.pdf>.

¹⁰¹ Burris and Fischer, *The Help America Vote Act and Election Administration*, 11.

¹⁰² Fischer, Garrett, and Whitaker, *State Voter Identification Requirements*, 7.

¹⁰³ Government Accountability Office, *ELECTIONS: State Laws Addressing Voter Registration and Voting on or before Election Day*, GAO-13-90R (Washington, DC: Government Accountability Office, 2012), 7.

¹⁰⁴ Help America Vote Act.

¹⁰⁵ Matt Vasilogambos, "Provisional Ballots Protect Voting Rights—When They Are Counted," PEW, November 16, 2018, <https://pew.org/2B8JRC6>.

ballots were not counted.¹⁰⁶ This statistic could lead voters to distrust election results. These statistics give validity to claims of voter suppression and voter fraud. Any vote not accurately counted is a failure on the part of the voting system. In the 2016 Presidential election, the Commission reported over 2.4 million provisional ballots were cast.¹⁰⁷ It is clear from the number of provisional ballots cast in 2016 that election administrators and the Commission need to take a closer look at how to improve the accuracy of voter registration databases and provide information to the public on voter identification laws to prevent voters from doubting the election results.

4. Recounts and Lawsuits

The 2000 election was just the beginning of many recounts and lawsuits to be filed because of an election and election management decisions.

In 2004, Secretary of State Kenneth Blackwell made the ill-advised decision to serve as President Bush's re-election team's co-chair.¹⁰⁸ Due to controversial decisions on voter registration forms and denial of provisional ballots, the public began to doubt partisan officials' ability to be impartial during election issues.¹⁰⁹ Many voters in Ohio saw it was a clear abuse of power since his decisions seem to favor President Bush.¹¹⁰ Blackwell's decisions resulted in long lines, challenges casting a provisional vote, and some never casting a vote at all.¹¹¹ The idea that the state election official is abusing his position will lead to voters to lose faith in the integrity of the election system. Citizens should be able to trust their chief election officers to make decisions based on what is best for the public and not themselves.

¹⁰⁶ Vasilogambos.

¹⁰⁷ Vasilogambos.

¹⁰⁸ Brennan Center for Justice, *Former Ohio Elections Chief Blackwell Brings a Troubled Record on Elections to Fraud Commission* (New York: New York University School of Law, n.d.), 1, accessed September 8, 2020, https://www.brennancenter.org/sites/default/files/analysis/Ken_Blackwell.pdf.

¹⁰⁹ Hasen, *The Voting Wars*, 120.

¹¹⁰ Brennan Center for Justice, *Former Ohio Elections Chief Blackwell Brings a Troubled Record on Elections to Fraud Commission*, 1.

¹¹¹ Brennan Center for Justice, 2–3.

Unfortunately, for Ohio, the 2008 Presidential election was just as divisive as the 2004 election. This time, the Republicans were accusing the Democratic Secretary of interpreting election laws in favor of Democrats.¹¹² The chief election official made controversial decisions on an absentee voter's qualification status and voter registration laws.

In this particular case, the issue came down to an administrative issue regarding absentee ballot requests.¹¹³ For absentee ballots to be sent out to voters, the voters must include a statement that they are "qualified voters."¹¹⁴ According to Ohio law, voters must include the statement but do not have to check the box next to the statement for the ballot to be sent out.¹¹⁵ The McCain campaign checked the box next to the statement for the one million registered Republican voters in Ohio.¹¹⁶ When forms began to show up without the box checked, Secretary Brunner advised county election officials to forgo sending the absentee ballot and stated they were not "qualified voters."¹¹⁷ This situation led to another showdown, and this time in the Ohio Supreme Court, which ruled against Secretary Brunner.¹¹⁸

A battle over absentee ballots was not the only run-in Brunner had with Republicans in 2008 over election laws. This time, Republicans challenged Brunner's interpretation of voter registration laws.¹¹⁹ Republicans argued a loophole that combined the requirement for voters to register 30 days prior to the election. The "early voting program" granting voters the ability to cast their votes 35 days before the election would lead to fraud.¹²⁰

¹¹² Hasen, *The Voting Wars*, 107–108.

¹¹³ Hasen, 107.

¹¹⁴ Hasen, 107–108.

¹¹⁵ "Absentee Voting," Ohio Secretary of State, accessed September 8, 2020, <https://www.ohiosos.gov/elections/voters/absentee-voting/>.

¹¹⁶ Hasen, *The Voting Wars*, 107.

¹¹⁷ Hasen, 107.

¹¹⁸ *Colvin v. Brunner*, State ex rel., 120 Ohio St.3d 110 (Ohio Supreme Ct. 2008-Ohio-5041).

¹¹⁹ Hasen, *The Voting Wars*, 109.

¹²⁰ Hasen, 109.

Democrats capitalized on the ability to register new voters and have them vote on the same day.¹²¹ This loophole led Democrats to gain approximately 13,000 new registered voters who registered and voted the same day in the 2008 U.S. Presidential election.¹²² Republicans called foul, arguing to the Ohio Supreme Court that it violated the voter registration law of having to register 30 days prior to the election.¹²³ The Ohio Supreme Court disagreed, stating since the vote was not counted until Election Day, it was not in violation of the law.¹²⁴

The Ohio Court cases have once again shown a light on the chief's election official's inability to be bi-partisan. These issues need to be addressed to restore the public's faith in U.S. election officials and trust in the U.S. election system.

B. 2016 PRESIDENTIAL ELECTION

The 2016 presidential election introduced the American public and government officials to a whole new set of election challenges. Federal, state, and local election officials were facing the threat of foreign interference through social media, voting machines, and voter registration databases. The American people heard terms from the U.S. government, such as disinformation, deep fakes, fake bots, and hacking.

1. Social Media and Fake News

Americans have relied on social media outlets for their news for most of the 21st century.¹²⁵ A Pew Research Center survey taken in January 2016 revealed that 35% of young Americans between 18 and 29 received their election and political information from social media.¹²⁶ Social media has provided the opportunity for everyone to have a

¹²¹ Hasen, 110.

¹²² Hasen, 110.

¹²³ Hasen, 110.

¹²⁴ *Brunner*, 23.

¹²⁵ Jeffrey Gottfried et al., "Where Americans Are Getting News About the 2016 Presidential Election," *Pew Research Center's Journalism Project* (blog), February 4, 2016, <https://www.journalism.org/2016/02/04/the-2016-presidential-campaign-a-news-event-thats-hard-to-miss/>.

¹²⁶ Gottfried et al.

voice.¹²⁷ The challenge with everyone having a voice is it affords an individual the ability to post or forward any story without oversight or fact checking.¹²⁸ Traditional journalists must verify facts before they are published.¹²⁹

The terms disinformation and misinformation became extremely popular during the 2016 election and social media platforms were a catalyst for spreading the information.¹³⁰ Misinformation is defined as taking the information believed to be true and sharing it with others.¹³¹ Disinformation, however, is purposefully spreading incorrect information to others in an attempt to manipulate them.¹³² Studies have revealed Facebook was the primary source of disinformation among American voters.¹³³ A Pew Research Center survey in November 2016 revealed 79% of internet users used Facebook.¹³⁴ Facebook CEO Mark Zuckerberg stated the following when testifying before the joint Senate committee:

It's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here.¹³⁵

¹²⁷ Ruth A. Harper, "The Social Media Revolution: Exploring the Impact on Journalism and News Media Organizations," *Inquiries Journal* 2, no. 03 (2010): 1, <http://www.inquiriesjournal.com/articles/202/the-social-media-revolution-exploring-the-impact-on-journalism-and-news-media-organizations>.

¹²⁸ Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (Spring 2017): 211–36.

¹²⁹ Harper, "The Social Media Revolution."

¹³⁰ Danielle Kurtzleben, "Did Fake News on Facebook Help Elect Trump? Here's What We Know," NPR, April 11, 2018, <https://www.npr.org/2018/04/11/601323233/6-facts-we-know-about-fake-news-in-the-2016-election>.

¹³¹ Dictionary.com, s.v. "'misinformation' vs. 'disinformation': get informed on the difference," May 15, 2020, <https://www.dictionary.com/e/misinformation-vs-disinformation-get-informed-on-the-difference/>.

¹³² Dictionary.com.

¹³³ Allcott and Gentzkow, "Social Media and Fake News in the 2016 Election."

¹³⁴ Shannon Greenwood, Andres Perrin, and Maeve Duggan, "Demographics of Social Media Users in 2016," Pew Research Center: Internet, Science & Tech, November 11, 2016, <https://www.pewresearch.org/internet/2016/11/11/social-media-update-2016/>.

¹³⁵ *Facebook, Social Media Privacy, and the Use and Abuse of Data*, Senate, 115th Cong., 2nd sess., April 10, 2018.

Social media is responsible for 40% of the visits to “fake news” sites.¹³⁶ Even if “fake news” was not responsible for the overall election results, it might have directly impacted a specific set of voters.¹³⁷

Ohio State University researchers conducted a study in 2016 on 2012 Obama voters.¹³⁸ To determine how disinformation plays into elections, the researchers provided false news statements about Hillary Clinton to the surveyors.¹³⁹ The results revealed that those who believed the “fake news” were 3.9 times more likely to vote against Clinton in the election.¹⁴⁰

The Internet Research Agency was responsible for the majority of the disinformation.¹⁴¹ The Research Agency entered into a social media campaign to cause chaos and discord among Americans.¹⁴² The agency completed its due diligence on social media apps for political sites in an effort to perfect its manipulation campaign.¹⁴³ It engaged in identity theft, training for social media specialists, round-the-clock monitoring and posting on sites, creating group pages, political advertisements, and providing derogatory information on Hillary Clinton.¹⁴⁴ Several rallies created under stolen U.S. identities were organized in an effort to garner support for Trump.¹⁴⁵

¹³⁶ Kurtzleben, “Did Fake News on Facebook Help Elect Trump?”

¹³⁷ Richard Gunther, Paul A. Beck, and Eric C. Nisbet, “Fake News Did Have a Significant Impact on the Vote in the 2016 Election: Original Full-Length Version with Methodological Appendix,” *The Conversation*, February 15, 2018.

¹³⁸ Gunther, Beck, and Nisbet.

¹³⁹ Gunther, Beck, and Nisbet.

¹⁴⁰ Gunther, Beck, and Nisbet.

¹⁴¹ Allcott and Gentzkow, “Social Media and Fake News in the 2016 Election.”

¹⁴² *U.S. VS Internet Research Agency, LLC*, No. Case 1:18-cr-00032-DLF, 3–4 (District of Columbia February 16, 2018).

¹⁴³ *Internet Research Agency, LLC*, 6.

¹⁴⁴ *Internet Research Agency, LLC*, 3–37.

¹⁴⁵ *Internet Research Agency, LLC*, 20–23.

The Research Agency favored the use of Facebook and Twitter in its disinformation campaign.¹⁴⁶ Facebook and Twitter collectively determined 4,284 accounts were maintained and controlled by representatives of the agency and exposed to over 127 million individuals.¹⁴⁷ They released this information through various online personas in an effort to conceal their true identity.¹⁴⁸

While it might never be honestly known if Russia's manipulation of disinformation directly affected the outcome of the 2016 U.S. presidential election, it has been proven that a disinformation campaign was utilized on social media apps as a mechanism to influence voters' opinions of the 2016 U.S. Presidential election.

2. Vulnerability of Election Infrastructure

Not only did Russia utilize social media as a means of “information warfare,” but agents working on behalf of the Russian government infiltrated the Democratic National Committee (DNC) emails and states voting machines, and voter registration databases.¹⁴⁹ The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), Russian Army Intelligence, hacked into the DNC email accounts and the Clinton campaign and then released the documents and emails under bogus identities.¹⁵⁰ Spear phishing was a tool Russian Intelligence used to access DNC and Clinton campaign staffers and volunteers' access credentials.¹⁵¹ Once the GRU was able to gain access to the networks, they installed malware that allowed for data transfers, the ability to take screenshots, and log keystrokes.¹⁵² The information retrieved from these databases involved campaign strategy, information on Clinton's competitor, and financial

¹⁴⁶ Robert S. Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: Department of Justice, 2019), 14–15, <https://www.justice.gov/storage/report.pdf>.

¹⁴⁷ Mueller, 4–141.

¹⁴⁸ *Internet Research Agency, LLC*, 17.

¹⁴⁹ Mueller, *Report on the Investigation*, 15.

¹⁵⁰ Mueller, 4–5.

¹⁵¹ Mueller, 36–38.

¹⁵² Mueller, 38–40.

information.¹⁵³ They were strategic in its release of the information. For example, almost immediately after the media released disparaging information on Donald Trump, they would release illegally obtained emails and documents involving Hillary Clinton.¹⁵⁴

The GRU's hacking mission continued with the scoping out of various election websites to identify vulnerable penetration points within election infrastructure.¹⁵⁵ A DHS investigation revealed Russia's intent to infiltrate all 50 states' election websites, but the Russian Intelligence failed to access most states' websites.¹⁵⁶ However, they were able to penetrate Illinois's state election infrastructure and gain access to over 200,000 voter registration content.¹⁵⁷ This access gave them the ability to manipulate voters' information that caused potential voting implications on Election Day.¹⁵⁸ While they did gain access, investigators did not find hard evidence of altered voter registration information.¹⁵⁹ Overall, it is believed that they infiltrated a small number of state election sites, but confirmation of actual information being altered has not been found.

The GRU sought to infiltrate a private company that provides software to election voting machines and registration databases.¹⁶⁰ The goal was to gain intelligence on the databases' software and hardware and obtain voters' personal identification information.¹⁶¹ An investigation revealed it successfully hacked into a U.S. vendor's

¹⁵³ Mueller, 41–42.

¹⁵⁴ Mueller, 4.

¹⁵⁵ Mueller, 50.

¹⁵⁶ *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views (Redacted)*, Senate, 116th Cong., 1st sess., July 25, 2019, 12, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

¹⁵⁷ *Report of the Select Committee on Intelligence*, 22–24.

¹⁵⁸ *Report of the Select Committee on Intelligence*, 23.

¹⁵⁹ *Report of the Select Committee on Intelligence*, 23.

¹⁶⁰ *United States of America v. Viktor Borisovich Netyksho [and 11 others]*, defendants, case 1:18-cr-00215-ABJ (District of Columbia 2018).

¹⁶¹ *Viktor Borisovich Netyksho*, 25–26.

network.¹⁶² It then used the information obtained from the U.S. vendor to conduct a spear phishing attack on election administrative personnel in select counties in Florida.¹⁶³

While no evidence of votes being altered has been found, it is obvious from the Mueller Report that the Russians used the 2016 U.S. Presidential election as a test run for future elections and continues to be a threat to U.S. election security. The infiltration of voter registration databases, election websites, and campaign emails reveal to U.S. foreign adversaries the tools needed to influence a future U.S. election. Russia's ability to infiltrate voting infrastructure highlighted the vulnerability of the U.S. voting infrastructure. The Obama administration recognized the area of vulnerability and began researching how to mitigate the threat and enhance security protocols.

C. CREATION OF A CYBER AGENCY TO PROTECT THE U.S. ELECTION SYSTEM

In an effort to protect U.S. democracy from foreign interference in the future U.S. elections, the Obama Administration designated election infrastructure as "critical infrastructure."¹⁶⁴ This designation led to many questions from state and local election officials regarding the federal government's involvement and influence over election security.¹⁶⁵ The responsibility for election infrastructure initially fell to the already established National Protection and Program Directorate. The Directorate created critical infrastructure security plans for those areas that had been identified as critical infrastructure by Homeland Security; to date, 16 critical infrastructure sub sectors.¹⁶⁶

One of the first steps the Directorate took was to create an election task force that involved federal, state and local election officials to improve information sharing involving

¹⁶² Viktor Borisovich Netyksho, 26.

¹⁶³ Viktor Borisovich Netyksho, 26.

¹⁶⁴ "Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," Department of Homeland Security, January 6, 2017, <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.

¹⁶⁵ Election Assistance Commission, *Starting Point: U.S. Election Systems as Critical Infrastructure* (Washington, DC: Election Assistance Commission, 2017), 1, https://www.eac.gov/sites/default/files/eac_assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

¹⁶⁶ Election Assistance Commission, 1.

threats against election infrastructure.¹⁶⁷ The Directorate initiated a Government Coordinating Council to focus on risk assessments, incident response, cybersecurity advising, and training resources for state and local election administrators.¹⁶⁸ In February 2018, the Directorate saw the need to create an additional council, the Subsector Coordinating Council, specifically to coordinate with private sector entities that provide election-related services for U.S. elections.¹⁶⁹ The councils worked diligently to provide state and local officials with guidance on election security.¹⁷⁰ The increase of foreign interference in 2016 caused legislators to replace the Directorate with an independent agency within DHS, the Cybersecurity and Infrastructure Security Agency, in 2018.¹⁷¹ The Cyber Agency continued its collaboration with state and local election officials but emphasized the need for a more inclusive working relationship between the private and public sectors to combat and mitigate cyber-attacks on U.S. critical infrastructure.¹⁷²

The institution was met with challenges from the start.¹⁷³ The role of Director remained vacant for months, lacked the necessary staffing levels, and failed to set performance metrics.¹⁷⁴ While faced with limitations, the Cyber Agency focused on forging a stronger relationship with election stakeholders.¹⁷⁵ This strengthening was done by creating two separate divisions within the agency.¹⁷⁶ The Cybersecurity Division's

¹⁶⁷ "NPPD at a Glance," National Protection and Programs Directorate, February 13, 2018, <https://www.cisa.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf>.

¹⁶⁸ "Written Testimony of NPPD for a House Oversight and Government Reform Subcommittees on Information Technology and Intergovernmental Affairs Hearing Titled 'Cybersecurity of Voting Machines,'" Department of Homeland Security, November 29, 2017, <https://www.dhs.gov/news/2017/11/29/written-testimony-nppd-house-oversight-and-government-reform-subcommittees>.

¹⁶⁹ D'Souza and Gambler, *Election Security*, 13.

¹⁷⁰ D'Souza and Gambler, 13.

¹⁷¹ Cynthia Brumfield, "What Is the CISA? How the New Federal Agency Protects Critical Infrastructure," CSO Online, July 1, 2019, <https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html>.

¹⁷² Brumfield.

¹⁷³ Office of Inspector General, *Progress Made*, 10.

¹⁷⁴ Office of Inspector General, 10.

¹⁷⁵ Office of Inspector General, 13–14.

¹⁷⁶ Office of Inspector General, 6–7.

responsibility was to ensure the integrity of the systems and networks and the Infrastructure Security Division took the lead on securing election facilities.¹⁷⁷ This separation of duties allowed those divisions to liaison with their respective election stakeholders more efficiently.

In 2018, the Cyber Agency began a new initiative of running tabletop exercises to prepare state and local officials for threats they may face in future elections.¹⁷⁸ The exercises inspired some state and local election officials to begin conducting exercises of their own.¹⁷⁹ The success of the 2018 “Tabletop the Vote” by this institution resulted in an additional exercise being executed in 2019.¹⁸⁰

A previous complaint from election shareholders was that the Cyber Agency failed to provide intelligence information on active threats.¹⁸¹ The Cyber Agency management recognized this challenge, and as a result, created the Election Infrastructure Information Sharing and Analysis Center to provide intelligence, technical, and operational support.¹⁸² In an effort for transparency, the Analysis Center provides quarterly reports to state and local election officials.¹⁸³ One of the Cyber Agency’s roadblocks is that state and local election officials do not possess the appropriate security clearance to receive the intelligence or the ability to access a secure facility to receive it effectively.¹⁸⁴ For this reason, the Cyber Agency was forced to work with the cybersecurity industry to create a method in which they can share the information.¹⁸⁵

¹⁷⁷ Office of Inspector General, 6.

¹⁷⁸ D’Souza and Gambler, *Election Security*, 16–17.

¹⁷⁹ D’Souza and Gambler, 22.

¹⁸⁰ D’Souza and Gambler, 16.

¹⁸¹ Office of Inspector General, *Progress Made*, 8.

¹⁸² D’Souza and Gambler, *Election Security*, 17–18.

¹⁸³ D’Souza and Gambler, 18.

¹⁸⁴ D’Souza and Gambler, 24.

¹⁸⁵ D’Souza and Gambler, 24.

An additional area of focus for the Cyber Agency has been providing technical and operational assistance to state and local election officials.¹⁸⁶ While the Cyber Agency has been successful in advising numerous election officials on best practices for cybersecurity, not all state and local officials have been unable to take advantage of these services due to the lack of calendar space.¹⁸⁷ The 2018 midterm election was an opportunity for the Cyber Agency and Homeland Security to evaluate the security plans and operations implemented since its inception. Prioritizing risks, providing special services, and intelligence sharing were areas the Cyber Agency needed to enhance.¹⁸⁸

The after-action report recommended internal changes for the Cyber Agency. The newly established agency lacked permanent leadership, direction, and resources necessary to complete tasks.¹⁸⁹ Suppose an election official or frontline worker reaches out for assistance on Election Day. In that case, they lack the appropriate communication channels to receive notification of an incident and the response mechanisms necessary to rectify an issue in a timely manner.¹⁹⁰

While strides have been made, the Cyber Agency is running out of time to meet the goal of forging stronger stakeholder relationships and educating the public and election administrators. As of November 2019, they were still actively working on a strategic and operational plan for challenges facing U.S. elections.¹⁹¹ The lessons learned from the 2016 election left officials focused on increasing the security of electronic voting infrastructure. U.S. adversaries took notice and began searching for additional ways to manipulate the system.

¹⁸⁶ D’Souza and Gambler, 15–19.

¹⁸⁷ D’Souza and Gambler, 23.

¹⁸⁸ D’Souza and Gambler, 28.

¹⁸⁹ D’Souza and Gambler, 29–30.

¹⁹⁰ D’Souza and Gambler, 30.

¹⁹¹ D’Souza and Gambler, 26.

D. 2020 ELECTION

Although lessons were learned from 2016, the 2020 election was not without its challenges. Ongoing disinformation campaigns from this nation's foreign adversaries, attacks on mail-in voting, and a global pandemic, exposed new vulnerabilities within the U.S. election system.

Foreign interference continued to be a threat to the U.S. election system in 2020. Russia, China, and Iran all had a stake in the Presidential election outcome and utilized social media as a weapon to create discord in the United States and cast doubt on the legitimacy of the election.¹⁹² The Intelligence Community, federal agencies, and private industry worked closely together to combat the threat.

The Federal Bureau of Investigation (FBI), Office of the Director of National Intelligence, and the Homeland Security Cyber Agency testified before the House of Representatives and Senate that foreign adversaries continued to manipulate American voters through social media and state-controlled news outlets.¹⁹³ While Russia's influence was not as prevalent as 2016, China and Iran saw the results of the 2016 influence and engaged in their own campaigns to disrupt or alter the 2020 elections in their favor. Russia actively targeted former Vice President Biden and his campaign to ensure President Trump was re-elected to office.¹⁹⁴ The Russians continued to use social media and the internet to spread disinformation but turned to previous familiar tactics, such as using state-controlled news to influence U.S. elections.¹⁹⁵

China took a specific interest in influencing the outcome of the 2020 U.S. Presidential election. U.S. intelligence reports revealed the Chinese disapproved of the current administration's hostile rhetoric against them, which led them to initiate their own

¹⁹² "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," Office of the Director of National Intelligence, August 7, 2020, <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>.

¹⁹³ Jen Kirby, "Are China and Iran Meddling in U.S. Elections? It's Complicated," Vox, September 15, 2020, <https://www.vox.com/21418513/china-iran-us-election-meddling-russia>.

¹⁹⁴ Office of the Director of National Intelligence, "Statement by NCSC Director William Evanina."

¹⁹⁵ Kirby, "Are China and Iran Meddling in U.S. Elections?"

disinformation campaign within the United States to oust the current administration from office.¹⁹⁶ In September 2020, Facebook identified and removed over 100 accounts with links to China.¹⁹⁷ Many election security and intelligence experts believed China was simply utilizing social media to persuade Americans to see China in a more positive light rather than influencing the outcome of an election.¹⁹⁸ The 2020 election would not be China's first attempt at swaying an election in their favor. In 2019, China launched a series of social media and fake news campaigns against Taiwan's current President.¹⁹⁹ While China's plan was unsuccessful, it revealed they were willing to engage in the use of Facebook, Twitter, and YouTube to influence another country's election.²⁰⁰

Iran looked to capitalize on the 2016 U.S. Presidential election's vulnerabilities to create distrust amongst voters.²⁰¹ Tactics included engaging in voter intimidation and disinformation campaigns. The Intelligence Community reported the Iranian's produced a bogus video highlighting the potential for mail-in voter fraud and a demonstration of how easily a voting machine could be hacked or ballots could be altered to lead to voter fraud.²⁰² The Proud Boys logo, a right-wing Pro-Trump organization, was embedded in the video and distributed via social media platforms to legitimize the video.²⁰³

U.S. foreign adversaries are not the only challenge to the spread of disinformation. The former Commander in Chief created a post early on November 4 on Twitter claiming

¹⁹⁶ Office of the Director of National Intelligence, "Statement by NCSC Director William Evanina,"

¹⁹⁷ Kirby, "Are China and Iran Meddling in U.S. Elections?"

¹⁹⁸ Kirby.

¹⁹⁹ Renee Diresta et al., *Tell China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives* (Stanford, CA: Stanford Internet Observatory, 2020), 16, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf.

²⁰⁰ Diresta et al., 17.

²⁰¹ Ellen Nakashima et al., "U.S. Government Concludes Iran Was behind Threatening Emails Sent to Democrats," *Washington Post*, October 20, 2020, <https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/>.

²⁰² Nakashima et al.

²⁰³ Nakashima et al.

victory even though crucial swing states had not revealed a winner.²⁰⁴ This type of misinformation led to confusion and a lack of trust in election results. Twitter and Facebook immediately flagged the former President's tweet.²⁰⁵ The former President and his supporters used social media platforms to cast doubt on mail-in voting's validity throughout the campaign. The former President even went so far as to state he may not accept the election results due to the amount of fraud associated with mail-in ballots.²⁰⁶

Election officials and experts would argue this is not the case and contributes to a minimal amount of voter fraud while giving more individuals the ability to vote.²⁰⁷ Oregon, which has been voting by mail long before any other states, has only had 15 attempted election fraud cases related to mail-in ballots over the last 20 years.²⁰⁸ Although very little fraud has been associated with mail-in voting in the past, the pandemic caused a mass influx of mail-in ballots. The massive amount of ballots led to instances in which mail couriers were charged with the delay or destruction of mail-in voting ballots. In Kentucky, a postal worker was charged with disposing of over 100 absentee ballots.²⁰⁹ In New Jersey, a postal worker was charged with discarding over 2,000 pieces of mail, which included 99 absentee ballots, in a dumpster instead of delivering it to residents in West Orange, New Jersey.²¹⁰

²⁰⁴ Elaine Kamarck and Christine Stenglein, "Low Rates of Fraud in Vote-by-Mail States Show the Benefits Outweigh the Risks," *Brookings* (blog), June 2, 2020, <https://www.brookings.edu/blog/fixgov/2020/06/02/low-rates-of-fraud-in-vote-by-mail-states-show-the-benefits-outweigh-the-risks/>.

²⁰⁵ Rachel Sandler, "Half of Trump's Twitter and Facebook Posts since Election Day Flagged," *Forbes*, November 6, 2020, <https://www.forbes.com/sites/rachelsandler/2020/11/04/over-half-of-trumps-twitter-and-facebook-posts-since-election-day-flagged/>.

²⁰⁶ Isobel Hamilton, "Twitter Labels Trump Mail-in Voting Tweet 'Misleading,' Stops Retweets," *Business Insider*, October 27, 2020, <https://www.businessinsider.com/twitter-trump-tweet-mail-voting-warning-label-misinformation-block-retweet-2020-10>.

²⁰⁷ Kamarck and Stenglein, "Low Rates of Fraud in Vote-by-Mail."

²⁰⁸ Kamarck and Stenglein.

²⁰⁹ Alison Durkee, "Kentucky Postal Worker Charged for Throwing 111 Ballots in Dumpster," *Forbes*, October 27, 2020, <https://www.forbes.com/sites/alisdurkee/2020/10/27/kentucky-postal-worker-charged-for-throwing-111-ballots-in-dumpster/>.

²¹⁰ "Postal Employee Arrested for Dumping Mail, Including Election Ballots Sent to West Orange Residents," United States Attorney's Office District of New Jersey, October 7, 2020, <https://www.justice.gov/usao-nj/pr/postal-employee-arrested-dumping-mail-including-election-ballots-sent-west-orange>.

Financial troubles, staffing constraints, and a voluminous amount of ballots led the Postal Service to fail to deliver ballots in the designated time to be counted. In fact, in the 2020 primaries, approximately 65,000 mail-in or absentee ballots were not counted.²¹¹ In an effort to help voters meet deadlines, the Postal Service provided warnings to states about the possibility of delayed returns. The Postal Service also began taking shortcuts by sidestepping the final scanning process and delivering the ballots directly to the board of elections.²¹² The lack of traceability led voters and the public to believe 300,000 ballots were not counted.²¹³

As a result of timely delivery concerns, a federal judge ordered the Postal Service to conduct nightly sweeps of processing facilities in key swing states.²¹⁴ In defiance, the Postal Service continued with its delivery plan, which resulted in 7% of absentee or mail-in ballots not being counted in the 2020 election.²¹⁵ Although the 7% would not have affected the election's overall outcome, it demonstrated how important it is for election officials to work closely with the Postal Service to provide information to voters and put in place security mechanisms to track ballots. If lessons are not learned from the 2020 election, the Postal Service may become a single point of failure for the election system.

The 2020 election caused many Americans to question the integrity of the U.S. election system. Disinformation attacks from U.S. adversaries, the former President questioning the validity of mail-in voting, and the rapid implementation of mail-in voting contributed to these doubts. Election officials must begin to analyze how changes or vulnerabilities to one part of the system directly affect the entire system. Placing a patch on a leak may stop that particular leak but can also lead to additional leaks in another

²¹¹ "What the Postal Service Crisis Means for the November Election," Brennan Center for Justice, August 19, 2020, <https://www.brennancenter.org/our-work/research-reports/what-postal-service-crisis-means-november-election>.

²¹² Phil McCausland, "Postal Service Says It Delivered Ballots on Time amid Concern over Untracked Votes," NBC News, November 4, 2020, <https://www.nbcnews.com/politics/2020-election/postal-service-says-it-delivered-ballots-time-amid-concern-over-n1246451>.

²¹³ McCausland.

²¹⁴ Jacob Bogage and Christopher Ingraham, "USPS Ballot Problems Unlikely to Change Outcomes in Competitive States," November 4, 2020, ProQuest.

²¹⁵ Bogage and Ingraham.

section of the pipe. Perhaps a new, dynamic way of thinking is required. Applying systems thinking approach may be the answer to how to improve the integrity of this nation's election system.

THIS PAGE INTENTIONALLY LEFT BLANK

III. U.S. ELECTORAL SYSTEM

The U.S. election system (Figure 2) is the sum of all parts used to run an election.²¹⁶ The U.S. founding fathers felt very strongly that voting was a states' rights issue.²¹⁷ The Articles of Confederation declared states should appoint delegates to represent the states in Congress and possessed the ability to remove them and replace them with new delegates if needed.²¹⁸ The Constitution followed suit and led voting up to the states, and stipulated only white male landowners held the ability to vote.²¹⁹ The states' ability to set voting laws has led the U.S. Election System to become rather complicated. While the core foundation remains, amendments to the election system have presented new vulnerabilities to the original system created by the Framers. To ensure the U.S. election system's integrity and resilience, an election official and legislators must understand what is encompassed in each stage and how altering one piece of the system could expose or create a vulnerability in the system.

²¹⁶ Alec Yasinsac and Matt Bishop, "The Dynamics of Counting and Recounting Votes," *IEEE Security & Privacy* 6, no. 3 (2008): 22–29, <https://doi.org/10.1109/MSP.2008.75>.

²¹⁷ Brian L. Fife, *Reforming the Electoral Process in America: Toward More Democracy in the 21st Century* (Santa Barbara, CA: ABC-CLIO, LLC, Praeger, 2010), 31.

²¹⁸ U.S. Congress, *United States Code, Articles of Confederation* (1952).

²¹⁹ U.S. Const. art. I § 2.

A. PRIMARIES AND CAUCUSES

As political parties emerged over time, so did the method for nominating individuals for President (Figure 3). In the early to 1800s, when parties first appeared, Congressional leaders from each party nominated a candidate through a process known as King Caucus.²²⁵ The King Caucus process was superseded by nominating conventions in which each party nominated a candidate at respective conventions. The lack of involvement from the public led to accusations of fraud. This process did not settle well with the public, who sought greater input into the process. As a result, states began holding primaries to determine who the delegate representatives would be.²²⁶ As of today, primaries have become an integral part of the U.S. election system.

²²⁵ Joanna Klonsky, “The Caucus System in the U.S. Presidential Nominating Process,” Council on Foreign Relations, accessed February 24, 2021, <https://www.cfr.org/backgroundunder/caucus-system-us-presidential-nominating-process>.

²²⁶ Kevin J. Coleman, Joseph E. Cantor, and Thomas H. Neale, *Presidential Elections in the United States: A Primer*, Order Code RL30527 (Washington, DC: Congressional Research Service, 2020), 6, <https://fas.org/sgp/crs/misc/RL30527.pdf>.

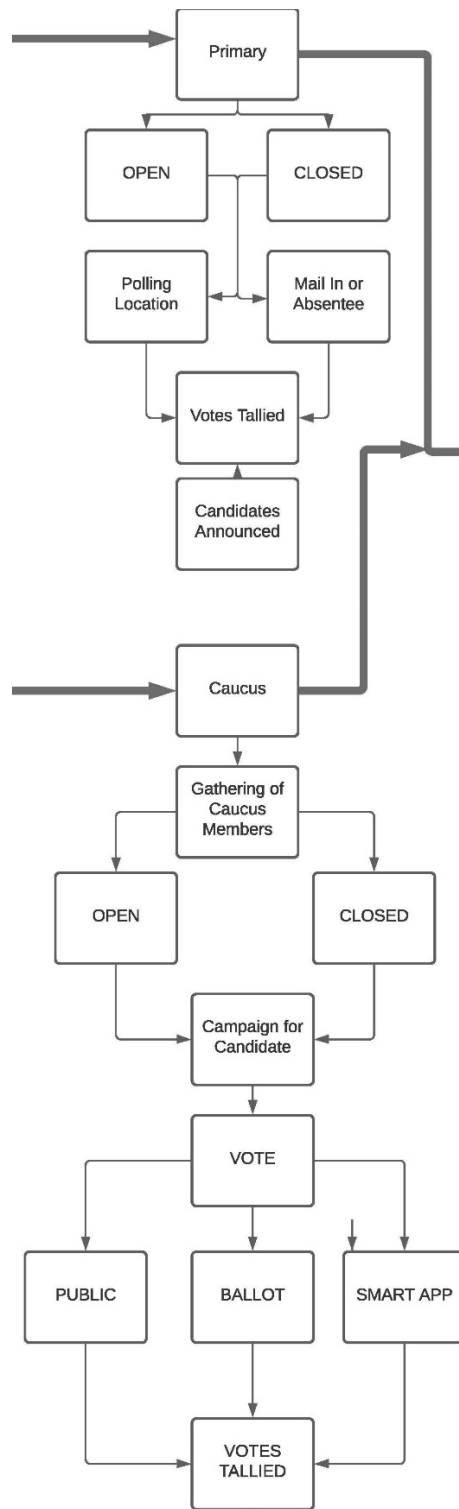


Figure 3. Primary and Caucus Flow Chart

Each state government sets the guidelines for how the primary elections should operate. The states have the option of holding an open or closed primary. In an open primary, party membership is not important.²²⁷ As a registered voter, people may vote for either the Republican or Democratic Party. However, in a closed primary, voters only have the ability to vote within their own party.²²⁸ While how someone votes can vary from state to state, all states afford all voters the ability to cast a vote via a secret ballot. Primaries are a true representation of the people, as they decide which candidate receives the majority of the state's delegates.

Instead of primaries, states have the option of holding caucuses. Caucuses are large community meetings where registered voters of a specific party gather to vote for the candidate and delegates who will represent them at the National Convention.²²⁹ Precinct caucuses are similar to a campaign rally; each candidate's supporters are siphoned into groups, where those supporters do their best to sway voters to switch to their candidate. Rather than place individuals in groups, some states have opted to vote for someone's candidate of choice via smart apps or paper. After a given amount of time, the number of individuals in a group is recorded to determine the number of delegates if any the candidate will receive.

Democratic primaries require a candidate to have 15% or more of the number of attendees to receive delegates.²³⁰ If particular candidates are considered to be nonviable, their supporters will have an opportunity to join a viable candidate's group before a final vote is taken. This process continues over and over again at the county level and congressional district level until the state convention, at which the final delegates for the national convention are chosen. Where Democrats rely solely on a proportional method for delegates, the Republican Party has allowed each state to choose between a winner-take-

²²⁷ Coleman, Cantor, and Neale, 10.

²²⁸ Coleman, Cantor, and Neale, 10.

²²⁹ Klonsky, "The Caucus System in the U.S. Presidential Nominating Process."

²³⁰ Kevin J. Coleman, *The Presidential Nomination Process and the National Party Conventions, 2016: Frequently Asked Questions*, CRS Report No. R42533 (Washington, DC: Congressional Research Service, 2015), 13.

all mentality or the balanced approach.²³¹ Due to limited participation by the public, and the time needed to participate in a caucus, the majority of states have opted to use primaries as the mechanism to determine the number of delegates and Presidential candidates. The Democratic Party uses a complicated mathematical formula to determine how many delegates and alternates each state can have, whereas Republican use a more simplistic method of winner take all.²³²

As more states turned to the use of primaries, the party nominee was identified well before the National Convention. Instead of battling it out on the convention floor, the battle takes place at the polls. This power shift led to conventions becoming more a formality than a necessity. What was once considered the epicenter of democracy is now a media event to introduce the party nominee.

B. NATIONAL CONVENTION

The idea of National Conventions (Figure 4) started with the anti-Masonic Party in 1831.²³³ Additional parties followed suit and held their own National Conventions to nominate their candidate for President. For over 100 years, the convention's primary focus was to nominate a candidate to represent the party in the Presidential election and create the party's platform. In recent years, this process has become more of a formality, as the nominee secures the necessary number of delegates prior to the convention.

²³¹ Coleman, 13.

²³² Coleman, 11–12.

²³³ Becky Little, "How Political Conventions Began—And Changed," History, accessed February 25, 2021, <https://www.history.com/news/political-conventions-change>.

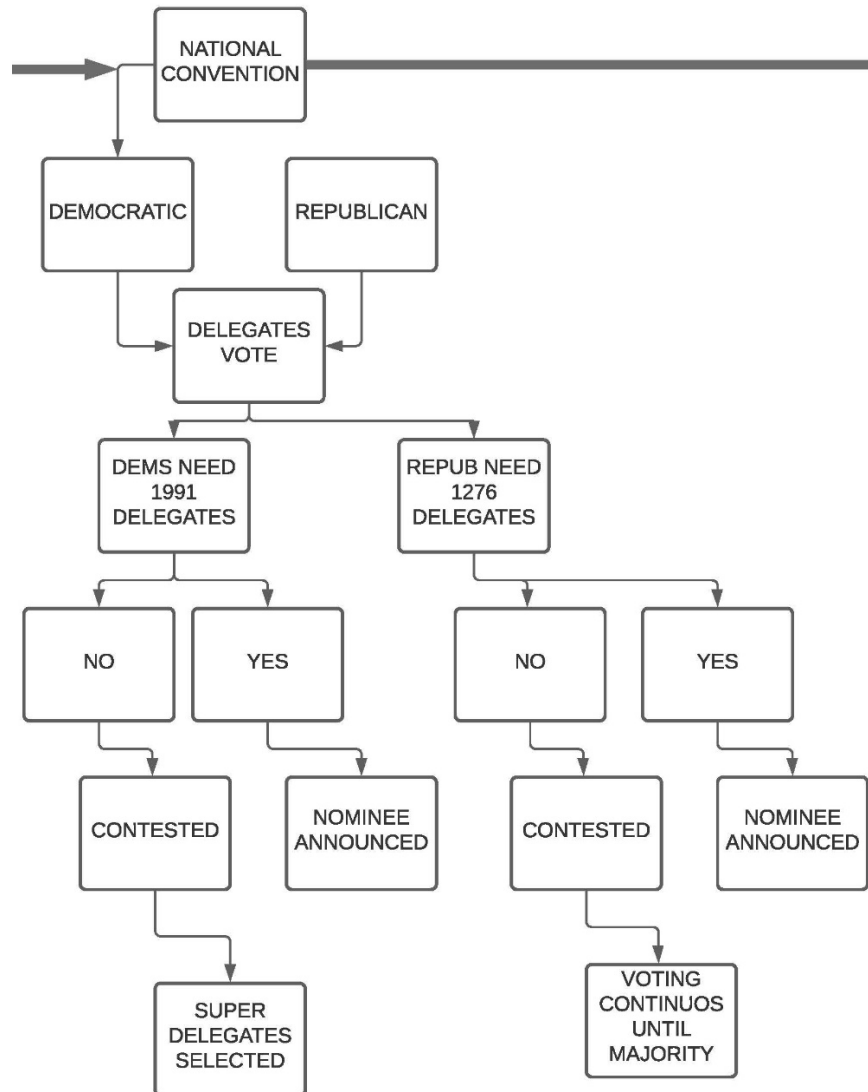


Figure 4. National Conventions Flow Chart.

In the early years of the United States, a formal democratic process did not decide the party nominee; instead, a select group of individuals decided it for the party.²³⁴ As the country grew, so did the need for a formal process resulting in party leaders holding conventions. The idea was to have a place where party leaders from all over the country could come together to discuss issues and determine their platforms.²³⁵ Current challenges facing the new nation led

²³⁴ Tevi Troy, "The Evolution of Party Conventions," Summer 2016, <https://www.nationalaffairs.com/publications/detail/the-evolution-of-party-conventions>.

²³⁵ Troy.

to combative conventions.²³⁶ To alleviate such battles, the parties began establishing policy and procedures, such as a Democratic Presidential candidate could not be designated the nominee until said nominee obtained two-thirds majority of the delegate votes.²³⁷ As new issues arose, the policies were evaluated and adjusted to improve the nomination process.

One of those issues was the advancement of technology, the increase of the media's coverage of conventions left party leaders concerned over the appearance of brokered and contested conventions. Specifically, pictures of protestors clashing with police tainted the image of the 1968 Democratic National Convention.²³⁸ To improve the National Convention's optics, the Democratic Party began to explore the use of primaries to identify the party nominee.²³⁹

Imagine watching a National Convention where delegates had to vote over 100 times before finally declaring a candidate the nominee. While this scenario may seem far-fetched today, it happened at the 1924 Democratic Convention. Delegates were unable to garner enough votes for a nominee, which left the party elites to convince delegates to go with a specific candidate.²⁴⁰ Although brokered conventions are rare in today's environment, the United States has come close to experiencing a contested convention.

The large candidate pool, intra-party division, and social media use to influence voters left both parties leading up to the 2016 Presidential election without a clear candidate and fearful of a contested convention.²⁴¹ Although the 2016 conventions were uncontested, it highlighted the role social media played in the primaries and conventions. Social media's power was slowly dismantling the power of the party establishment and sending this nation back in time when conventions decided the nominee.²⁴²

²³⁶ Troy.

²³⁷ Troy.

²³⁸ Coleman, *The Presidential Nomination Process and the National Party Conventions*, 2016, 17.

²³⁹ Coleman, 17.

²⁴⁰ Coleman, 18.

²⁴¹ Troy, "The Evolution of Party Conventions."

²⁴² Troy.

C. ELECTION DAY

This country's founding fathers did not see a need to have Presidential elections on a specific day. Giving states the ability to hold elections on their day of choosing in November or early December also allowed voters in other states to change their minds. Congress recognized this challenge and passed a federal law in the mid-1800s declaring the first Tuesday after the first Monday in November as Election Day.²⁴³ While the day itself has not changed, over time, states have implemented early voting, mail-in voting, and absentee voting as a way to increase voter turnout.

Early elections saw Americans vote by shouting out their vote in a public place. This method of voting did not last long, and by the 1800s, Americans were voting via paper ballot. As technology advanced, so did voting mechanisms. Over the last two centuries, voters have utilized mechanical lever machines, punch-card machines, and computerized machines. When voters go to the polls today, a volunteer poll worker will verify they are a registered voter via a pollbook. If a voter's registration is unable to be verified, a provisional ballot will be offered to the voter.²⁴⁴ Provisional ballots were created under the Voter Act to provide an opportunity for individuals still to vote if their registration was called into question. The provisional ballot will not be counted until the voter's registration information is validated to prevent fraud.

If registration is verified, the voter will be directed to a voting machine. The current voting machines utilized in the United States are hand-marked optical scan, ballot marking device, and direct-recording electronic voting machines. Although the increased use of electronic voting machines helped rectify the past problems, it brought with it new security challenges.

Some election infrastructure experts argue electronic voting machines will always be susceptible to hackers and it is not possible to 100% secure the equipment itself.²⁴⁵ Experts

²⁴³ Time of Election, 2 *U.S. Code* 7 (1934).

²⁴⁴ Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology et al., *Securing the Vote: Protecting American Democracy* (Washington, DC: National Academies Press, 2018), 38, <https://doi.org/10.17226/25120>.

²⁴⁵ Jen Schwartz, "The Vulnerabilities of Our Voting Machines," *Scientific American*, accessed September 16, 2020, <https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/>.

maintain that a solution to this problem is for all voting machines used in the United States to possess the capability to print a paper ballot.²⁴⁶ The paper ballot acts as a secondary backup to the voting machine and would be used to conduct an audit to ensure the validity of the count.²⁴⁷

Some experts would argue that having a decentralized way of voting works in the United States' favor.²⁴⁸ Hackers would have to be knowledgeable about various voting machines to have maximum disruption.²⁴⁹ Attacking just one type of device would have minimal impact on an election's outcome.²⁵⁰ Although the U.S. voting system's current decentralization makes it challenging for hackers, it does not make it impossible. Other election experts argue having a decentralized system makes it difficult for election security experts to implement universal protocols and detect potential threats to the U.S. election infrastructure.²⁵¹

An additional challenge for election officials is the vendors who supply the hardware and software for the voting equipment.²⁵² The supply-chain continues to come from third parties, often foreign countries that have an interest in the outcome of U.S. elections.²⁵³ A small number of vendors have a monopoly over voting equipment, which makes it difficult for county and state election officials to find alternative options and the vendors offer little incentive to enhance cybersecurity.²⁵⁴

²⁴⁶ Schwartz.

²⁴⁷ Schwartz.

²⁴⁸ Chris Good, "When It Comes to Election Cybersecurity, Decentralized System Is Viewed as Both Blessing and Curse," ABC News, October 31, 2018, <https://abcnews.go.com/Politics/election-cybersecurity-decentralized-system-viewed-blessing-curse/story?id=58877082>.

²⁴⁹ Good.

²⁵⁰ Good.

²⁵¹ Committee on Homeland Security Democrats, *Congressional Task Force on Election Security: Final Report* (Washington, DC: Committee on Homeland Security, 2018), 20, <https://cha.house.gov/sites/democrats.cha.house.gov/files/documents/TFESReport.pdf>.

²⁵² Blaze et al., *DEF CON 27*, 6–7.

²⁵³ Blaze et al., 6–7.

²⁵⁴ Lawrence Norden, Gowri Ramachandran, and Christopher Detuzio, "A Framework for Election Vendor Oversight," November 12, 2019, <https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight>.

Depending on the voting mechanism used will depend on how the vote is counted. Suppose a paper ballot is printed from the voting machine. In that case, the votes are scanned via an optical scanner and uploaded to a central location or stored on a memory device securely transported to a central tallying location. Even though Election Day has been the primary way Americans have voted, states recognized the need to have alternatives for those who cannot be present on Election Day.

What started as a way for Civil War soldiers to vote during the war has morphed into states creating absentee ballots laws for those with disabilities, serving in the U.S. military, and business obligations on Election Day.²⁵⁵ As a response to these challenges, more than half of the 50 states have implemented no-excuse absentee voting. Various forms of absentee voting are available, such as excuse required, no-excuse, permanent absentee, all vote-by mail, the Uniform and Overseas Citizens Absentee Voting Act.²⁵⁶ Each state is responsible for implementing laws regarding the type of absentee voting, timelines, and security procedures regarding absentee voting.²⁵⁷ Over the years, five states began casting ballots solely through universal mail-in voting successfully for years.²⁵⁸ The recent global pandemic forced states to permit voters to request absentee ballots or vote by mail citing the pandemic as an excuse, which created an impossible task for election officials.²⁵⁹

When returning the ballot, it must contain a signature on the outside of one of the envelopes. The voter then can return it via mail, ballot drop boxes, or election offices. States have implemented various security procedures, such as sending ballots to tracking mechanisms, secured in multiple envelopes, address mechanisms, registration verification, and

²⁵⁵ Paul G. Steinbicker, “Absentee Voting in the United States,” *The American Political Science Review* 32, no. 5 (1938): 898–907, <https://doi.org/10.2307/1948225>.

²⁵⁶ Election Assistance Commission, *The Election Administration and Voting Survey: 2016 Comprehensive Report* (Washington, DC: Election Assistance Commission, 2017), 9, https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf.

²⁵⁷ Matt Vasilogambos, “States Begin Prep for Mail-In Voting in Presidential Election,” PEW, March 23, 2020, <https://pew.org/3a97s4G>.

²⁵⁸ Kamarck and Stenglein, “Low Rates of Fraud in Vote-by-Mail.”

²⁵⁹ Vasilogambos, “States Begin Prep for Mail-In Voting in Presidential Election.”

signature verification process.²⁶⁰ Critics would argue this method could lead to delayed or never received ballots, misprinted ballots, confusion with ballots, voter coercion, or voter fraud via family members.²⁶¹

An additional option now being offered to voters is in-person early voting. Voting locations are pre-selected by election officials. Each state will determine when early voting will begin. Texas, for example allows early voting up to 21 days prior to the election.²⁶² As a result of relaxed mail-in voting and absentee ballots laws, a few states began allowing voters to use these types of voting mechanisms to vote early. The recent 2020 election saw a record number of voters participate in early voting.²⁶³ As early voting and mail-in voting becomes more popular, states have begun to favor vote centers instead of precinct locations. This popularity has resulted in precinct locations being closed and frustrated voters waiting in long line. Election officials must notify the public of changes and updates to the location of poll locations or vote centers. Election administrators continue to study and evaluate polling locations to serve the public on Election Day best (Figure 5).²⁶⁴

²⁶⁰ Darrell M. West, “How Does Vote-by-Mail Work and Does It Increase Election Fraud?,” *Brookings* (blog), June 22, 2020, <https://www.brookings.edu/policy2020/votervital/how-does-vote-by-mail-work-and-does-it-increase-election-fraud/>.

²⁶¹ Atanu Das, “Mitigating Potential Vote-By-Mail Fraud while Simultaneously Increasing Vote-By-Mail Ballot Acceptance by Utilizing Facial Recognition and Multifactor Authentication Technology,” *Harvard Journal of Law* 34 (Fall 2020): 1–16.

²⁶² Paul Gronke, “Early Voting Reforms and American Elections,” *William and Mary Bill of Rights Journal* 17, no. 2 (December 2008): 423–51.

²⁶³ Drew Desilver, “Amid Pandemic, the Long Decline of in-Person Voting on Election Day Is Likely to Accelerate This Year,” *Pew Research Center* (blog), November 3, 2020, <https://www.pewresearch.org/fact-tank/2020/11/03/amid-pandemic-the-long-decline-of-in-person-voting-on-election-day-is-likely-to-accelerate-this-year/>.

²⁶⁴ Election Assistance Commission, *The Election Administration and Voting Survey*, 13.

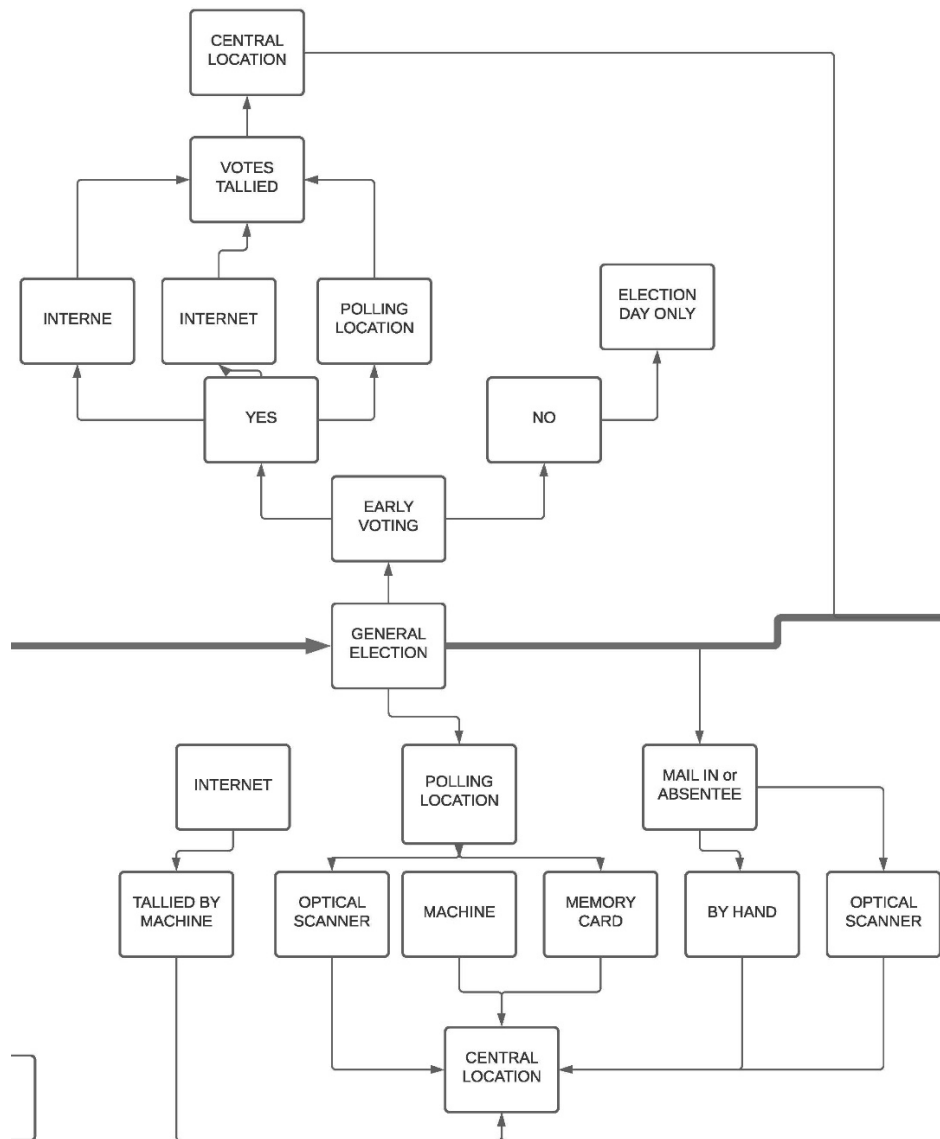


Figure 5. General Election Voting Flow Chart.

Although providing voters with additional mechanisms increases voters' convenience, it has caused challenges for the U.S. voting system. Electronic voting machines are costly, require training for poll workers, and are vulnerable to an attack from bad actors. Increased mail-in and absentee voting has placed an enormous amount of strain on the Postal Service and election officials to obtain the necessary personnel needed, secure the ballots, and ensure chain of custody protocols are established and followed.

D. CERTIFYING ELECTIONS

Polls have closed, and the nation anxiously awaits the results, but the job continues as all votes are tallied for election administrators. What Americans see reported by the media late into the night are unofficial results. The detailed process of counting may take one day, five days, or several weeks depending on individual state laws (Figure 6). States must process early voting, provisional ballots, mail-in and absentee ballots, and ballots stored on a media device. The recent global pandemic has caused states to amend laws to account for the voluminous amount of mail-in voting in the 2020 election.

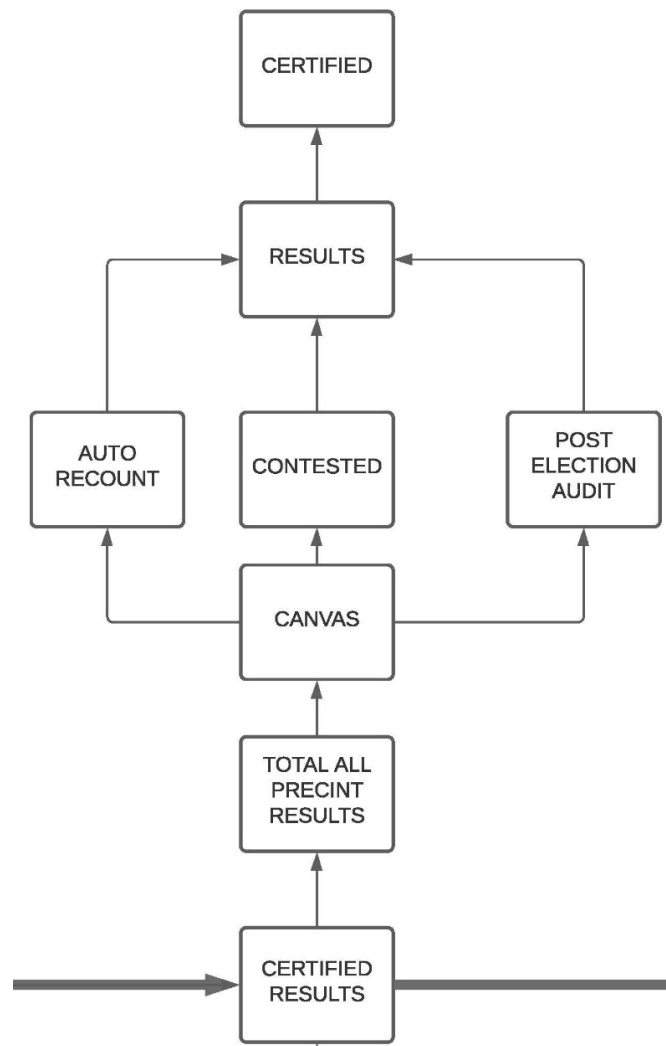


Figure 6. Certifying Elections Flow Chart

The goal of canvas boards is to ensure that every ballot cast is accurately represented in the final count and includes ballots that were called into question, such as mismatched signatures, damaged ballots, or voter intent.²⁶⁵ Canvas boards are composed of the state’s chief election official, judges, or state officials. For transparency purposes, observers are allowed to witness counting procedures but must follow election officials’ guidelines. Some jurisdictions will even go so far as to live-stream the canvas to provide transparency.²⁶⁶ To prevent fraud claims, a detailed report will be conducted and submitted by election officials and a final canvas meeting will be held to certify the results.²⁶⁷ While most canvases end with a clear winner, this is not always the case.

In some instances, a canvas will reveal the race is too close to call. In many states, if the total count falls within a half percent of another, an automatic recount will be generated.²⁶⁸ Recounts are conducted under specific guidelines established by the states, including timeframes, staffing and training requirements, and type of recount. Election officials should work with local law enforcement or private security firms to establish security protocols. These policies and procedures are detailed for members of the recount board, observers, and the media. While each state is different, recount boards are made up of bi-partisan members to help maintain the recount’s integrity. Once they arrive, each member of the recount team will be assigned an area of responsibility and observers will be led to their designated area.²⁶⁹ Depending on each state law, a recount may be conducted by hand or through an optical scanner. Tally sheets, batch sheets, and ballots are kept for each type of voting mechanisms and are added together to reveal the results of the recount. The more transparent a recount can be, the less likely it will be used as a vehicle for a disinformation campaign.

²⁶⁵ “After the Voting Ends: The Steps to Complete an Election,” National Conference of State Legislatures, October 28, 2020, <https://www.ncsl.org/research/elections-and-campaigns/after-the-voting-ends-the-steps-to-complete-an-election.aspx>.

²⁶⁶ Sarah J. Eckman, R. Sam Garrett, and Karen L. Shanton, *Federal Election Results: Frequently Asked Questions*, CRS Report No. R46565 (Washington, DC: Congressional Research Service, 2020), 6.

²⁶⁷ U.S. Election Assistance Committee, *Election Management Guidelines* (Washington, DC: U.S. Election Assistance Committee, n.d.), 137

²⁶⁸ U.S. Election Assistance Committee, 147.

²⁶⁹ U.S. Election Assistance Committee, 148–151.

Even if the general election does not generate an automatic recount, a candidate can contest the election. Each state sets guidelines for when a candidate can contest an election, which must be done within a specific time period and may require the candidate to pick up the tab.²⁷⁰ In the 2020 election, the small percentage of victory in Wisconsin by Biden led the Trump campaign to request a recount in two Wisconsin counties and cited voter fraud as the reason.²⁷¹ Although the Trump campaign was unable to produce evidence of fraud, the campaign was willing to spend \$3 million to identify potential fraud.²⁷² The recount debunked the fraud claims and certified Biden as the winner.

The 2020 election highlighted states' abilities to conduct audits without being requested or mandatory. States use audits to measure the resilience of the election system in place. Traditional or risk limiting audits are the primary methods utilized to conduct audits. A traditional audit fails to distinguish between a close election and a large victory margin by creating a preset percentage of districts to recount.²⁷³ Paper ballots are hand-counted and compared to the results of the electronic voting machines. Whereas in risk-limiting audits, the margin of victory determines how many votes are counted. Researchers argue it is not necessary to count every vote and that using statistical methods to analyze fewer votes allows election officials to determine the accuracy of the tally.²⁷⁴

To debunk claims of voter fraud involving Dominion voting machines, the Georgia Secretary of State ordered a risk-limiting audit of the paper ballots produced by election

²⁷⁰ U.S. Election Assistance Committee.

²⁷¹ Scott Bauer, "Wisconsin Issues Recount Order in 2 Counties as Trump Wanted," AP NEWS, November 19, 2020, <https://apnews.com/article/wisconsin-recount-2-counties-f408a7b43deb96e2ac7ff0b24a2f968a>.

²⁷² Bauer.

²⁷³ National Conference of State Legislatures, "Post-Election Audits," October 25, 2019, <https://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx>.

²⁷⁴ Philip B. Stark, *An Introduction to Risk-Limiting Audits and Evidence-Based Elections* (Berkeley, CA: University of California, Berkeley, 2018), 3–4, <https://www.stat.berkeley.edu/~stark/Preprints/lhc18.pdf>.

machines.²⁷⁵ An Election Commission certified company would oversee the testing of the touchscreen machines and tabulation scanners.²⁷⁶ For complete transparency, the Secretary of State required all votes cast be manually counted.²⁷⁷ During the audit, a few counties identified errors, such as memory cards not being uploaded for counting. These errors were rectified and the results were re-certified for those counties. In the end, the audit confirmed Biden did indeed win Georgia and the allegations against the voting machines in Georgia were false.²⁷⁸ President Trump continued to use social media to express his doubt over the audit results, which resulted in the President's lawyers requesting a formal recount in Georgia.²⁷⁹ Georgia law requires recounts to be completed via optical scanners.²⁸⁰ In the end, the third recount once again verified Biden won the state, which led the Secretary of State to certify the results on December 7, 2020.²⁸¹

Post-election audits provide states the ability to validate the state's current election system. Audits identify errors made during the general election, correct them, and prevent them from happening in a future election. The 2020 election represented how social media use can be used to sow doubt in the validity of the U.S. election system. The use of post-election offers a solution to mitigating the spread of misinformation. The audits provide the public with the transparency needed to discredit attacks on the legitimacy of an election.

²⁷⁵ "Secretary Raffensperger Announces Completion of Voting Machine Audit Using Forensic Techniques No Sign of Foul Play," Georgia Secretary of State Press Office, accessed February 25, 2021, https://sos.ga.gov/index.php/elections/secretary_raffensperger_announces_completion_of_voting_machine_audit_using_forensic_techniques_no_sign_of_foul_play.

²⁷⁶ Kate Brumback, "Second Georgia County Finds Previously Uncounted Votes from 2020 Presidential Election," ABC11 Raleigh-Durham, November 17, 2020, <https://abc11.com/8049192/>.

²⁷⁷ "Historic First Statewide Audit of Paper Ballots Upholds Result of Presidential Race," Georgia Secretary of State Press Office, November 19, 2021, https://sos.ga.gov/index.php/elections/historic_first_statewide_audit_of_paper_ballots_upholds_result_of_presidential_race.

²⁷⁸ Brumback, "Second Georgia County Finds Previously Uncounted Votes from 2020 Presidential Election."

²⁷⁹ Kate Brumback, "Georgia Again Certifies Election Results Showing Biden Won," AP NEWS, December 7, 2020, <https://apnews.com/article/election-2020-joe-biden-donald-trump-georgia-elections-4eeea3b24f10de886bcdab6c26b680a>.

²⁸⁰ Ga. Comp R & Regs, R. 183-1-15-.0(b) (2020).

²⁸¹ Brumback, "Georgia Again Certifies Election Results Showing Biden Won."

E. ELECTORAL COLLEGE

When creating the U.S. Constitution, the Framers recognized the need to outline the process for choosing the President of the United States. The challenge became that the framers struggled to agree on the process. The founders considered all options but ultimately compromised on each state's idea holding a number of electoral votes in proportion to the number of Senators and House members.²⁸² However, the framers did place stipulations on who could serve as an elector; members of the Congress or Senate were forbidden, as was an individual who held an office of trust.²⁸³ In true federalist form, how electors were chosen was left up to each state. Once selected by state legislatures, electors met in their home states and cast a ballot for two individuals with the caveat that they are prohibited from voting for a candidate from their home state.²⁸⁴ The votes are listed, certified and sealed, and sent securely to the President of the Senate (Figure 7).²⁸⁵ The individual with the highest number of electoral votes was named President and the runner-up became the Vice President. If the electoral vote resulted in a tie, then the House of Representatives would each cast a vote per state delegation to determine who is President.

²⁸² U.S. Const. art II § 1, cl. 2.

²⁸³ U.S. Const. art II § 1, cl. 2.

²⁸⁴ U.S. Const. art II § 1, cl. 2.

²⁸⁵ U.S. Const. art II § 1, cl. 2.

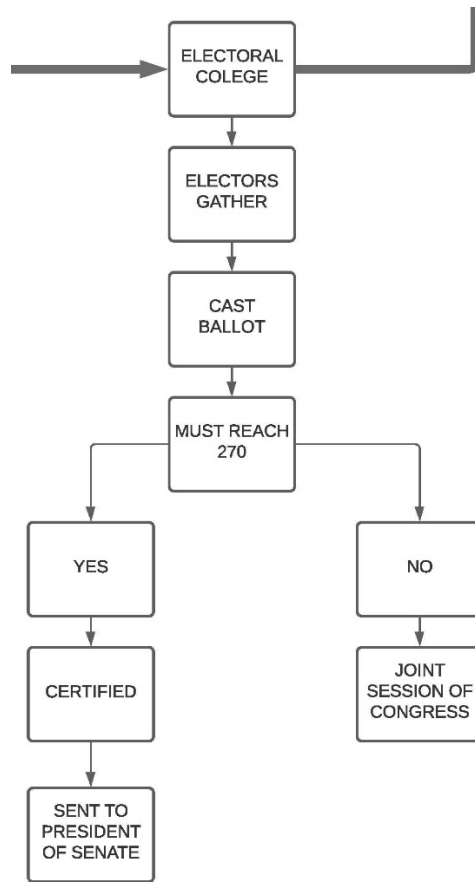


Figure 7. Electoral College Flow Chart

The election of 1800 identified vulnerabilities to the electoral system structure. The introduction of party line voting led to Thomas Jefferson and Aaron Burr receiving the same number of votes to Congress. After 36 tries and backroom negotiations, the House elected Thomas Jefferson President of the United States. To prevent this predicament from happening again, Congress enacted an amendment to the Constitution.²⁸⁶ Due to the Electoral College provision, the President and Vice President were listed on separate ballots and the list of candidates presented to the House in a contested electoral vote shrunk from five to three.²⁸⁷ Over the years, states have ratified laws to enable the public to choose the electors to represent their respective state. Today, in all but two states, the winner of

²⁸⁶ U.S. Const. amend. XII (1804).

²⁸⁷ U.S. Const. amend. XII (1804).

the statewide election receives all the electoral votes.²⁸⁸ In December, on the first Monday after the second Wednesday, electors gather as mandated by state law and cast their ballots for the President. The results are sealed, certified, and sent by the Governor of the State to the President of the Senate, Secretary of State Office, Archivists of the United States, and a federal judge in the states district.²⁸⁹ This complex process has led many critics of the Electoral College to question if reform is needed.

Critics of the Electoral College feel as though the popular vote should declare the winner of the election and not the Electoral College.²⁹⁰ In the history of the United States, only five instances have occurred in which the candidate who won the popular vote did not win the Electoral College.²⁹¹ One of those instances was in 2016; Presidential Candidate Hillary Clinton was the victor of the popular vote by more than two million votes but failed to obtain the necessary 270 electoral votes.²⁹² Meanwhile, Presidential Candidate Trump acquired 304 electoral votes that resulted in him being certified as the next President.²⁹³ The 2016 election reignited the debate on whether the Electoral College is archaic and undemocratic and should be modified to reflect the people's will, not a chosen few.

F. JOINT SESSION OF CONGRESS CERTIFICATION

The final phase of the U.S. election system is the ratification by the House and the Senate of the Electoral College votes. The 12th amendment of the Constitution requires the House and the Senate to convene in a joint session on January 6 when the Vice President will open the states certified results in alphabetical order (Figure 8).²⁹⁴ The process

²⁸⁸ “The Electoral College,” National Conference of State Legislatures, accessed February 25, 2021, <https://www.ncsl.org/research/elections-and-campaigns/the-electoral-college.aspx>.

²⁸⁹ Congressional Research Service, *Counting Electoral Votes: An Overview of Procedures as the Joint Session, Including Objections by Members of Congress*, CRS Report No. RL32717 (Washington, DC: Congressional Research Service, 2020), 2–3.

²⁹⁰ Elaine Kamarck and John Hudak, “How to Get Rid of the Electoral College,” *Brookings* (blog), December 9, 2020, <https://www.brookings.edu/blog/fixgov/2020/12/09/how-to-get-rid-of-the-electoral-college/>.

²⁹¹ Kamarck and Hudak.

²⁹² Kamarck and Hudak.

²⁹³ Kamarck and Hudak.

²⁹⁴ Counting Electoral Votes in Congress, *U.S. Code* 3 (1948) §15.

stipulates the Vice President will then hand each state's vote to the tellers, who are preselected by members of the House and Senate, to announce the vote verbally. After each state's vote is read aloud, lawmakers will have the opportunity to provide an objection to the vote in writing. A member of each chamber must support the objection.²⁹⁵ The objection will lead to a breakout session for each chamber, during which they will discuss the merits of the objection and then vote to uphold the electoral vote or overturn it. Rejecting a state's vote would require a simple majority by both chambers, which is only likely to happen when a party occupies both the House and the Senate. After two hours, the chambers reconvene and announce their decision; if the vote fails to reject the state's electoral vote, the teller counts the vote and moves on to the next state. If both chambers were able to agree to overturn the vote, the state's governor becomes the decision maker.²⁹⁶

²⁹⁵ Congressional Research Service, *Counting Electoral Votes*, 6.

²⁹⁶ Congressional Research Service, 9.

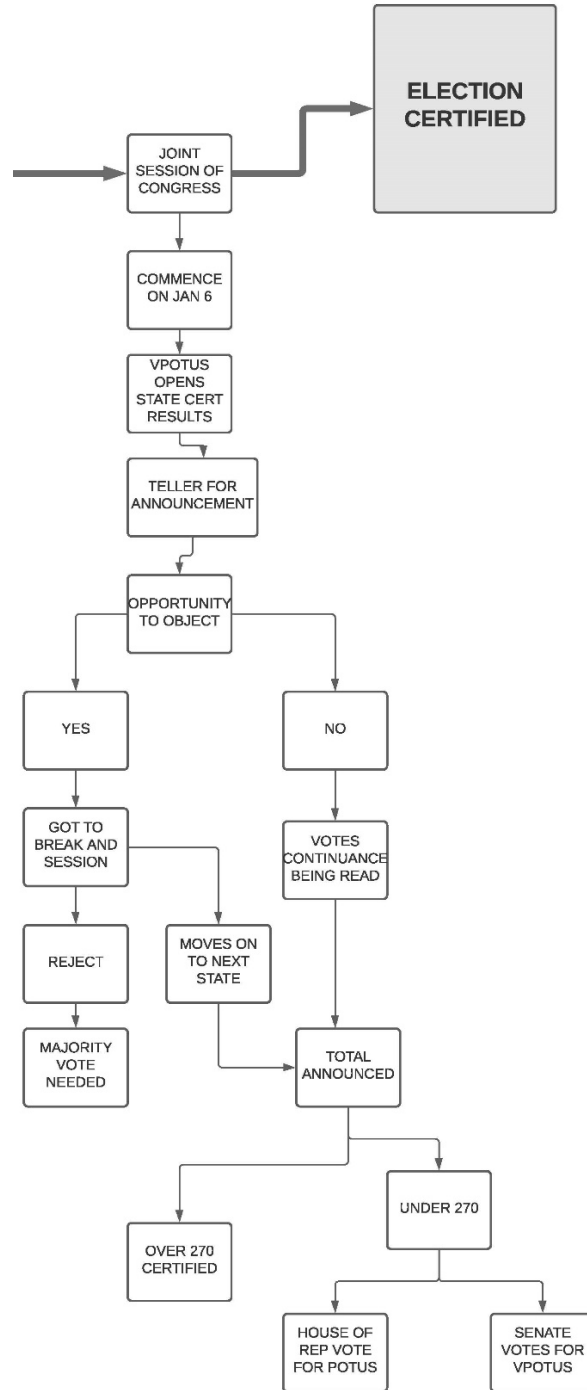


Figure 8. Joint Sessions of Congress Flow Chart

Despite what many Americans may think, the Constitution does not give the Vice President the power to overturn electoral votes.²⁹⁷ The Vice President merely presides over the session to preserve the validity of the process. Once all 50 states and the District of Columbia certified results have been read and counted, the Vice President will announce if a candidate has reached the required votes necessary to obtain the presidency's office. This announcement serves as the final verification of who has been certified as the next President of the United States.

If either candidate fails to reach the necessary 270 electoral votes, then the House votes on the Presidency, and the Senate votes on the Vice President.²⁹⁸ Legislatures from each state must put forth one vote from their state; the process does not allow each individual to cast a ballot (Figure 9).²⁹⁹ The 2020 election saw the former President and his supporters call for lawmakers to challenge the certified electoral votes on January 6 in crucial swing states by citing voter fraud as the reason. On January 6, several Republicans did indeed provide a written challenge to the electoral votes in Arizona and Pennsylvania.³⁰⁰ After deliberations and chamber votes, Republicans failed to secure the necessary votes needed to overturn the electoral votes, and Biden was declared the President of the United States.

²⁹⁷ U.S. Const. art II § 1, cl. 2.

²⁹⁸ Congressional Research Service, *Counting Electoral Votes*, 10.

²⁹⁹ Congressional Research Service, 10.

³⁰⁰ Barbara Sprunt, "Here Are the Republicans Who Objected to the Electoral College Count," NPR, accessed February 25, 2021, <https://www.npr.org/sections/insurrection-at-the-capitol/2021/01/07/954380156/here-are-the-republicans-who-objected-to-the-electoral-college-count>.

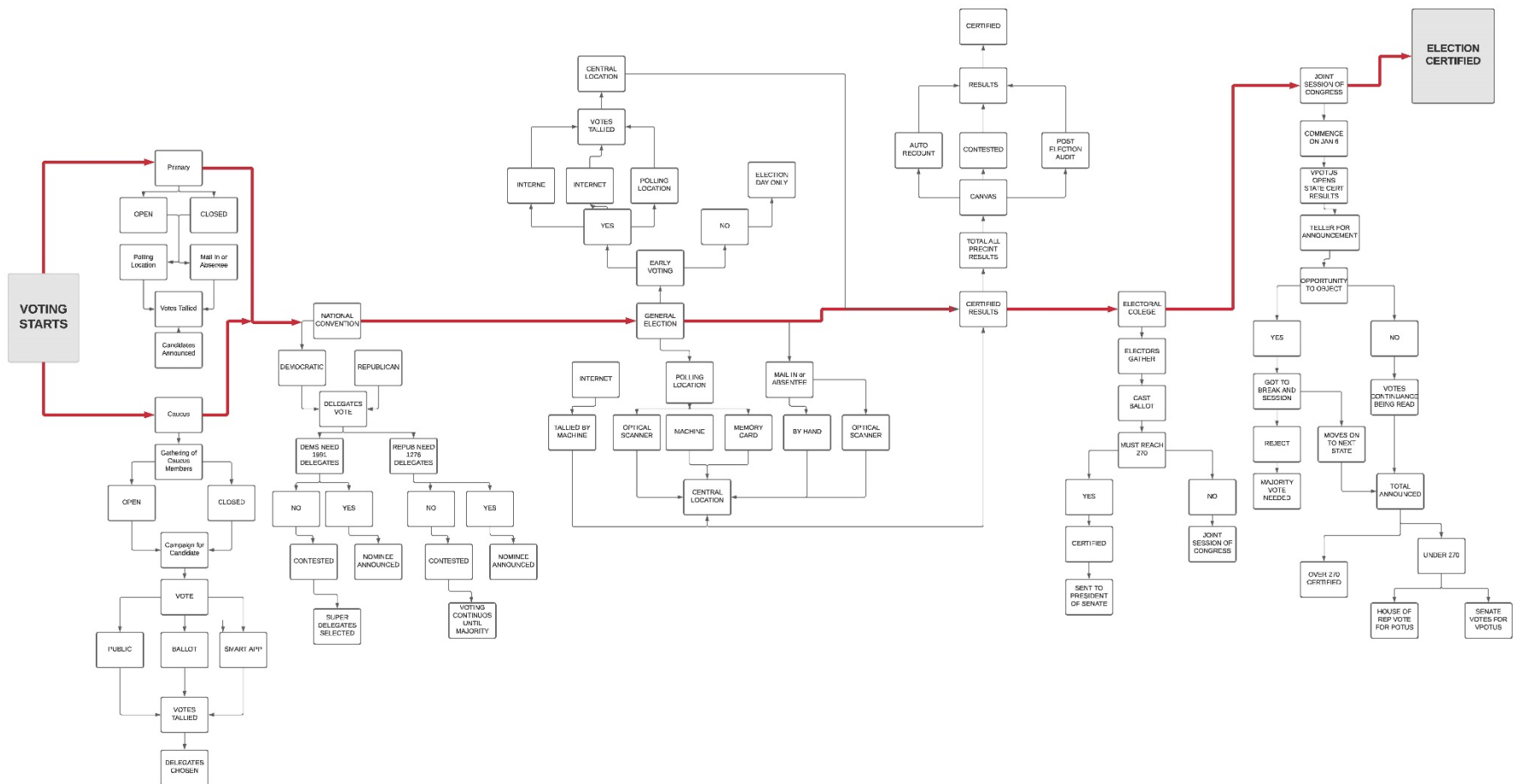


Figure 9. The U.S. Electoral Process Flow Chart

Prior to objections, the nation saw Trump supporters and right-wing activists storm the Capitol in an attempt to disrupt or delay the electoral count. The rioting and destruction of federal property resulted in lawmakers being evacuated from the House floor to a secure location. In a sign of unity, lawmakers recognized the need to preserve the process and continue with the joint session. While rioters were successful in disrupting the process, they could not destroy the democratic process.

The Capitol's attack revealed election officials, legislatures, and government agencies must acknowledge foreign adversaries are not the only groups attempting to attack the U.S. election system but domestic groups as well. What happened at the Capitol exposed not only a security vulnerability but also the ability to halt the process.

Had law enforcement not been able to rectify the security situation so quickly, lawmakers would not have been able to reconvene and finish the count.

This situation is not the only vulnerability within the Joint Session. The current system in place poses challenges in today's partisan environment. Allowing only one vote per state delegation could give a candidate an unfair advantage in securing the Presidency. For example, although the Democrats controlled the house on January 6, some states had a Republican majority. Under the current 12th amendment, a state could have voted for Trump over Biden and pave the way for a Trump victory even though Biden won the popular vote and controlled the House.³⁰¹

Due to the times, the founding fathers saw the need for a decentralized U.S. electoral system. Still, as the country expanded and became more democratic, the system became even more complex. What was once the decision of a select few now consists of involvement by state election officials and legislatures, oversight by federal agencies and legislation, third-party vendors, advanced technology, and widespread mail-in and absentee voting. As these changes were made, election administrators and legislatures failed to recognize each change's effect on other components within the election system. Applying systems thinking and red teaming to the idea will assist in determining if this potential change is a viable solution.

³⁰¹ U. S. Const. amend. XII (1804).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. APPLYING SYSTEMS THINKING AND RED TEAMING TO THE U.S. ELECTORAL SYSTEM

While systems thinking and red teaming could be applied to each component within the U.S. electoral system, this thesis explores how the rapid implementation of widespread mail-in voting in the 2020 election affected various components within the system. As a result of the recent pandemic, election officials and legislatures were forced to find a way to conduct primaries and a general election still while maintaining the safety of the public. This situation resulted in states expanding legitimate reasons to include COVID, with some states excluding a signature-matching requirement, and extending the return deadline date.

Prior to the 2020 pandemic, only five states utilized universal voting, which left the majority of election administrators unprepared to handle the vast amount of mail-in ballots.³⁰² Election administrators needed to ensure that security protocols for processing ballots were in place, efficient numbers of personnel and training were provided, obtaining the necessary equipment to count, increasing the number of ballot drop boxes, and coordinating with the Postal Service. Numerous critics, including President Trump, believed this voting method would lead to large amounts of voter fraud.³⁰³ President Trump and his supporters continued to use social media in an effort to create doubt about mail-in voting and the election results. A decentralized electoral system combined with a global pandemic and negative rhetoric by high-ranking government officials made the process of mail-in voting challenging for election officials. Although the 2020 election did not see an increase in voter fraud, the mass influx of mail-in ballots did expose vulnerability points and adversely affected various components of the election system.

A. CHAIN OF CUSTODY PROCEDURES FOR MAIL-IN BALLOTS

A key component to preserving the integrity of voting via mail is the security and chain of custody protocols created by election officials. Oregon, which has been voting by

³⁰² National Conference of State Legislatures, “VOPP: Table 18: States with All-Mail Elections,” April 21, 2020, <https://www.ncsl.org/research/elections-and-campaigns/vopp-table-18-states-with-all-mail-elections.aspx>.

³⁰³ Das, “Mitigating Potential Vote-By-Mail Fraud.”

mail long before any other states, has only identified 15 attempted election fraud cases related to mail-in ballots over the last 20 years.³⁰⁴ Part of Oregon's success can be attributed to the chain of custody protocols established by election officials. Oregon has spent years perfecting security protocols to ensure a ballot is tracked from inception until the time it is counted.³⁰⁵

1. Voter Registration and Distribution of Universal Mail-In Ballots

After years of wasting time and money on ballots for voters who have moved or were no longer viable registered voters, Oregon passed legislation for automatic voter registration.³⁰⁶ Since an individual is already required to provide the Department of Motor Vehicles (DMV) with identification documents, Oregon legislators leveraged this collection of documents to register someone to vote. Since the individual is not presented with a choice at the DMV, Oregon does provide an opportunity for an individual to opt-out by returning a postcard provided by the state to be unregistered. If the card arrives within the specified time period, the individual will be removed from the voter roll. The voter registration database is the primary source for all voter registration information, including name, address, and proof of life. In an effort to maintain accurate records, election officials rely on receiving updated voter roll information from the DMV.

While the law has led to an increase in Oregon's voter registration, it has also exposed a new vulnerability point within the election system. The Cyber Agency offers states the opportunity to have their election machines, websites, and databases analyzed for potential breaches, but the DMV database falls outside the agency's scope of responsibility. If election officials receive voter information through the DMV, altering specific individuals' information could result in voters not receiving a ballot. The Oregon DMV website is also connected to the internet, which makes it visible to hackers and vulnerable to an attack. The Cyber Agency's assessment would not reveal a breach since it occurred

³⁰⁴ Kamarck and Stenglein, "Low Rates of Fraud in Vote-by-Mail."

³⁰⁵ Don Hamilton, "The Oregon Voting Revolution," *The American Prospect* 17, no. 5 (2006): A3.

³⁰⁶ Oregon Rev. Stat. § 247.019.

on the DMV database. A hacker only has to change a small number of addresses for the public to begin to doubt the process of mail-in voting.

Election officials in Oregon determined mailing ballots three weeks ahead of elections would provide a sufficient amount of time for voters to cast and return a ballot.³⁰⁷ While maybe enough time to identify a mailing error and request a new ballot, some states allow individuals to request ballots up to six days before the election, and as such, a new ballot would never reach them in time. A state like Oregon that has been executing universal mail-in voting for over 20 years has experienced these hardships, learned from them, and rectified the problem. States new to mail-in voting as a result of the pandemic failed to recognize the impact of incorrect voter rolls and requests so close to the election could have on ballots being returned on time. This oversight could lead to voters' ballots not being returned in time to be counted. In a state where the election is anticipated to be close, this lapse in policy change could alter election results or cause voters to become disenfranchised with the process.

For example, a red teaming exercise could include a political activist acting as a volunteer to assist in the preparation of mail-in ballots. The activist would have access to the voter registration information and can identify liberal voters by zip code. The activist can easily find this information through an open-source search on the internet. For example, Dekalb County in Georgia has 79.1% of voters who lean Democratic.³⁰⁸ By removing thousands of ballots, it is easily possible to stand an 80% chance of discarding Democratic ballots. In the case of universal mail-in voting, ballots do not have to be requested; thus, the activist would have the ability to forgo sending a large number of ballots to that particular zip code intentionally.

2. Casting Mail-In Ballots

The 2020 U.S. general election forced election officials to relax or alter election laws for mail-in voting, such as deadline dates for ballots to be counted. Many of the

³⁰⁷ Hamilton, "The Oregon Voting Revolution."

³⁰⁸ Bert Sperling, "DeKalb County, Georgia Politics & Voting," accessed February 25, 2021, <https://www.bestplaces.net/voting/county/georgia/dekalb>.

changes to election laws were challenged by both parties and resulted in decisions being made by the state supreme courts. The legal challenges, combined with many first-time voters' anticipation, led election officials to provide guidance on election websites as to how to complete and return a ballot.

In most states, when a voter receives a ballot, included inside the package are two envelopes, a return envelope with a barcode for tracking purposes, and a privacy envelope for the ballot itself.³⁰⁹ While most states require the voter to sign the return envelope as a form of proof of identity, a few states require a notary or witness to sign the ballot as an extra step of voter identification.³¹⁰ State election officials are constantly trying to strike a balance between convenience for the voter while maintaining the integrity of the system. As a result of the pandemic, states waived or altered the requirement to prevent the spread of COVID-19. For example, North Carolina's state chose to require one witness instead of the standard two for the 2020 election.³¹¹

The pandemic has altered the manner in which mail-in voting and absentee voting operates. North Carolina recognized how important it is still to require security protocols for voter identification due to its association with the most notable absentee voter fraud case in recent history.³¹² In 2018, an individual working for a House Representative Republican Candidate in North Carolina was indicted along with co-conspirators for attempting to defraud the state with fraudulently obtained absentee ballots.³¹³

The indictment alleges these individuals hired his co-conspirators to collect absentee ballots from voters and lie about witnessing their votes.³¹⁴ Once the absentee

³⁰⁹ Hamilton, "The Oregon Voting Revolution."

³¹⁰ "VOPP: Table 14: How States Verify Voted Absentee Ballots," National Conference of State Legislatures, April 17, 2020.

³¹¹ "FAQ: Voting by Mail in North Carolina in 2020," North Carolina State Board of Elections, <https://www.ncsbe.gov/voting/vote-mail/faq-voting-mail-north-carolina-2020#how-many-witnesses-do-i-need-for-my-absentee-ballot>.

³¹² Richard Gonzales, "North Carolina GOP Operative Faces New Felony Charges that Allege Ballot Fraud," NPR, July 30, 2019, <https://www.npr.org/2019/07/30/746800630/north-carolina-gop-operative-faces-new-felony-charges-that-allege-ballot-fraud>.

³¹³ Gonzales.

³¹⁴ *State of North Carolina v. Leslie McCrae Dowless*, No. 19CRS001934 (n.d.).

ballots were in his possession, he then mailed the ballots to give the appearance they were mailed by the voter.³¹⁵ These tainted ballots were then counted in the 2018 election, which gave the Republican candidate a 900-vote advantage over his opponent.³¹⁶

Selling ballots is always a risk when it comes to mail-in voting. Although the act of buying or selling votes is illegal in the United States, it does not stop individuals from trying to earn a quick buck or attempting to influence an election. The challenge with mail-in voting is the lack of oversight over the casting of a ballot, and just security protocols in place to verify a voter's identity at a counting facility. However, this verification process fails to identify individuals willingly signing the envelope but handing over a blank ballot to an interest group or community organizers from the comfort of their own home.

Voters, interest groups, and bad actors utilize e-commerce markets to buy and sell ballots. Before being turned in by a concerned citizen, a Minnesota man attempted to sell his vote on eBay for the 2008 U.S. Presidential election.³¹⁷ The individual was charged, and no one placed a bid on his ballot auction. An individual in upstate New York took the idea of selling votes to a whole new level when he created a website called voteauction.com.³¹⁸ This website sought out individuals who had no interest in voting in elections and auctioned them off in bulk per each state. The auction house then acted as a broker between the voter and the individual or special interest groups advising the voter to choose a particular candidate.³¹⁹ The auction house then verified the voter did indeed vote for that candidate; the voter then returned the ballot via mail and received payment.³²⁰ The website was sold and several states obtained court-ordered restraining orders against the

³¹⁵ *Leslie McCrae Dowless*.

³¹⁶ *Leslie McCrae Dowless*.

³¹⁷ David Hanners, "Minneapolis Man Charged with Offering to Sell His Presidential Vote on EBay," *Twin Cities* (blog), July 2, 2008, <https://www.twincities.com/2008/07/02/minneapolis-man-charged-with-offering-to-sell-his-presidential-vote-on-ebay/>.

³¹⁸ Sascha Segan, "Internet Sites Try to Sell Votes," ABC News, January 6, 2006, <https://abcnews.go.com/Politics/story?id=123069&page=1>.

³¹⁹ Segan.

³²⁰ Segan.

site.³²¹ While these sites do not exist anymore, the dark web would be a perfect environment for this type of activity to thrive on.

While cases like the one in North Carolina are rare, the 2020 U.S. Presidential election did see an influx of absentee ballots due to the pandemic. This influx presents a challenge for election officials to ensure all those who requested an absentee ballot receive them, properly execute them, and return them in a timely manner. The combination of a lack of clarity on the voter's part and the logistical and staffing challenge on election administrators leads to public and campaign questions.

Once again, providing the information on election websites will help alleviate confusion among voters.

Using county or state election websites to display instructions for voters exposes county election websites to foreign adversaries and bad actors. Leading up to the 2020 general election, the Cyber Agency and FBI warned the public and election officials of the potential for Iranian actors to infiltrate election infrastructure in an attempt to disrupt the election.³²² The advisory specifically warned of election website defacements, where a bad actor can access website content and alter the data to fit their narrative.³²³ In an election year where arming the public with as much knowledge as possible about the election process was important, casting doubt on the validity of the county website's information would lead to voter suppression.

Third-party software vendors are still a challenge for the Cyber Agency and election officials. Hackers recently were successful in committing a cybersecurity attack on a large IT firm, SolarWinds, in the United States that provides software to over 33,000 government agencies and private entities.³²⁴ The large IT firm unknowingly introduced

³²¹ Segan.

³²² CISA and FBI, "Joint Cybersecurity Advisory: Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems," Advisory, October 22, 2020.

³²³ CISA and FBI.

³²⁴ Thomas Brewster, "DHS, DOJ and DOD Are All Customers of SolarWinds Orion, The Source of the Huge U.S. Government Hack," *Forbes*, accessed February 20, 2021, <https://www.forbes.com/sites/thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/>.

malware to its customers through a software update they pushed out that allowed hackers to access the customer's technology systems once installed.³²⁵ The malicious code went undetected for over nine months and was finally identified by a private entity cybersecurity team, not the federal government.

A red team could run an operation in which they purchase swing state voter registration information off the dark web. It is estimated that 20 U.S. states' voter registration information, including name, address, party affiliation, and addresses, was located and listed for sale on the dark web in 2018.³²⁶ Low-income areas can be identified using open-source tools, such as the county's website. The red team can obtain party affiliation information along with the address and provide it to special interest groups to be used to purchase votes. These special interest groups often hold the purse strings for these types of grassroots operations, and have, for years, organized social functions, free dinners, and bus rides to the polls. The special interest group would then have local representatives go door-to-door at lower-income voters' homes and offer to purchase their ballot for a certain amount of money. The voter would complete the ballot, sign the outer envelope, and hand it to the individual representing the interest group. The representative will return the ballots via mail or ballot dropbox with election officials none the wiser.

B. RETURNING MAIL-IN BALLOTS

Once a ballot has been cast, a voter has the option of returning the ballot via mail, dropbox, or to an election office by 8 pm on Election Day. Some states will accept ballots ranging from three to 14 days after the election assuming the ballots were postmarked by Election Day. A recent Pew Research survey conducted revealed that returning ballots via mail was still the preferred method but only slightly ahead of ballot drop boxes for voters

³²⁵ Brewster.

³²⁶ Davey Winder, "81.5M Voter Records for Sale on Dark Web Ahead of Midterm Elections," *Forbes*, October 30, 2018, <https://www.forbes.com/sites/daveywinder/2018/10/30/81-5m-voter-records-for-sale-on-dark-web-ahead-of-midterm-elections/>.

in the 2020 election.³²⁷ In anticipation of a rise in mail-in or absentee ballots and relief for the Postal Office, election officials increased the number of ballot drop boxes.

1. Ballot Drop Boxes

States who use universal mail-in voting have relied on ballot drop boxes as an alternative method for returning ballots by mail for years. The use of drop boxes varies from state to state depending on election laws or policies and procedures set in place by state or county election officials. Two types of drop boxes are used by states, indoor boxes monitored by election officials and outdoor unattended boxes near government or election offices. While drop boxes are not new to election security, the number of states that have experience with this process is slim. In the 2016 election, less than 20% of voters returned their ballots via drop boxes.³²⁸ As a result of a warning to states issued by the Postal Service regarding the potential for ballots to be returned after the election, additional states implemented the use of ballot drop boxes as an alternative to return ballots.

With its new popularity comes many questions about its security and the process. For those states inexperienced with drop boxes, the challenge became purchasing drop boxes, identifying the necessary locations, and establishing security protocols in a short period of time.³²⁹ Such challenges led some states to opt to forgo the use of ballot drop boxes over concerns of voter suppression or voter fraud.³³⁰ Even election officials in states with extensive experience with ballot drop boxes raised concerns over election officials in inexperienced states not having sufficient time to implement security protocols, such as security cameras and pick up procedures.

³²⁷ Pew Research Center, “Mail-in Voting, Absentee Ballots and Voter Engagement,” *Pew Research Center—U.S. Politics & Policy* (blog), October 9, 2020, <https://www.pewresearch.org/politics/2020/10/09/voter-engagement-and-interest-voting-by-mail-and-in-person/>.

³²⁸ Pam Fessler, “Ballot Drop Boxes Become Latest Front in Voting Legal Fights,” NPR, August 11, 2020, <https://www.npr.org/2020/08/11/901066396/ballot-drop-boxes-become-latest-front-in-voting-legal-fights>.

³²⁹ Fessler.

³³⁰ Alex Hufford, “The Rise of Ballot Drop Boxes Due to the Coronavirus,” Lawfare, August 27, 2020, <https://www.lawfareblog.com/rise-ballot-drop-boxes-due-coronavirus>.

Manufacturers advise it takes up to six months to create a custom drop box and approximately two months for installation.³³¹ Election officials must also consider the cost of the drop boxes, which is on average \$6,000.³³² With many county election officials operating off limited budgets, states would need to look for assistance from the federal government to obtain the necessary funds. Manufacturers of the drop boxes argue the ballot boxes are impenetrable and can even withstand a car crashing into them.³³³ Security protocols, such as placing security cameras on the box, bolting them to the ground, and built using steel have been put in place to mitigate an attack.³³⁴

The security of a drop box itself is not the only concern for election officials. Security protocols for how the ballots are retrieved and returned must be established to ensure safe delivery to election facilities. For example, in Washington State, county election officials have implemented security protocols, such as requiring a two-person pick up, logbooks, evidence seals with serial numbers, and global positioning system trackers to ensure the successful delivery of all ballots.³³⁵ Establishing security protocols is similar to how law enforcement handles evidence in a criminal case. The mishandling of evidence could result in a case being dropped against the defendant or an individual being acquitted at trial. For this reason, law enforcement agencies have detailed security protocols in place when handling evidence. For election officials, security protocols are just as important, as the mishandling of ballots may possibly result in a voter's ballot not being counted in an election. The challenge becomes, will states with less experience have enough time to implement the necessary security protocol to ensure a fair election?

Although most election officials have a strong security plan, it does not leave them immune from an attack. In October 2020, a drop box in Massachusetts was set on fire and

³³¹ Hufford.

³³² Hufford.

³³³ Fessler, "Ballot Drop Boxes Become Latest Front in Voting Legal Fights."

³³⁴ Fessler.

³³⁵ Melissa Santos, "Security and Ballot Drop Boxes: Here's How It Works in Washington," Renton, WA Patch, August 30, 2020, <https://patch.com/washington/renton/security-ballot-drop-boxes-heres-how-it-works-washington>.

with over 120 ballots inside.³³⁶ Once the fire was extinguished, it was determined a small number of ballots were unreadable or uncountable.³³⁷ A second fire was reported in California in late October where approximately 100 ballots were found damaged.³³⁸ Despite the fact neither one of these cases adversely affected the outcome of the election, it damages the election system's integrity.

In an effort to increase security protocols for ballot drop boxes, red teaming exercises should be conducted against ballot drop boxes around the country to determine how feasible it would be for someone to penetrate or destroy a ballot drop box. The scenarios should cover both attended and unattended ballot drop boxes, an insider and outsider attack, and drop boxes for which administrative controls are in place and for boxes that do not them in place.

2. United States Postal Service

Since the Civil War, the United States Postal Service has been successfully delivering ballots as a result of mail-in voting and absentee ballots.³³⁹ Abraham Lincoln wanted to give soldiers the ability to cast a vote from the battlefield.³⁴⁰ Up until the 2020 Presidential election, neither voters, election officials, nor government officials have aired significant complaints about mail-in voting or the Postal Service's ability to return ballots in a timely manner. In 2014, only 3% of voters expressed doubt in the Postal Service's ability.³⁴¹

³³⁶ Kim Young-Jin and Kaitlin Becker, "Boston Man Arrested in Connection with Ballot Box Fire in Copley Square," *NBC Boston* (blog), October 26, 2020, <https://www.nbcboston.com/news/local/a-ballot-drop-box-in-boston-was-set-on-fire-heres-what-we-know/2218418/>.

³³⁷ Young-Jin and Becker.

³³⁸ Joshua Bote, "Ballot Drop Box Set on Fire in California, 100 Ballots Damaged," *USA Today*, October 20, 2020, <https://www.usatoday.com/story/news/nation/2020/10/20/ballot-drop-box-set-fire-california-100-ballots-damaged/5992101002/>.

³³⁹ Blake Stillwell, "How Absentee Voting for U.S. Troops Won the Civil War and Ended Slavery," *Military.Com Network*, 2020, <https://www.military.com/military-life/how-absentee-voting-us-troops-won-civil-war-and-ended-slavery.html>.

³⁴⁰ Stillwell.

³⁴¹ Natalie Adona and Paul Gronke, *Understanding the Voter Experience: The Public's View of Election Administration and Reform* (Washington, DC: Democracy Fund, 2018), 12.

Over recent years, the Postal Service has experienced financial troubles due to the rise in competitors, lack of sales, and the passage of legislation requiring retirement be paid up front.³⁴² To alleviate the economic problems, the current Postmaster General eliminated many sorting machines, authorized the removal of collection boxes, and cut overtime for employees.³⁴³ Critics of these changes argue the recent changes are well beyond past cost-saving operations and more likely the result of President Trump's goal of eliminating universal mail-in voting in the 2020 election.³⁴⁴ This argument was reinforced when President Trump acknowledged he opposed the signing of a pandemic relief bill that included funding for the Postal Service to perform its duties, including collecting mail-in ballots.³⁴⁵ Although President Trump did ultimately sign the relief bill, he continued to make unfounded accusations against mail-in voting.³⁴⁶

Critics of the Postmaster General saw his changes as a move to enhance the current administration's claim mail-in voting would result in voter fraud.³⁴⁷ It is no secret the Postmaster General has contributed to former President Trump's re-election campaign prior to being appointed Postmaster General.³⁴⁸ The uproar resulted in the Postmaster General agreeing to forego any additional changes until after the 2020 general election.³⁴⁹

³⁴² Miles Parks and Barbara Sprunt, "Louis DeJoy Vows Post Office Can Handle Mail-In Ballots, In Senate Hearing," NPR, August 21, 2020, <https://www.npr.org/2020/08/21/904366258/postmaster-general-faces-senate-as-controversy-persists-over-usps-cuts>.

³⁴³ Parks and Sprunt.

³⁴⁴ Zeeshan Aleem, "The White House Says USPS Isn't Removing Mail-Sorting Machines. Postal Workers Say It Is," Vox, August 16, 2020, <https://www.vox.com/2020-presidential-election/2020/8/16/21370963/usps-postal-service-mail-sorting-machines-trump-meadows-2020-election-ballots>.

³⁴⁵ Barbara Sprunt and Alana Wise, "Trump Opposes Postal Service Funding but Says He'd Sign Bill Including It," NPR, August 13, 2020, <https://www.npr.org/2020/08/13/902109991/trump-admits-to-opposing-funding-for-postal-service-to-block-more-voting-by-mail>.

³⁴⁶ Sprunt and Wise.

³⁴⁷ Parks and Sprunt, "Louis DeJoy Vows Post Office Can Handle Mail-In Ballots"

³⁴⁸ Barbara Sprunt, "Post Office Chief Suspends Controversial Changes until after Election," NPR, August 18, 2020, <https://www.npr.org/2020/08/18/903477948/postmaster-general-will-testify-at-senate-hearing-friday>.

³⁴⁹ Sprunt.

Before the Senate, the Postmaster General testified the Postal Service could deliver ballots “securely and on time,” calling it a “sacred duty.”³⁵⁰

These divisive decisions combined with staffing constraints due to the pandemic have led to individuals seeing delayed delivery of necessities, such as prescriptions and benefits, and raising concerns amongst legislators and government officials about the Postal Service’s ability to deliver ballots on time.³⁵¹ Recent warnings to states about the possibility of delayed returns, combined with the fact that approximately 65,000 mail-in or absentee ballots were not counted in the recent primaries, did little to improve the Postal Service’s reputation with voters and election officials.³⁵²

The previous administration’s comments on mail-in voting, the recent changes to the Postal Service, and the rise in absentee ballot requests have caused voters to question the Postal Service’s ability to deliver their ballots on time or even at all. Prior to the 2020 primaries in Michigan, the Secretary of State released a statement to Michigan voters encouraging them to forgo the use of the postal service and return their ballots via drop box to ensure the ballot is counted.³⁵³

Ultimately, the 2020 election exposed shortcuts taken by the Postal Service’s ability to return ballots in a timely manner.³⁵⁴ The increase in the number of ballots forced the Postal Service to sidestep the final scanning process and deliver directly to the board of elections.³⁵⁵ The lack of scanning led voters and the public to believe 150,000 ballots were not counted, and in response, the Postal Service came out and publicly debunked the claim.³⁵⁶

³⁵⁰ Parks and Sprunt, “Louis DeJoy Vows Post Office Can Handle Mail-In Ballots.”

³⁵¹ Brennan Center for Justice, “What the Postal Service Crisis Means for the November Election.”

³⁵² Brennan Center for Justice.

³⁵³ Sarah Payne, “Secretary of State Encourages Michigan Voters to Use Drop Boxes Six Days before Primary Election,” *The Michigan Daily*, July 29, 2020, <https://www.michigandaily.com/section/government/secretary-state-encourages-michigan-voters-use-drop-boxes-six-days-primary>.

³⁵⁴ McCausland, “Postal Service Says It Delivered Ballots.”

³⁵⁵ McCausland.

³⁵⁶ McCausland.

The exposure of skipped protocols was not the only bad press the Postal Service received. As a result of the concerns of timely deliveries, a federal judge ordered the Postal Service to conduct nightly sweeps of processing facilities in crucial swing states.³⁵⁷ In defiance, the Postal Service stayed its course, which resulted in 7% of absentee or mail-in ballots not being counted in the 2020 election.³⁵⁸

The 7% would not affect the overall outcome of the election, but it demonstrates how important it is for election officials to work closely with the Postal Service to provide information to voters and put security mechanisms in place to track ballots.³⁵⁹ The rapidly increased implementation of mail-in voting highlighted deficiencies within the Postal Service not noticed before that led election officials and the public to doubt the Postal Service and the results of the election. If lessons are not learned from the 2020 election, the Postal Service could become a single point of failure for the election system.

When considering red team attacks against the Postal Service, a direct physical attack might prove sufficient. The processing centers that collect mail-in ballots generally lack complex security that other government buildings have, such as federal courthouses. The Office of Inspector General reports, readily available online for public viewing, often note non-working gates, inoperable cameras, and broken or unlocked doors.³⁶⁰ This information can be used to plan a coordinated breach on a processing center. Targeting a postal processing center in a major city, on a Saturday evening, after hours, could make it easy for red team members to have access to collected ballots that could allow for either the theft or potential alteration of thousands of ballots. These types of operations against secure facilities are already part of government red teaming quite frequently, even with

³⁵⁷ Bogage and Ingraham, “USPS Ballot Problems Unlikely to Change Outcomes in Competitive States.”

³⁵⁸ Bogage and Ingraham.

³⁵⁹ Bogage and Ingraham.

³⁶⁰ Office of Inspector General, *Physical and Environment Controls Site Security View—Summary Report* (Arlington, VA: United States Postal Service, 2019), 6.

targets as sensitive as the Transportation Security Administration and airport access in and around magnetometer stations.³⁶¹

C. STORAGE OF BALLOTS

After a ballot is successfully returned via drop box, mail, or in-person to a central processing facility or county election office, officials can proceed with administrative protocols set in place. Each state determines when ballots will be authorized to be counted and what procedures will be followed. Since ballot counting takes place behind closed doors, election officials recognized the need to provide transparency to the public by creating a tracking system for every ballot cast. Accounting for every ballot at each stage of the administrative process is vital to mail-in voting integrity.

For the process to run smoothly, election officials must hire the appropriate amount of bipartisan staff, train the staff, acquire the necessary amount of space and equipment for processing, and designate a viewing area for poll watchers. As the ballots arrive, the chain of custody will be verified, ballots transferred to trays, and dated and time stamped for tracking purposes. To prevent a voter from voting twice, the envelope barcode is scanned, or an entry is made in the voter registration affirming receipt of the ballot. Signatures are then verified manually or via a scanner and are categorized as accepted or rejected. Rejected ballots will be handled accordingly to state election laws, and accepted ballots will be opened and separated from signature envelopes.

Verifying signatures against the voter registration database provides an opportunity for a bad actor to disrupt the verification process by conducting a ransomware attack on the registration database. A ransomware attack is malware installed on a database that encrypts the information that essentially holds the individual's information until a ransom is paid. Over the last year, ransomware attacks have cost hospitals over \$7 billion in ransom

³⁶¹ "Statement by Secretary Jeh C. Johnson on Inspector General Findings on TSA Security Screening," DHS Press Office, June 1, 2015, <https://www.dhs.gov/news/2015/06/01/statement-secretary-jeh-c-johnson-inspector-general-findings-tsa-security-screening>.

payments for hospital files' return.³⁶² The success of the attacks has led to additional targets; local and state governments have been victimized.³⁶³

Local and state government records include election administrative systems that leave them ripe for an attack.³⁶⁴ Hall County, Georgia, experienced this firsthand in October 2020. The county computer system was compromised, which included the voter signature database.³⁶⁵ The attack did not significantly impact voters' ability to vote; it did slow down the verification process of the signatures on absentee ballots.³⁶⁶ If several of these attacks are done over the country, it could severely impact the Election Day's electoral system.

After several verification processes are conducted, the privacy envelopes are then opened by hand or a machine and run through an optical scanner that records the mark and is stored in the computer's memory. If the machine is unable to verify a mark, a bipartisan team of election workers will flag and review it. If a team of two can determine voter intent, a new ballot will be completed and run through the scanner. The paper ballots are placed back into sorted bins and stored in an evidence vault until 22 days after the election in case of an audit or recount.

Since a voter has the ability to return a ballot to a precinct location, optical scanners located at the precinct will be utilized to scan and tally the ballots. The votes are stored on a media card and transported in a sealed bag by an individual from each party to the central counting location. As an extra security protocol, some states utilize law enforcement as an escort to maintain the storage device's integrity.

³⁶² Richard Forno, "Ransomware Can Interfere with Elections and Fuel Disinformation—Basic Cybersecurity Precautions Are Key to Minimizing the Damage," *Government Technology*, October 30, 2020, <https://www.govtech.com/security/Ransomware-Can-Interfere-with-Elections-and-Fuel-Disinformation--Basic-Cybersecurity-Precautions-Are-Key-to-Minimizing-the-Damage.html>.

³⁶³ Jenni Bergal, "Ransomware Attacks Prompt Tough Question for Local Officials: To Pay or Not to Pay?," *PEW*, March 3, 2020, <https://pew.org/39i2an8>.

³⁶⁴ Forno, "Ransomware Can Interfere with Elections and Fuel Disinformation."

³⁶⁵ Linn F. Freedman, "Ransomware Attack Affects Georgia County Election Administration System," *The National Law Review*, October 27, 2020, <https://www.natlawreview.com/article/ransomware-attack-affects-georgia-county-election-administration-system>.

³⁶⁶ Freedman.

Physical security of election infrastructure is a crucial component to maintaining the integrity of U.S. elections. State and local election officials should ensure they have a security plan in place for the storage of election equipment during and after the election.

Currently, no federal regulations exist dictating how election officials should store and secure their voting equipment.³⁶⁷ The storage facility should be treated like an offsite government facility, and implement controlled access, security cameras, a buddy system, and login procedures.³⁶⁸ J. Alex Halderman, an election infrastructure researcher, recently encountered an unattended voting tabulation machine.³⁶⁹ The machine was left unprotected in a township hall where anyone could gain access to it.³⁷⁰ Having this type of unlimited access to election equipment gives bad actors the ability and time to conduct their attack of choice.³⁷¹

The lack of security resulted in a warehouse in Philadelphia that houses election infrastructure being broken into and items, such as memory cards used to program voting machines and a manufacturer's laptop, were stolen.³⁷² Being in possession of a memory card used to program election infrastructure provides a bad actor the opportunity to manipulate election results. While it appears no attack took place, it is extremely concerning that a storage facility took such little precaution in securing election infrastructure.

Access to funding has caused safeguards for the physical security of election infrastructure to vary amongst local election jurisdictions, which can cause bad actors to focus their attention on jurisdictions where security is lax and has the greatest effect on the

³⁶⁷ "Election Security: State Policies," National Conference of State Legislatures, August 2, 2019, <https://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx>.

³⁶⁸ National Conference of State Legislatures.

³⁶⁹ Steve Friess, "Is Your Vote Secure in Michigan? Cybersecurity Expert Alex Halderman Is Cautiously Optimistic," *Hour Detroit Magazine* (blog), September 4, 2020, <https://www.hourdetroit.com/community/is-voting-secure-in-michigan-cybersecurity-expert-alex-halderman-cautiously-optimistic/>.

³⁷⁰ Friess.

³⁷¹ National Conference of State Legislatures, "Election Security."

³⁷² Frank Bajak and Claudia Lauer, "Laptop, USB Drives Stolen from Philly Election-Staging Site," AP NEWS, October 1, 2020, <https://apnews.com/article/voting-machines-voting-custodio-elections-philadelphia-f8a6453dc9e211ef20e9412d003511b1>.

outcome of the election. The impact could be catastrophic if a virus placed by a bad actor spreads throughout the entire state system.³⁷³ Election officials would argue security procedures are in place to prevent these types of attacks, but with a lack of funding and knowledge available in certain jurisdictions, it is impossible to ensure all jurisdictions have the means and capability to have strong security protocols in place.³⁷⁴

Red team attacks against storage facilities for election infrastructure devices could be approached by locating and identifying the larger storage facility prior to the elections. Once voting machines and scanners are delivered to the individual polling locations, it would be more difficult to access each location and lead to a greater chance of discovery. To identify the storage facility location, a review of the county election website will identify election officials for the county. Surveillance of election officials will eventually lead to the storage facility's location; members can then gain insight into the security protocols. By locating and accessing machines in the primary storage area, tampering with scanners could become easier. Whether or not the machines are actually tampered with, just the theft of scanners and voting machines from a low-security storage facility weeks before an election can easily sow doubt in the minds of voters as to the validity of any votes on Election Day. After a team or individual has gained access, it will be essential to determine how long it takes for election officials to notice their facility's breach and if any election devices were exploited.

D. ELECTION RESULTS

With over 80 million mail-in ballots cast during the 2020 election, it would be impossible for some states to project a winner on election night. Making it even more challenging is that some states allow ballots to be counted up to 14 days after the election, combined with the opportunity for voters to correct an unreadable ballot. The public may not know whom the President is for up to two weeks. Adding to this problem is the fact that electronic voting machines can produce immediate results that are then reported to the

³⁷³ National Conference of State Legislatures, "Election Security."

³⁷⁴ Elizabeth Howard et al., *Defending Elections: Federal Funding Needs for State Elections Security* (New York: Brennan Center for Justice, 2019), 2.

media. In the case of the 2020 election, results from in-person voting revealed President Trump was in the lead in key swing states.

As the mail-in ballots began to be counted in crucial swing states, the pendulum began to swing toward Presidential Candidate Biden. As the polls continued to change in favor of Biden, individuals began circulating disinformation posts on social media about hundreds of ballots being found in crucial swing states to attack the integrity of the system. For example, a social media post began circulating “claiming over a hundred thousand votes had been found in Wisconsin.”³⁷⁵ Election officials quickly debunked the rumor and stated the rise in votes for Biden resulted from the central count facility completing the tally of mail-in ballots, not fraud as claimed.³⁷⁶

Before the general election, the FBI warned the public to be wary of election information being posted on websites or on social media platforms following the closing of election polls on November 3.³⁷⁷ An increasing fear rose amongst the Intelligence Community that due to the unique circumstances of voting in the 2020 U.S. Presidential election, the American public and the world would most likely not know the U.S. Presidential election winner on the morning of November 4.³⁷⁸

The delay in results allowed U.S. adversaries to spread disinformation about the 2020 U.S. elections and cast further doubt in the minds of American’s about the legitimacy of U.S. elections. The FBI encouraged all Americans to bear responsibility for ensuring the information came from a valid source before sharing it with others verbally or on social media sites.³⁷⁹

³⁷⁵ Eric Litke and Madeline Heim, “Fact Check: Wisconsin Did Not ‘Find’ 100K Ballots around 4 a.m. the Morning after the Election, or Take Break from Counting Votes,” *Milwaukee Journal Sentinel*, accessed February 20, 2021, <https://www.jsonline.com/story/news/politics/elections/2020/11/04/wisconsin-didnt-find-ballots-stop-count-voter-fraud-claims-untrue-politifact/6165435002/>.

³⁷⁶ Litke and Heim.

³⁷⁷ Internet Crime Complaint Center (IC3), “Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results,” Federal Bureau of Investigation, September 22, 2020, <https://www.ic3.gov/media/2020/200922.aspx>.

³⁷⁸ Internet Crime Complaint Center (IC3).

³⁷⁹ Internet Crime Complaint Center (IC3).

This nation's foreign adversaries are not the only challenge to the spread of disinformation. The Commander in Chief created a post early on the morning of November 4 on Twitter claiming victory even though crucial swing states had not revealed a winner.³⁸⁰ This type of misinformation can lead to confusion and lack of trust in election results.³⁸¹ Twitter and Facebook immediately flagged the President's tweet to prevent the spread of misinformation.³⁸² The 2020 election was a perfect example of how a disinformation campaign against mail-in voting could be used to cause distrust in the U.S. electoral system.

An example of a red teaming attack would consist of members scouring social media and blogs to research the various activist groups to identify which group trends the most. Once activist groups are chosen, a deep fake video is created showing a prominent newscaster airing a news story and video of several crates full of ballots being removed from unmarked vehicles and brought in through the back door of a central counting facility at 3 a.m. The video will then be circulated to activist groups in an effort to spread disinformation and discredit the mail-in ballot process. The Stanford History Education Group conducted a study to determine 3,446 high school students' ability to distinguish between what is real or fake on the internet.³⁸³ The study revealed approximately 52% of students took a video of an individual stuffing ballots as proof of voter fraud in the 2016 election without attempting to verify the truth.³⁸⁴ The goal of the attacks is to determine how quickly social media platforms are able to identify a deep fake and flag the posts as disinformation and how effective election officials are in combating the attack.

³⁸⁰ Sandler, "Half of Trump's Twitter and Facebook Posts since Election Day Flagged."

³⁸¹ Elizabeth Dwoskin and Craig Timberg, "Misinformation Dropped Dramatically the Week after Twitter Banned Trump and Some Allies," *Washington Post*, January 16, 2021, <https://www.washingtonpost.com/technology/2021/01/16/misinformation-trump-twitter/>.

³⁸² Sandler, "Half of Trump's Twitter and Facebook Posts since Election Day Flagged."

³⁸³ Joel Breakstone et al., *Students' Civic Online Reasoning: A National Portrait* (Stanford, CA: The Stanford History Education Group, 2020), 3, <https://stacks.stanford.edu/file/druid:gf151tb4868/Civic%20Online%20Reasoning%20National%20Portrait.pdf>.

³⁸⁴ Breakstone et al., 3.

While history had demonstrated fraud is rare when voting by mail, the rapid increase in its use in the 2020 U.S. Presidential election exposed vulnerabilities within the electoral system. Election officials faced the monumental task of implementing a complex system in a short amount of time. Applying systems thinking by mapping out the process would have afforded election officials the ability to recognize vulnerabilities prior to implementing the change. Unfortunately, some of the quick decisions made with universal mail-in voting were made without consideration of how those changes could adversely affect other components within the electoral system. Systems mapping would have revealed how vital chain of custody procedures were, how severely underfunded and understaffed the Postal Service was, and how vulnerable voter registration databases were to a ransomware attack. The diagram, as shown in Figure 10, would have afforded the officials the ability to pivot and increase security protocols.

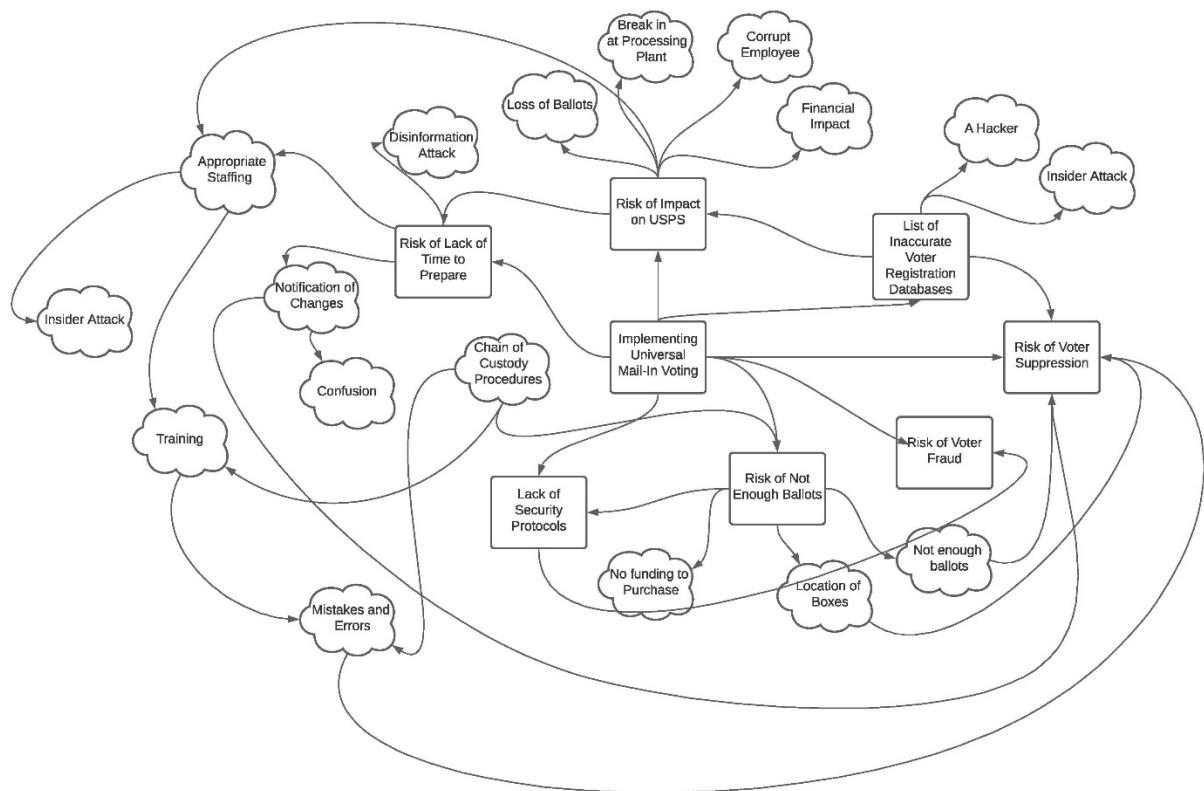


Figure 10. Systems Thinking Mapping of the Implementation of Mail-In Voting

Preparing for future attacks is a key component of securing the U.S. electoral system. While nothing is ever 100% secure, planning for what is possible will assist election officials in putting protocols in place to mitigate the damage. Thus, red teaming could be crucial to election security. Election officials are so busy correcting the problems at hand that they neglect to plan for the future. Foreign adversaries are constantly testing the U.S. electoral system for vulnerabilities to exploit. By applying red teaming to the U.S. electoral system, it may finally be possible to play a competitive game with this nation's adversaries.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

Any election's goal is to ensure that all individuals willing and eligible to vote are afforded the opportunity and that their votes are accurately counted. While past work by election officials, researchers, and legislatures has succeeded in increasing voter participation and experienced fewer cases of voter fraud, the system is still experiencing challenges that prevents it from obtaining its goal of 100% participation with 100% accuracy. In a time when U.S. politics are more polarized than ever, everyone must continue to evaluate and reinforce the U.S. electoral system to prevent potential vulnerabilities that U.S. adversaries and political opponents can exploit to cast doubt on the validity of the system. In the past, election officials have solved challenges within the system using linear thinking. They identify the problem at hand and create a solution. What election officials may not realize is that the solution may lead to unintended consequences in other system components. For example, the 2020 election saw that only addressing the problem at hand did indeed create additional challenges to the system, which were then used to cast doubt on the validity of the results. This thesis studied how systems thinking and red teaming could be applied as a method to evaluate and reinforce the integrity of the electoral system.

Systems thinking provides an opportunity for election officials to study the inner workings of the relationships between the various components that make up the electoral system and how making a change to one area will directly impact another. Systems thinking will help election officials identify potential pitfalls or advantages of the prospective changes to the system prior to implementation. Applying systems thinking to the challenge of voting in a global pandemic would have helped officials identify the vulnerabilities associated with the rapid implementation of universal mail-in voting. By mapping out the mail-in voting, officials would have recognized that relaxing security and chain of custody protocols, last-minute changes to election laws and procedures, and poor communication could lead the public to doubt the integrity of the system.

Red teaming is not new to the U.S. electoral system. After the 2016 election, the Cyber Agency began focusing on how to secure electronic election infrastructure and

enlisted the use of red team exercises to test the resilience of electronic critical infrastructure and incident response.³⁸⁵ While the agency has made great strides in testing and securing the electronic critical infrastructure, the focus now needs to shift to ensure security protocols are in place for the physical critical infrastructure, such as storage and processing facilities, voting locations, and election officials.³⁸⁶ While the Cyber Agency has provided election officials with written guidance on preparing and securing election facilities, additional steps need to be taken to protect them from a potential attack.³⁸⁷ The recent polarization of the 2020 U.S. Presidential election and the civil unrest ultimately led to an attack on the Capitol. While the attacks did not prevent the Joint Session of Congress from certifying Joe Biden as the winner of the 2020 election, it did leave a large scar on this country's democracy. Election officials must be prepared in the future for potential attacks on election-related facilities. Red team exercises should be conducted on all election critical infrastructure to include physical locations to test the durability of security protocols and election officials.

A. RECOMMENDATIONS

Over the years, election officials and stakeholders have solely focused on the current challenge at hand rather than analyzing the system as a whole. The focus becomes identifying what the specific problem is and how to fix it before the next election. The recent attack on mail-in voting and the electoral system highlighted the need for election officials to evaluate why individuals could create a large-scale disinformation campaign against mail-in voting. Election officials should explore the incorporation of after-action reviews to assess an election's performance and any problems identified in the election,

³⁸⁵ Cybersecurity and Infrastructure Security Agency, *Elections Cyber Tabletop Exercise Package: Situation Manual* (Rosslyn, Arlington, VA: Cybersecurity and Infrastructure Security Agency, 2020), 3, <https://www.cisa.gov/sites/default/files/publications/Elections-Cyber-Tabletop-Exercise-Package-20200128-508.pdf>.

³⁸⁶ Office of Inspector General, *DHS Has Secured the Nation's Election Systems, but Work Remains to Protect the Infrastructure* (Washington, DC: Department of Homeland Security, 2020), 10, <https://www.oig.dhs.gov/sites/default/files/assets/2020-10/OIG-21-01-Oct20.pdf>.

³⁸⁷ Cybersecurity and Infrastructure Security Agency, *Election Security—Physical Security of Voting Locations and Election Facilities* (Rosslyn, Arlington, VA: Cybersecurity and Infrastructure Security Agency, 2020), 1–3, https://www.cisa.gov/sites/default/files/publications/physical-security-of-voting-location-election-facilities_v2_508.pdf.

analyze the process through the lens of systems thinking, and conduct red teaming exercises to test the security protocols put in place.

1. Conducting After-Action Reports through the Use of Systems Thinking

Local, state, and federal law enforcement agencies and the U.S. military conduct after-action reviews of major events to evaluate the performance of the security or response plan.³⁸⁸ Often law enforcement agencies conduct after-action reviews following a major incident, but after-action reviews are still beneficial in a successful event. After-action reviews allow stakeholders to conduct a thorough review of what worked, what needs to be improved, and how to reinforce or strengthen the security plan. Agencies or departments must continue to conduct a self-examination of security protocols and response plans to ensure their effectiveness.

The U.S. electoral system can benefit from conducting after-action reviews in which systems thinking methodologies are utilized for the final analysis. While the U.S. electoral system has experienced very little fraud over the years, continuing to study and evaluate the resiliency of the system is vital to maintaining this democracy. Conducting after-action reviews in each state and local jurisdiction will allow election officials to identify vulnerabilities within the system that political opponents or adversaries can exploit. Systems thinking will provide the insight needed to determine how the components are connected and how to use those relationships to create a solution. Just as law enforcement agencies must continue to plan for future attacks, so must election officials.

First, the head election official for each state will need to establish an after-action review's purpose and size.³⁸⁹ Due to the U.S. electoral system's decentralized nature, each state's electoral system varies in complexity. It should be analyzed from beginning to end to determine how intertwined the subsystems are compared to the system as a whole. Unlike after-action reviews conducted by law enforcement personnel or the U.S. military

³⁸⁸ National Police Foundation, *How to Conduct an After Action Review* (Washington, DC: Office of Community Oriented Policing Services, 2020), 1–7, <https://cops.usdoj.gov/RIC/Publications/cops-w0878-pub.pdf>.

³⁸⁹ National Police Foundation, 37.

in which each entity has a specific incident or operation to review, election officials must consider the process as a whole. Any recommendations made to the electoral process could severely impact other areas of the system and inadvertently cause more damage.

Second, election officials will need to determine if the review will be conducted internally or by an outside source or a combination of both.³⁹⁰ Choosing an outsider as team lead will ensure impartiality when reviewing the current process in place. When it comes to rounding out the team, election officials should seek individuals who have election experience and familiarity with the specific state laws. Still, they can also remain unbiased while conducting the review. The political component must also be addressed. For that reason, the team should be composed of bi-partisan officials to prevent accusations of bias towards one party.

Once the team has been established, team members should seek U.S. stakeholders and interview them regarding their role in the system, challenges, if any, they face, and provide insight into how they interact directly with the other subsections. Team members should highlight the importance of these interviews and how their information can be used to reinforce the electoral system.

The information collected from the stakeholders can then be used to conduct an analysis through systems thinking. Team members should begin by mapping out all the components that encompass the electoral system. Once the components are identified, members can start highlighting how interconnected each of those relationships are and begin to identify the system's strengths and weaknesses. When evaluating vulnerabilities, those interconnected relationships must be considered when looking for solutions. Even the smallest change could inadvertently affect another component and create an additional vulnerability. That diagram will allow the team members to foresee any challenges that may arise due to the potential change. This visual can then be presented in a report format in conjunction with a set of recommendations to the election officials in each state.

³⁹⁰ National Police Foundation.

2. Executing Red Team Attacks on Non-Cyber Election Infrastructure

While CISA currently conducts red teaming exercises on cyberinfrastructure, the Cyber Agency should expand its red teaming exercises to include all election critical infrastructure consisting of postal processing centers, voting machine storage facilities, central counting locations, insider attacks at polling stations, among others. Ultimately, a red team's functions frequently involve vulnerability probes with team members assuming the role of a potential adversary.³⁹¹ In these types of attacks, the red teams can test defenses, identify shortcomings, document their findings, and report back to the Cyber Agency for disbursement to the nation's election officials. The agency should consult with subject matter experts from within the DHS, DOD, and private entities to ascertain the best methods of attack employed in previous investigations made by the private sector or government agencies.

The results of those findings, after a formal review, can then be presented to all the election stakeholders, particularly the state election officials, in the form of Tabletop Exercise Packets. These tabletop exercises are a cost-efficient and productive way for the Cyber Agency to share these findings, receive input, and increase critical thinking in all stakeholders.³⁹² Presenting these tabletop exercises in the form of an actual, ongoing, immediate crisis is also a way for all players to engage with a sense of urgency actively. For example, adding the urgency of news reporters calling the Governor's Office to inquire about allegations of ballot tampering by polling station members could be a way of increasing pressure on local officials to resolve situations directly in the face of television and social media attacks.

Participants should be notified ahead of time of the tabletop exercises but should not be provided any information regarding the scenarios. Although these scenarios are not being conducted in the field, they should be treated with a sense of urgency. The scenario should be used to put as much pressure as possible on all players, including the poll workers, the media relations team, the board of electors, the head county election official,

³⁹¹ Zenko, *Red Team*, xxii.

³⁹² Zenko, 133–141.

and others. Developing exercise objectives will help organizers identify gaps in the stakeholder's plans; it will allow others to test policies and evaluate the team's capabilities. Time constraints can even be placed on the scenarios to keep the pressure on teams and allow the exercise to stay on track. Finally, a summary of the exercise enables all involved to dissect what went wrong and create viable solutions.

B. CONCLUSION

This thesis sought to answer the question: How can red teaming and systems thinking be applied to reinforce the integrity of the U.S. electoral system? Over the last decade, foreign adversaries and high-ranking elected officials have tested the U.S. electoral system, which exposed vulnerabilities within the system that must be addressed to preserve its integrity. The recent implementation of universal mail-in voting provided the perfect case study to test the application of systems thinking and red teaming. Based on the case study findings, this thesis recommended two proposals for inserting the use of after-action reports in which systems thinking methodologies are utilized for the final analysis and the use of vulnerability probes to test the resiliency of election infrastructure. The recommendations can identify current and future vulnerabilities within the electoral system and provide the opportunity to test solutions prior to implementation. It should be noted the recommendations will require buy-in from election stakeholders and will require additional funding to obtain the personnel necessary to perform the tasks. While election officials must consider the challenges to implementing the recommendations, they must also consider the importance of maintaining a secure and resilient electoral system.

LIST OF REFERENCES

- Adams, Margot. "The Voting Technology Problem." Stanford Law School, January 16, 2018. <https://pacscenter.stanford.edu/publication/the-voting-technology-problem/>.
- Adona, Natalie, and Paul Gronke. Understanding the Voter Experience: The Public's View of Election Administration and Reform. Washington, DC: Democracy Fund, 2018.
- Aleem, Zeeshan. "The White House Says USPS Isn't Removing Mail-Sorting Machines. Postal Workers Say It Is." Vox, August 16, 2020. <https://www.vox.com/2020-presidential-election/2020/8/16/21370963/usps-postal-service-mail-sorting-machines-trump-meadows-2020-election-ballots>.
- Allcott, Hunt, and Matthew Gentzkow. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31, no. 2 (Spring 2017): 211–36.
- Alvarez, R. Michael Thad E. Hall, and Morgan H. Llewellyn. "Are Americans Confident Their Ballots Are Counted?." *Journal of Politics* 70, no. 3 (July 2008): 754–66.
- Atkeson, Lonna Rae, Yann P. Kerevel, R. Michael Alvarez, and Thad E. Hall. "Who Asks for Voter Identification? Explaining Poll-Worker Discretion." *Journal of Politics* 76, no. 4 (2014): 944–57. <https://doi.org/10.1017/s0022381614000528>.
- Bajak, Frank, and Claudia Lauer. "Laptop, USB Drives Stolen from Philly Election-Staging Site." AP NEWS, October 1, 2020. <https://apnews.com/article/voting-machines-voting-custodio-elections-philadelphia-f8a6453dc9e211ef20e9412d003511b1>.
- Bauer, Scott. "Wisconsin Issues Recount Order in 2 Counties as Trump Wanted." AP NEWS, November 19, 2020. <https://apnews.com/article/wisconsin-recount-2-counties-f408a7b43deb96e2ac7ff0b24a2f968a>.
- Bergal, Jenni. "Ransomware Attacks Prompt Tough Question for Local Officials: To Pay or Not to Pay?." PEW, March 3, 2020. <https://pew.org/39i2an8>.
- Berman, Ari. "How the 2000 Election in Florida Led to a New Wave of Voter Disenfranchisement." July 28, 2015. <https://www.thenation.com/article/archive/how-the-2000-election-in-florida-led-to-a-new-wave-of-voter-disenfranchisement/>.
- Blaze, Matt, Harri Hurst, Margaret MacAlpine, Mark Hanley, Jeff Moss, Rachel Wehr, Kendall Spencer, and Christopher Ferris. *DEF CON 27: Voting Machine Hacking Village*. Furlong, PA: Voting Village, 2019. <https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf>.

- Bogage, Jacob, and Christopher Ingraham. "USPS Ballot Problems Unlikely to Change Outcomes in Competitive States." November 4, 2020. ProQuest.
- Bote, Joshua. "Ballot Drop Box Set on Fire in California, 100 Ballots Damaged." USA Today, October 20, 2020. <https://www.usatoday.com/story/news/nation/2020/10/20/ballot-drop-box-set-fire-california-100-ballots-damaged/5992101002/>.
- Boudreaux, Benjamin, Quentin E. Hodgson, and Edward Chan. Quick Look: Elections Security Lessons Learned from 2017–2018 Election Cycle, Homeland Security Operational Analysis Center. Santa Monica, CA: RAND, 2019.
- Breakstone, Joel, Mark Smith, Sam Wineberg, Amie Rapaport, Jill Carle, Marshall Garland, and Anna Saavedra. *Students' Civic Online Reasoning: A National Portrait*. Stanford, CA: The Stanford History Education Group, 2020. <https://stacks.stanford.edu/file/druid:gf151tb4868/Civic%20Online%20Reasoning%20National%20Portrait.pdf>.
- Brennan Center for Justice. *Former Ohio Elections Chief Blackwell Brings a Troubled Record on Elections to Fraud Commission*. New York: New York University School of Law, n.d. Accessed September 8, 2020. https://www.brennancenter.org/sites/default/files/analysis/Ken_Blackwell.pdf.
- . "The Mueller Report Exposed Weaknesses in U.S. Democratic Institutions that H.R. 1 Would Address." July 10, 2019. <https://www.brennancenter.org/our-work/research-reports/mueller-report-exposed-weaknesses-us-democratic-institutions-hr-1-would>.
- . "What the Postal Service Crisis Means for the November Election." August 19, 2020. <https://www.brennancenter.org/our-work/research-reports/what-postal-service-crisis-means-november-election>.
- Brewster, Thomas. "DHS, DOJ and DOD Are All Customers of SolarWinds Orion, The Source of the Huge U.S. Government Hack." *Forbes*. Accessed February 20, 2021. <https://www.forbes.com/sites/thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/>.
- Brumback, Kate. "Georgia Again Certifies Election Results Showing Biden Won." AP NEWS, December 7, 2020. <https://apnews.com/article/election-2020-joe-biden-donald-trump-georgia-elections-4eeea3b24f10de886bcdeab6c26b680a>.
- . "Second Georgia County Finds Previously Uncounted Votes from 2020 Presidential Election." ABC11 Raleigh-Durham, November 17, 2020. <https://abc11.com/8049192/>.

- Brumfield, Cynthia. “What Is the CISA? How the New Federal Agency Protects Critical Infrastructure.” CSO Online, July 1, 2019. <https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html>.
- Burden, Barry C., David T. Canon, Kenneth R. Mayer, Donald P. Moynihan, and Jacob R. Neiheisel. “What Happens at the Polling Place: Using Administrative Data to Look Inside Elections.” *Public Administration Review* 77, no. 3 (2017): 354–64.
- Burris, Arthur L., and Eric Fischer. *The Help America Vote Act and Election Administration: Overview of 2016*. Washington, DC, Congressional Research Service, 2016.
- Cain, Bruce E., Todd Donovan, and Caroline J. Tolbert. *Democracy in the States: Experiments in Election Reform*. Washington, DC: Brookings Institute Press, 2008.
- CISA and FBI. “Joint Cybersecurity Advisory: Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems.” Advisory, October 22, 2020.
- Coleman, Kevin J. The Presidential Nomination Process and the National Party Conventions, 2016: Frequently Asked Questions. CRS Report No. R42533. Washington, DC: Congressional Research Service, 2015.
- Coleman, Kevin J., Joseph E. Cantor, and Thomas H. Neale, *Presidential Elections in the United States: A Primer*. Order Code RL30527. Washington, DC: Congressional Research Service, 2020. <https://fas.org/sgp/crs/misc/RL30527.pdf>.
- Committee on Homeland Security Democrats. *Congressional Task Force on Election Security: Final Report*. Washington, DC: Committee on Homeland Security, 2018. <https://cha.house.gov/sites/democrats.cha.house.gov/files/documents/TFESReport.pdf>.
- Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology, Committee on Science, Technology, and Law, Policy and Global Affairs, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, and National Academies of Sciences, Engineering, and Medicine. *Securing the Vote: Protecting American Democracy*. Washington, DC: National Academies Press, 2018. <https://doi.org/10.17226/25120>.
- Congressional Research Service. Counting Electoral Votes: An Overview of Procedures as the Joint Session, Including Objections by Members of Congress. CRS Report No. RL32717. Washington, DC: Congressional Research Service, 2020.
- Connors, Edward. Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement. Alexandria, VA: Institute for Law & Justice, 2007.

- Corse, Alexa. "Voting-Machine Parts Made by Foreign Suppliers Stir Security Concerns." *Wall Street Journal*, December 16, 2019. <https://www.wsj.com/articles/voting-machine-parts-made-by-foreign-suppliers-stir-security-concerns-11576494003>.
- Cybersecurity and Infrastructure Security Agency. *Election Security—Physical Security of Voting Locations and Election Facilities*. Rosslyn, Arlington, VA: Cybersecurity and Infrastructure Security Agency, 2020. https://www.cisa.gov/sites/default/files/publications/physical-security-of-voting-location-election-facilities_v2_508.pdf.
- . *Elections Cyber Tabletop Exercise Package: Situation Manual*. Rosslyn, Arlington, VA: Cybersecurity and Infrastructure Security Agency, 2020. <https://www.cisa.gov/sites/default/files/publications/Elections-Cyber-Tabletop-Exercise-Package-20200128-508.pdf>.
- D'Souza, Vijay, and Rebecca Gambler. *Election Security: DHS Plans Are Urgently Needed to Address Identified Challenges before the 2020 Elections*. GAO-20-267. Washington, DC: Government Accountability Office, 2020. <https://www.gao.gov/assets/710/704314.pdf>.
- Das, Atanu. "Mitigating Potential Vote-By-Mail Fraud while Simultaneously Increasing Vote-By-Mail Ballot Acceptance by Utilizing Facial Recognition and Multifactor Authentication Technology." *Harvard Journal of Law* 34 (Fall 2020): 1–16.
- Department of Homeland Security. "Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector." January 6, 2017. <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.
- . "Written Testimony of NPPD for a House Oversight and Government Reform Subcommittees on Information Technology and Intergovernmental Affairs Hearing Titled 'Cybersecurity of Voting Machines.'" November 29, 2017. <https://www.dhs.gov/news/2017/11/29/written-testimony-nppd-house-oversight-and-government-reform-subcommittees>.
- Department of Homeland Security Office of Inspector General. *United States Secret Service After-Action Review of Inaugural Security (Redacted)*. Washington, DC: Department of Homeland Security, 2009. https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIGr_10-04_Oct09.pdf.
- Department of Justice. "The Help America Vote Act of 2002." August 6, 2015. <https://www.justice.gov/crt/help-america-vote-act-2002>.

- Desilver, Drew. “Amid Pandemic, the Long Decline of in-Person Voting on Election Day Is Likely to Accelerate This Year.” *Pew Research Center* (blog). November 3, 2020. <https://www.pewresearch.org/fact-tank/2020/11/03/amid-pandemic-the-long-decline-of-in-person-voting-on-election-day-is-likely-to-accelerate-this-year/>.
- DHS Press Office. “Statement by Secretary Jeh C. Johnson on Inspector General Findings on TSA Security Screening.” June 1, 2015. <https://www.dhs.gov/news/2015/06/01/statement-secretary-jeh-c-johnson-inspector-general-findings-tsa-security-screening>.
- Diresta, Renee, Carly Miller, Vanessa Molter, John Pomfret, and Glenn Tiffert. *Tell China’s Story: The Chinese Communist Party’s Campaign to Shape Global Narratives*. Stanford, CA: Stanford Internet Observatory, 2020. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf.
- Durkee, Alison. “Kentucky Postal Worker Charged for Throwing 111 Ballots in Dumpster.” *Forbes*, October 27, 2020. <https://www.forbes.com/sites/alisondurkee/2020/10/27/kentucky-postal-worker-charged-for-throwing-111-ballots-in-dumpster/>.
- Dwoskin, Elizabeth, and Craig Timberg. “Misinformation Dropped Dramatically the Week after Twitter Banned Trump and Some Allies.” *Washington Post*, January 16, 2021. <https://www.washingtonpost.com/technology/2021/01/16/misinformation-trump-twitter/>.
- Eckman, Sarah J., R. Sam Garrett, and Karen L. Shanton. *Federal Election Results: Frequently Asked Questions*. CRS Report No. R46565. Washington, DC: Congressional Research Service, 2020.
- Election Assistance Commission. *History of the National Clearinghouse on Election Administration*. Washington, DC: Election Assistance Commission, 2019.
- . *Starting Point: U.S. Election Systems as Critical Infrastructure*. Washington, DC: Election Assistance Commission, 2017. https://www.eac.gov/sites/default/files/eac_assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.
- . *The Election Administration and Voting Survey: 2016 Comprehensive Report*. Washington, DC: Election Assistance Commission, 2017. https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf.
- Elving, Ron. “The Florida Recount of 2000: A Nightmare That Goes on Haunting.” National Public Radio, November 12, 2018. <https://www.npr.org/2018/11/12/666812854/the-florida-recount-of-2000-a-nightmare-that-goes-on-haunting>.

- Federal News Network. "DHS Teams Hunt for Weaknesses in Federal Cyber Networks." July 11, 2012. <https://federalnewsnetwork.com/all-news/2012/07/dhs-teams-hunt-for-weaknesses-in-federal-cyber-networks/>.
- Fessler, Pam. "Ballot Drop Boxes Become Latest Front in Voting Legal Fights." NPR, August 11, 2020. <https://www.npr.org/2020/08/11/901066396/ballot-drop-boxes-become-latest-front-in-voting-legal-fights>.
- Fife, Brian L. *Reforming the Electoral Process in America: Toward More Democracy in the 21st Century*. Santa Barbara, CA: ABC-CLIO, LLC, Praeger, 2010.
- Fischer, Eric A., R. Sam Garrett, and L. Paige Whitaker. *State Voter Identification Requirements: Analysis, Legal Issues, and Policy Considerations*. Washington, DC: Congressional Research Service, 2016.
- Forno, Richard. "Ransomware Can Interfere with Elections and Fuel Disinformation—Basic Cybersecurity Precautions Are Key to Minimizing the Damage." *Government Technology*, October 30, 2020. <https://www.govtech.com/security/Ransomware-Can-Interfere-with-Elections-and-Fuel-Disinformation--Basic-Cybersecurity-Precautions-Are-Key-to-Minimizing-the-Damage.html>.
- Freedman, Linn F. "Ransomware Attack Affects Georgia County Election Administration System." *The National Law Review*, October 27, 2020. <https://www.natlawreview.com/article/ransomware-attack-affects-georgia-county-election-administration-system>.
- Friess, Steve. "Is Your Vote Secure in Michigan? Cybersecurity Expert Alex Halderman Is Cautiously Optimistic." *Hour Detroit Magazine* (blog). September 4, 2020. <https://www.hourdetroit.com/community/is-voting-secure-in-michigan-cybersecurity-expert-alex-halderman-cautiously-optimistic/>.
- Garnett, Holly Ann. "Evaluating Electoral Management Body Capacity." *International Political Science Review* 40, no. 3 (2019): 335–53.
- Georgia Secretary of State Press Office. "Historic First Statewide Audit of Paper Ballots Upholds Result of Presidential Race." November 19, 2021. https://sos.ga.gov/index.php/elections/historic_first_statewide_audit_of_paper_ballots_upholds_result_of_presidential_race.
- . "Secretary Raffensperger Announces Completion of Voting Machine Audit Using Forensic Techniques No Sign of Foul Play." Accessed February 25, 2021. https://sos.ga.gov/index.php/elections/secretary_raffensperger_announces_completion_of_voting_machine_audit_using_forensic_techniques_no_sign_of_foul_play.

- Gonzales, Richard. "North Carolina GOP Operative Faces New Felony Charges that Allege Ballot Fraud." NPR, July 30, 2019. <https://www.npr.org/2019/07/30/746800630/north-carolina-gop-operative-faces-new-felony-charges-that-allege-ballot-fraud>.
- Good, Chris. "When It Comes to Election Cybersecurity, Decentralized System Is Viewed as Both Blessing and Curse." ABC News, October 31, 2018. <https://abcnews.go.com/Politics/election-cybersecurity-decentralized-system-viewed-blessing-curse/story?id=58877082>.
- Gottfried, Jeffrey, Michael Barthel, Elisa Shearer, and Amy Mitchell. "Where Americans Are Getting News About the 2016 Presidential Election." *Pew Research Center's Journalism Project* (blog). February 4, 2016. <https://www.journalism.org/2016/02/04/the-2016-presidential-campaign-a-news-event-thats-hard-to-miss/>.
- Government Accountability Office. *ELECTIONS: State Laws Addressing Voter Registration and Voting on or before Election Day*. GAO-13-90R. Washington, DC: Government Accountability Office, 2012.
- Greenwood, Shannon, Andres Perrin, and Maeve Duggan. "Demographics of Social Media Users in 2016." Pew Research Center: Internet, Science & Tech, November 11, 2016. <https://www.pewresearch.org/internet/2016/11/11/social-media-update-2016/>.
- Gronke, Paul. "Early Voting Reforms and American Elections." *William and Mary Bill of Rights Journal* 17, no. 2 (December 2008): 423–51.
- Gunther, Richard, Paul A. Beck, and Eric C. Nisbet. "Fake News Did Have a Significant Impact on the Vote in the 2016 Election: Original Full-Length Version with Methodological Appendix." *The Conversation*, February 15, 2018.
- Halderman, J. Alex. *Testimony: Russian Interference in the 2016 Elections*. Washington, DC: Senate Select Committee on Intelligence, 2017. <https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf>.
- Hall, Thad, J. Quin Monson, and Kelly D. Patterson. "Poll Workers and the Vitality of Democracy: An Early Assessment." *PS: Political Science & Politics* 40, no. 4 (October 2007): 647–54. <https://doi.org/10.1017/S104909650707103X>.
- Hamilton, Don. "The Oregon Voting Revolution." *The American Prospect* 17, no. 5 (2006): A3.
- Hamilton, Isobel. "Twitter Labels Trump Mail-in Voting Tweet 'Misleading,' Stops Retweets." Business Insider, October 27, 2020. <https://www.businessinsider.com/twitter-trump-tweet-mail-voting-warning-label-misinformation-block-retweet-2020-10>.

- Hanners, David. "Minneapolis Man Charged with Offering to Sell His Presidential Vote on EBay." *Twin Cities* (blog). July 2, 2008. <https://www.twincities.com/2008/07/02/minneapolis-man-charged-with-offering-to-sell-his-presidential-vote-on-ebay/>.
- Harper, Ruth A. "The Social Media Revolution: Exploring the Impact on Journalism and News Media Organizations." *Inquiries Journal* 2, no. 03 (2010): 1. <http://www.inquiriesjournal.com/articles/202/the-social-media-revolution-exploring-the-impact-on-journalism-and-news-media-organizations>.
- Hasen, Richard L. *The Voting Wars: From Florida 2000 to the Next Election Meltdown*. New Haven, CT: Yale University Press, 2012.
- Howard, Elizabeth, Christopher Deluzio, Paul Rosenzweig, Rachael Dean Wilson, and David Salvo. *Defending Elections: Federal Funding Needs for State Elections Security*. New York: Brennan Center for Justice, 2019.
- Hufford, Alex. "The Rise of Ballot Drop Boxes Due to the Coronavirus." Lawfare, August 27, 2020. <https://www.lawfareblog.com/rise-ballot-drop-boxes-due-coronavirus>.
- Internet Crime Complaint Center (IC3). "Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results." Federal Bureau of Investigation, September 22, 2020. <https://www.ic3.gov/media/2020/200922.aspx>.
- James, Toby. *Comparative Electoral Management: Performance, Networks and Instruments*. London: Routledge, 2019. <https://doi.org/10.4324/9781315545172>.
- Kamarck, Elaine, and Christine Stenglein. "Low Rates of Fraud in Vote-by-Mail States Show the Benefits Outweigh the Risks." *Brookings* (blog). June 2, 2020. <https://www.brookings.edu/blog/fixgov/2020/06/02/low-rates-of-fraud-in-vote-by-mail-states-show-the-benefits-outweigh-the-risks/>.
- Kamarck, Elaine, and John Hudak. "How to Get Rid of the Electoral College." *Brookings* (blog). December 9, 2020. <https://www.brookings.edu/blog/fixgov/2020/12/09/how-to-get-rid-of-the-electoral-college/>.
- Kerner, Sean Michael. "DHS Using Red Team Approach to Identify Cyber-Security Issues." eWeek, August 13, 2018. <https://www.eweek.com/security/dhs-using-red-team-approach-to-improve-national-cyber-security>.
- Kirby, Jen. "Are China and Iran Meddling in U.S. Elections? It's Complicated." Vox, September 15, 2020. <https://www.vox.com/21418513/china-iran-us-election-meddling-russia>.

- Klonsky, Joanna. "The Caucus System in the U.S. Presidential Nominating Process." Council on Foreign Relations. Accessed February 24, 2021. <https://www.cfr.org/backgrounders/caucus-system-us-presidential-nominating-process>.
- Kurtzleben, Danielle. "Did Fake News on Facebook Help Elect Trump? Here's What We Know." NPR, April 11, 2018. <https://www.npr.org/2018/04/11/601323233/6-facts-we-know-about-fake-news-in-the-2016-election>.
- Litke, Eric, and Madeline Heim. "Fact Check: Wisconsin Did Not 'Find' 100K Ballots around 4 a.m. the Morning after the Election, or Take Break from Counting Votes." *Milwaukee Journal Sentinel*. Accessed February 20, 2021. <https://www.jsonline.com/story/news/politics/elections/2020/11/04/wisconsin-didnt-find-ballots-stop-count-voter-fraud-claims-untrue-politifact/6165435002/>.
- Little, Becky. "How Political Conventions Began—And Changed." History. Accessed February 25, 2021. <https://www.history.com/news/political-conventions-change>.
- McCarthy, Justin. "Four in Five Americans Support Voter ID Laws, Early Voting." Gallup, August 22, 2016. <https://news.gallup.com/poll/194741/four-five-americans-support-voter-laws-early-voting.aspx>.
- McCausland, Phil. "Postal Service Says It Delivered Ballots on Time amid Concern over Untracked Votes." NBC News, November 4, 2020. <https://www.nbcnews.com/politics/2020-election/postal-service-says-it-delivered-ballots-time-amid-concern-over-n1246451>.
- Meadows, Donella H. *Thinking in Systems: A Primer*. White River Junction, VT: Chelsea Green Publishing, 2008.
- Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: Department of Justice, 2019. <https://www.justice.gov/storage/report.pdf>.
- Nakashima, Ellen, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg. "U.S. Government Concludes Iran Was behind Threatening Emails Sent to Democrats." *Washington Post*, October 20, 2020. <https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/>.
- National Conference of State Legislatures. "After the Voting Ends: The Steps to Complete an Election." October 28, 2020. <https://www.ncsl.org/research/elections-and-campaigns/after-the-voting-ends-the-steps-to-complete-an-election.aspx>.
- . "Election Security: State Policies." August 2, 2019. <https://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx>.

- . “Post-Election Audits.” October 25, 2019. <https://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx>.
- . “The Electoral College.” Accessed February 25, 2021. <https://www.ncsl.org/research/elections-and-campaigns/the-electoral-college.aspx>.
- . “VOPP: Table 14: How States Verify Voted Absentee Ballots.” April 17, 2020.
- . “VOPP: Table 18: States with All-Mail Elections.” April 21, 2020. <https://www.ncsl.org/research/elections-and-campaigns/vopp-table-18-states-with-all-mail-elections.aspx>.
- National Police Foundation. *How to Conduct an After Action Review*. Washington, DC: Office of Community Oriented Policing Services, 2020. <https://cops.usdoj.gov/RIC/Publications/cops-w0878-pub.pdf>.
- National Protection and Programs Directorate. “NPPD at a Glance.” February 13, 2018. <https://www.cisa.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf>.
- Norden, Lawrence, Gowri Ramachandran, and Christopher Detuzio. “A Framework for Election Vendor Oversight.” Brennan Center for Justice, November 12, 2019. <https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight>.
- Norris, Pippa. *Why American Elections Are Flawed (and How to Fix Them)*. New York: Cornell University Press, 2017.
- Norris, Pippa, Alessandro Nai, and Max Gromping. “The Electoral Integrity Project EIP.” Harvard Dataverse, December 15, 2016. <https://doi.org/10.7910/DVN/YXUV3W>.
- North Carolina State Board of Elections. “FAQ: Voting by Mail in North Carolina in 2020.” <https://www.ncsbe.gov/voting/vote-mail/faq-voting-mail-north-carolina-2020#how-many-witnesses-do-i-need-for-my-absentee-ballot>.
- Office of Inspector General. *DHS Has Secured the Nation’s Election Systems, but Work Remains to Protect the Infrastructure*. Washington, DC: Department of Homeland Security, 2020. <https://www.oig.dhs.gov/sites/default/files/assets/2020-10/OIG-21-01-Oct20.pdf>.
- . Physical and Environment Controls Site Security View—Summary Report. Arlington, VA: United States Postal Service, 2019.
- . *Progress Made, but Additional Efforts Are Needed to Secure the Election Infrastructure*. Washington, DC: Department of Homeland Security, 2019. <https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf>.

- Office of the Director of National Intelligence. "Statement by NCSC Director William Evanina: Election Threat Update for the American Public." August 7, 2020. <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>.
- Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Defense Science Board Task Force on The Role and Status of DOD Red Teaming Activities*. Washington, DC: Department of Defense, 2003. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a430100.pdf>.
- Ohio Secretary of State. "Absentee Voting." Accessed September 8, 2020. <https://www.ohiosos.gov/elections/voters/absentee-voting/>.
- Palazzolo, Daniel, Vincent G. Moscardelli, Meredith Patrick, and Doug Rubin. "Election Reform after HAVA: Voter Verification in Congress and the States." *Publius: The Journal of Federalism* 38, no. 3 (January 1, 2008): 515–37. <https://doi.org/10.1093/publius/pjn013>.
- Parks, Miles, and Barbara Sprunt. "Louis DeJoy Vows Post Office Can Handle Mail-In Ballots, In Senate Hearing." NPR, August 21, 2020. <https://www.npr.org/2020/08/21/904366258/postmaster-general-faces-senate-as-controversy-persists-over-usps-cuts>.
- Payne, Sarah. "Secretary of State Encourages Michigan Voters to Use Drop Boxes Six Days before Primary Election." *The Michigan Daily*, July 29, 2020. <https://www.michigandaily.com/section/government/secretary-state-encourages-michigan-voters-use-drop-boxes-six-days-primary>.
- Pew Research Center. "Mail-in Voting, Absentee Ballots and Voter Engagement." *Pew Research Center—U.S. Politics & Policy* (blog). October 9, 2020. <https://www.pewresearch.org/politics/2020/10/09/voter-engagement-and-interest-voting-by-mail-and-in-person/>.
- . *Public Expects Gridlock, Deeper Divisions with Changed Political Landscape*. Washington, DC: Pew Research Center, 2018. <https://www.people-press.org/2018/11/15/public-expects-gridlock-deeper-divisions-with-changed-political-landscape/>.
- Polsby, Nelson W., Aaron Wildarsky, Steven E. Schier, and David A. Hopkins. *Presidential Elections: Strategies and Structures of American Politics*. 13th ed. Lanham, MD: Rowan & Littlefield, 2011.
- Rinfret, Sara, Christinia Barsley, and Scott Samuel. "Public Perceptions, Elections, Administration, and the Role of Street Level Bureaucrats." *Public Administration Quarterly* 42, no. 4 (December 2018): 493–515.

- Rosenstein, Rod J. *Appointment of Special Counsel to Investigate Russian Interference with the 2016 Presidential Election and Related Manners*. Washington, DC: Office of the Deputy Attorney General, 2017. <https://www.justice.gov/opa/press-release/file/967231/download>.
- Sandler, Rachel. “Half of Trump’s Twitter and Facebook Posts since Election Day Flagged.” *Forbes*, November 6, 2020. <https://www.forbes.com/sites/rachelsandler/2020/11/04/over-half-of-trumps-twitter-and-facebook-posts-since-election-day-flagged/>.
- Santos, Melissa. “Security and Ballot Drop Boxes: Here’s How It Works in Washington.” Renton, WA Patch, August 30, 2020. <https://patch.com/washington/renton/security-ballot-drop-boxes-heres-how-it-works-washington>.
- Schwartz, Jen. “The Vulnerabilities of Our Voting Machines.” *Scientific American*. Accessed September 16, 2020. <https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/>.
- Secret Service. “The Protective Mission.” Accessed July 3, 2020. <https://www.secretservice.gov/protection/#who>.
- Segan, Sascha. “Internet Sites Try to Sell Votes.” ABC News, January 6, 2006. <https://abcnews.go.com/Politics/story?id=123069&page=1>.
- Shackelford, Scott, Bruce Schneier, Michael Sulmeyer, Anne Boulstead, Ben Buchanan, Amanda N. Craig Deckard, Trey Herr, and Jessica Malekos Smith. “Making Democracy Harder to Hack.” *University of Michigan Journal of Law Reform* 50 (2017): 629–68.
- Sperling, Bert. “DeKalb County, Georgia Politics & Voting.” Accessed February 25, 2021. <https://www.bestplaces.net/voting/county/georgia/dekalb>.
- Spolaore, Enrico, and Phillip Garner. “Why Chads? Determinants of Voting Equipment Use in the United States.” *Public Choice* 123 (February 1, 2005): 363–92. <https://doi.org/10.1007/s11127-005-7167-0>.
- Sprunt, Barbara. “Here Are the Republicans Who Objected to the Electoral College Count.” NPR. Accessed February 25, 2021. <https://www.npr.org/sections/insurrection-at-the-capitol/2021/01/07/954380156/here-are-the-republicans-who-objected-to-the-electoral-college-count>.
- . “Post Office Chief Suspends Controversial Changes until after Election.” NPR, August 18, 2020. <https://www.npr.org/2020/08/18/903477948/postmaster-general-will-testify-at-senate-hearing-friday>.

- Sprunt, Barbara, and Alana Wise. “Trump Opposes Postal Service Funding but Says He’d Sign Bill Including It.” NPR, August 13, 2020. <https://www.npr.org/2020/08/13/902109991/trump-admits-to-opposing-funding-for-postal-service-to-block-more-voting-by-mail>.
- Stark, Philip B. *An Introduction to Risk-Limiting Audits and Evidence-Based Elections*. Berkeley, CA: University of California, Berkeley, 2018. <https://www.stat.berkeley.edu/~stark/Preprints/lhc18.pdf>.
- Steinbicker, Paul G. “Absentee Voting in the United States.” *The American Political Science Review* 32, no. 5 (1938): 898–907. <https://doi.org/10.2307/1948225>.
- Stillwell, Blake. “How Absentee Voting for U.S. Troops Won the Civil War and Ended Slavery.” Military.Com Network, 2020. <https://www.military.com/military-life/how-absentee-voting-us-troops-won-civil-war-and-ended-slavery.html>.
- Tokaji, Daniel P. “The New Vote Denial: Where Election Reform Meets the Voting Rights.” *South Carolina Law Review* 57, no. 4 (Summer 2006): 689–734.
- Troy, Tevi. “The Evolution of Party Conventions.” Summer 2016. <https://www.nationalaffairs.com/publications/detail/the-evolution-of-party-conventions>.
- U.S. Congress. Senate. *Facebook, Social Media Privacy, and the Use and Abuse of Data*. Congressional Hearing. 115th Cong., 2nd sess., April 10, 2018.
- . *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views (Redacted)*. 116th Cong., 1st sess., July 25, 2019. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.
- U.S. Election Assistance Committee. *Election Management Guidelines*. Washington, DC: U.S. Election Assistance Committee, n.d.
- . “Help America Vote Act.” Accessed May 13, 2020. https://www.eac.gov/about_the_eac/help_america_vote_act.aspx.
- United States Attorney’s Office District of New Jersey. “Postal Employee Arrested for Dumping Mail, Including Election Ballots Sent to West Orange Residents.” October 7, 2020. <https://www.justice.gov/usao-nj/pr/postal-employee-arrested-dumping-mail-including-election-ballots-sent-west-orange>.

- University of Foreign Military and Cultural Studies, U.S. Army Training and Doctrine Command, U.S. Army Training and Doctrine Command, and University of Foreign Military and Cultural Studies. *The Red Team Handbook*. v. 9. Fort Leavenworth, KS: University of Foreign Military and Cultural Studies, 2018. https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf.
- Vasilogambos, Matt. “Provisional Ballots Protect Voting Rights—When They Are Counted.” PEW, November 16, 2018. <https://pew.org/2B8JRC6>.
- . “States Begin Prep for Mail-In Voting in Presidential Election.” PEW, March 23, 2020. <https://pew.org/3a97s4G>.
- Weiner, Jay. *This Is Not Florida: How Al Franken Won the Minnesota Senate Race*. Minneapolis: University of Minnesota Press, 2010.
- West, Darrell M. “How Does Vote-by-Mail Work and Does It Increase Election Fraud?.” *Brookings* (blog). June 22, 2020. <https://www.brookings.edu/policy2020/votervital/how-does-vote-by-mail-work-and-does-it-increase-election-fraud/>.
- Williams, Katie Bo. “DHS Designates Election Systems as ‘Critical Infrastructure.’” *The Hill*, January 6, 2017. <https://thehill.com/policy/national-security/313132-dhs-designates-election-systems-as-critical-infrastructure>.
- Winder, Davey. “81.5M Voter Records for Sale on Dark Web Ahead of Midterm Elections.” *Forbes*, October 30, 2018. <https://www.forbes.com/sites/daveywinder/2018/10/30/81-5m-voter-records-for-sale-on-dark-web-ahead-of-midterm-elections/>.
- Yasinsac, Alec, and Matt Bishop. “The Dynamics of Counting and Recounting Votes.” *IEEE Security & Privacy* 6, no. 3 (2008): 22–29. <https://doi.org/10.1109/MSP.2008.75>.
- Young-Jin, Kim, and Kaitlin Becker. “Boston Man Arrested in Connection with Ballot Box Fire in Copley Square.” *NBC Boston* (blog). October 26, 2020. <https://www.nbcboston.com/news/local/a-ballot-drop-box-in-boston-was-set-on-fire-heres-what-we-know/2218418/>.
- Zenko, Micah. *Red Team: How to Succeed By Thinking Like the Enemy*. New York: Basic Books, 2015.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California