



EMEFA ADDO AGAWU

HOW TO THINK ABOUT ELECTION CYBERSECURITY

A Guide for Policymakers

APRIL 2018

About the Author



Emefa Addo Agawu is a former program associate with New America's Cybersecurity Initiative, where she led the initiative's work on cybersecurity at the state & local level. Previously, Emeфа

worked for Professor Jacob Shapiro on the Empirical Studies of Conflict (ESOC) Project at Princeton University's Woodrow Wilson School of Public and International Affairs, where her research focused primarily on the role of information in asymmetric conflict.

Acknowledgments

I gratefully acknowledge comments from David Forscey, Joshua Geltzer, Dipayan Ghosh, J. Alex Halderman, David Mussington, Brian Nussbaum, Allison Stanger, Maurice Turner, Ian Wallace, and David Weinstein. All errors are my own.

About New America

New America is a nonprofit, nonpartisan public policy institute dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

Find out more at newamerica.org/our-story.

About the C2B Partnership

The Florida International University - New America Cybersecurity Capacity Building Partnership (C2B Partnership) brings two cutting edge institutions together to address one of the biggest issues of our day: cybersecurity.

Cyber insecurity is not an issue that will suddenly be fixed by a "silver bullet" technical or policy solution. Even as the risk inherent in connectivity increases, so too does global reliance on network technology for everything from sharing cat memes to conducting interstate commerce to organizing history-altering protests. Only those individuals, companies, organizations, and countries that can build the capacity to thrive in such an environment will thrive. In short, we see cybersecurity capacity building—in state and local governments in the U.S., at the federal policy-making level, in industry, and with the workforce broadly—as one of the most pressing challenges facing the world now and into the future.

Cybersecurity capacity building is the process of developing expertise, skills, tools, and policies needed to help people, organizations, and entire nations face and manage the risk inherent in the increasing connectivity of society. At the FIU-New America C2B Partnership, we are pursuing four major pillars of cybersecurity capacity building work: building workforce capacity, building capacity at the state and local level, international capacity building, and building the capacity of policymakers to understand the complexity and nuance of cybersecurity policy issues.

Find out more at newamerica.org/cybersecurity-initiative/c2b.

Contents

Introduction	2
Chapter 1: Context: A Brief History of Voting Reforms	3
Chapter 2: The 2016 Election and the Response	6
Manipulating Voters	7
Manipulating Votes	8
Causing Disruption	12
Chapter 3: Looking Ahead: Understanding Future Challenges	14
Funding the Future of Voting Reform	15
Increasing Public Faith in Elections	16
Evolving Voter Technologies	16
Chapter 4: Looking Ahead: Identifying Appropriate Responses	19
Expanding and Communicating about Existing Safeguards	19
Creating New Mechanisms or Systems to Provide Confidence	20
Conclusion	21
Notes	22

INTRODUCTION

The drama of modern American elections boasts a full cast of characters. There are voters, who make up their minds about whom to support in a turbulent information environment; there are political campaigns, which increasingly rely on digital tools alongside traditional methods to operate and persuade voters; and on the frontlines, there are state and local election officials, who have primary responsibility for administering elections in the country's 8,000 voting jurisdictions. Running secure and trusted elections has never been a simple production. After the 2016 election, during which the Russian government launched an unprecedented attack on the United States' democratic institutions, it is even more complicated.

In responding to the weakness exposed in the 2016 election, the United States finds itself having an enormously complex election security discussion. For some, election cybersecurity is a story about Russian influence operations. For others, it tells of the dangers of Big Tech. For others still, it is about the persistent challenges of election administration. In truth, it is all these stories, and more. It is difficult to think of another issue that straddles so many different communities of practice and expertise, that is as likely to shift so rapidly as technological capabilities evolve, and that is so central to our democratic process. These realities present at least two challenges to productive conversations.

First, because election cybersecurity means radically different things to different communities even as they engage overlapping material, what is often missing is a clear understanding of which piece of the debate is being considered, as well as an articulation of where that piece fits in the larger story of election cybersecurity.

Second, in addition to the urgent, short-term steps that need to be taken to improve our election cybersecurity before the 2018 midterm and 2020 presidential elections, more questions loom on the horizon. While it is difficult to create space to consider the medium-term while the short-term is so urgent, the seriousness of the questions on the horizon demands that we do so.

This report is a response to those two challenges. Rather than repeat analysis that the election security emergency has already inspired, we aim to provide a guide to understanding that body of work and the implications for the future. The report offers a brief history of voting reforms to place this conversation in a broader context. Then, it breaks down the threat of election hacking into three separate threats: manipulating voters, manipulating votes, and causing disruption. These distinctions offer a conceptual framework through which to understand the current state of response to the 2016 election. Finally, the report looks forward to consider key questions looming just beyond the current debate, and the factors to consider in responding to them.

CHAPTER 1

CONTEXT: A BRIEF HISTORY OF VOTING REFORMS

Early Voting in the United States¹

Modern American expectations for elections are radically different from what they once were. Apart from crucial differences in who could cast a ballot, our methods of voting—and accompanying expectations of the security and anonymity of the voting process—have also drastically changed.

Prior to American independence, elections were administered largely at the colonial level, which resulted in great procedural variety among the Colonies. Within that variety, one common practice was that of oral voting, or *vive voce*. With this method, voters verbally declared support for a candidate—who was often present—in front of the person tallying votes. Unsurprisingly, this practice enabled rampant voter coercion, intimidation, and payoffs from party leaders, landlords, and others with vested interests in election outcomes.

The failings of the *vive voce* method encouraged many states to move towards paper ballots in the late eighteenth and early nineteenth centuries. However, the use of ballots neither guaranteed secrecy nor prevented coercion. In some states, political parties

simply printed and distributed their own ballots, using easily identifiable colors, shapes, or styles, which compromised ballot secrecy.

Widespread coercion and fraud at the ballot box continued throughout the nineteenth century. Pre-stuffed boxes were a popular method of tipping the scale.² To counteract such fraud and encourage (literal) transparency in the voting process, some states introduced glass ballot boxes by the start of the Civil War.³ Nevertheless, voter coercion continued. Political machines, most famously of Chicago and New York City, employed a range of both blunt and sophisticated tactics throughout the nineteenth century—from physical intimidation to patronage and vote-buying—to secure electoral victories, in addition to other forms of electoral corruption.⁴

Concern over voter coercion buoyed support for the secret ballot, which was meant to reduce voter coercion by undermining the coercer's ability to confirm the vote of the would-be coerced. With the secret ballot—also known as the Australian Ballot—uniform ballots are produced and distributed by a government entity, and privately cast by the voter. The secret ballot appeared and spread in the United

States in the late nineteenth century.⁵

Around that time, advancements in mechanization gave rise to new voting technologies, though hand-completed and hand-counted ballots remained popular. Most notable was the mechanical lever machine, which allowed voters to make selections directly on the machine, and could keep a tally of votes throughout the voting process. With no paper ballots to be counted, lever machines reduced the time it took to determine election results, and reduced the number of citizens needed to count ballots.⁶ Lever machines rose in popularity throughout the twentieth century. By the 1964 presidential election, 65 percent of all voters used lever machines, with most other voters using hand-counted paper ballots.⁷

It did not take long for advancements in computing to reach voting, and in the later part of the twentieth century, lever machine use fell as computer-readable ballots rose in popularity. One type of computer-readable ballot was the punched card ballot. With this kind of ballot, votes were recorded by punching holes in cards that were then collected from individual voting machines and sent to central tabulators, where they would be counted rapidly. The Votomatic was the leading punched-card system in the second half of the twentieth century. By 1980, over 29 percent of U.S. voters were using Votomatic-style punched-card ballots.⁸ By 1988, that number was over 40 percent.⁹

Another popular style of computer-readable ballot in the second half of the twentieth century was the optical scan ballot, which functions similarly to the Scantron answer sheets commonly used for standardized testing in the United States. With optical scan voting systems, voters mark their choices directly on a paper ballot, which is then scanned and counted by a computer. Optical scan machines are often contrasted with direct-recording electronic (DRE) machines. DRE machines allowed voters to make selections directly onto a digital touch panel. Some DRE machines produce a paper trail for voters to verify their choice and for election officials to audit, while others do not.

For all the advancements in convenience, accessibility for disabled voters, and cost efficiency that some computer-based ballots in the twentieth century brought, these developments also brought fears of software fraud and technical irregularities. Though voting systems in previous eras certainly confronted technical difficulties, the proprietary nature of the software code used in computer-enabled voting systems fed fears that new voting machines were insecure, because the software code was owned by election technology companies and could not be widely reviewed by independent security researchers for errors or irregularities. In 1988, Roy G. Saltman, a leading expert on election administration and technology, published an extensive report that exposed a number of challenges and vulnerabilities in voting systems.¹⁰ That same year, Ronnie Dugger, drawing in part on Saltman's work, published a long *New Yorker* article on the topic. In it, he made what is, decades later, a familiar point: "Whether or not elections have ever been stolen by computer before, some citizens and some officials are asking if it could happen in the future."¹¹

Recent Voting History

The last major chapter in the history of U.S. voting reforms begins with the 2000 presidential election, which focused the nation's attention on the state of Florida. In a dramatic sequence of events, the narrow vote margin in Florida put the election outcome in the hands of the Supreme Court. In the middle of this political and legal whirlwind, serious voting irregularities in Florida were widely publicized, including so called "hanging-chads"—some ballots were improperly punched and the voters' intent was unclear, which resulted in lost votes. These irregularities caused outrage and highlighted the nation's outdated voting infrastructure, prompting Congress to act. Though a number of bills were quickly introduced to address various elements of the election administration, the Help America Vote Act (HAVA) ultimately passed in October 2002.

HAVA authorized \$3.65 billion in federal funds to help states upgrade their voting equipment and improve

other areas of election administration. It was the first major U.S. federal election legislation to provide federal funds, and the first to mandate requirements for voting equipment since 1899.¹² States largely used this money to purchase new voting machines, prioritizing replacing their oldest machines.

HAVA also created the Election Assistance Commission (EAC), a federal, bipartisan commission that guides states in election administration. While the EAC has no regulatory authority over states, it provides extensive resources and voluntary procedures to support states in everything from acquiring and testing new voting machines to auditing elections.

Along with funding for new voting machines, HAVA prioritized accessibility for disabled voters, especially the visually impaired. The legislation included a provision that required each voting location to offer at least one “direct recording electronic voting system

or other voting system equipped for individuals with disabilities.”¹³ Given the inevitable administrative burden that would arise from having both paper ballots and electronic voting machines at the same location, many states took this HAVA mandate as an incentive to replace paper ballots with electronic voting machines.¹⁴ Some of these electronic voting machines were paperless direct-recording electronic machines that capture votes digitally, but did not produce a paper trail.

While HAVA provided a necessary influx of cash to states to purchase new voting machines, it also set up the current situation, typical of major infrastructure projects: states have electronic voting machines in widespread use, with few or no plans to properly maintain them, and uncertain funding to purchase the next round of technology.

CHAPTER 2

THE 2016 ELECTION AND THE RESPONSE

Whether or not Russia interfered in the 2016 presidential election is no longer a matter for serious debate. The unanimous assessment from the CIA, FBI, and NSA at the start of 2017 was that “Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election.”¹⁵ This judgment is echoed by senior officials throughout the Trump administration, including by former Secretary of State Rex Tillerson, U.S. Ambassador to the United Nations Nikki Haley, and former National Security Advisor H. R. McMaster.^{16,17,18} In February 2018, the intelligence community’s Worldwide Threat Assessment identified the U.S. 2018 midterm elections as a possible target for Russian influence operations.¹⁹

Despite the mixed messages from President Trump, who has both supported and undermined claims of Russian interference,²⁰ Russian interference in 2016 spurred a flurry of reactive activity in many spaces. From government to private industry, academia to civil society, concerned groups and individuals are waking up to the urgency of election security, joining a mix of dedicated election officials, security researchers, and others who have been focused on these matters for years.

Even with this enormous range of activity, much remains undone. However, any oversimplified narrative that “nothing is being done” is simply untrue. It is worth debating whether current efforts will be sufficient, but in order to more clearly understand how far we have to go, we must understand the current state of response.

Election Hacking is Three Separate Threats

The current state of response is best understood as responses to the specific threats that surfaced during the 2016 election. “Election hacking,” “election meddling” or “election interference” is not a monolithic threat, but rather three separate threats: manipulating voters, manipulating votes, and causing disruption.

- To **manipulate voters** is to influence a voter by affecting their information environment.
- To **manipulate votes** is to cause a vote to be recorded in a way that is different from what the voter intended.
- To **cause disruption** is to interfere with

electoral proceedings, which could undermine voter confidence or disrupt the ability to vote.

While election officials and experts are well aware of the distinction between these separate threats, they are often conflated in popular discourse. While this is conflation is unhelpful, it is also understandable; there is compelling evidence that Russian agents attempted to interfere in more than one of these ways. Even more confusing is when the matter of contact between Trump campaign officials and Russian agents is blurred into the discussion. While it is tempting to move seamlessly from one topic to another, using Russia as the connecting link, it is important to consider them separately.

Conflating these separate threats, along with the question of collusion between the Trump campaign and Russian agents, muddies the election security discourse, makes it more difficult to track the state of response, and hinders preparedness efforts for future elections. The “collusion” question can be meaningfully separated from the election hacking discussion here, as none of the three threats named above require collusion to be potent threats. Furthermore, while Russia was the adversary in 2016 and, according to key intelligence figures, is likely to return,²¹ future elections may bring new adversaries with sophisticated cyber operations, such as China or North Korea. In addition to responding to this specific, known adversary, our broader national response must be premised on the societal and systemic vulnerabilities that were exposed, rather than on this specific iteration of the threat.

This section further details each “election-hacking” threat that surfaced in 2016, and briefly overviews the current state of response.

Threat 1. Manipulating Voters

The threat of manipulating voters—altering a voter’s information environment in order to affect their decision-making process—has figured prominently in the sprawling post-election discourse, and for good reason. In January 2017, after months of analysis, the intelligence community released a report, stating:

“Moscow’s influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or ‘trolls.’”²²

Voters make up their minds about whom to support based on a number of factors, and there is evidence to suggest that it is extraordinarily difficult to change peoples’ minds about whom to support.²³ Given the complexity of the individual decision-making process, especially in a changing information environment, it is difficult to determine whether Russian campaigns actually critically influenced voters’ support for specific candidates. However, Russia influence operations have traditionally been about far more than securing votes for a favored candidate.²⁴ In keeping with a classic Russian strategy to sow political and social discord, Russian disinformation campaigns (*dezinformatsiya*) during the 2016 election specifically promoted divisive content,²⁵ focusing on politically sensitive topics like race and LGBTQ rights.”²⁶

Russian attempts to alter voters’ information environment in the 2016 were not limited to social media platforms. They also involved assaults on campaign infrastructure and private individuals, as well as state-run media efforts, a strategy they practiced and honed in Estonia, Ukraine, and elsewhere.^{27,28}

Responses to the Threat of Voter Manipulation

Thus far, the major types of responses fall into the following categories:

- Federal government-led fact-finding
- Efforts to reform social media
- Renewed research into disinformation campaigns and enabling platforms
- Improving voter media literacy
- Fortifying campaign infrastructure

Federal Government-led Fact-Finding

After the 2016 election, questions remained about the reach of foreign-sponsored content that found its way onto social media platforms. Entities within the federal government have undertaken fact-finding efforts, including:

- On February 16, 2018, special counsel Robert Mueller filed an indictment against 13 Russian nationals and three Russian entities. The charges included conspiracy to defraud the United States and aggravated identity theft. The 37-page indictment revealed details of Russia's sustained and organized efforts to "sow discord in the U.S. political system, including the 2016 U.S. presidential election" beginning as far back as 2014.²⁹
- On January 6, 2017, an intelligence community assessment coordinated by the CIA, FBI, and NSA titled Assessing Russian Activities and Intentions Recent U.S. Elections was released. Using information available as of December 29, 2016, the report "covers the motivation and scope of Moscow's intentions regarding U.S. elections and Moscow's use of cyber tools and media campaigns to influence U.S. public opinion."³⁰
- On October 31, 2017, officials from Facebook, Google, and Twitter testified before the Senate Judiciary Subcommittee on Crime & Terrorism at a hearing on Russian disinformation on social media.³¹
- The next day (November 1, 2017) officials from the same companies testified before the House Intelligence Committee. In these testimonies, it was revealed that Russian-linked content reached 126 million users on Facebook, and that Russian agents published 131,000 messages on Twitter and uploaded over 1,000 videos to YouTube.³²

Efforts to Reform Social Media

Efforts are underway to improve transparency about the source of advertisements that appear on social media platforms, both to platforms themselves and for platform users. Notable efforts to reform advertising transparency include:

- On October 19, 2017, Sens. Amy Klobuchar (D-Minn.), Mark Warner (D-Va.), and John McCain (R-Ariz.) introduced the Honest Ads Act, to "improve disclosure requirements for online political advertising."³³
- Companion legislation was introduced in the House of Representatives by Reps Derek Kilmer (D-Wash.) and Mike Coffman (R-Colo.).³⁴
- On October 24, 2017, Twitter announced a series of reforms to increase transparency for ads.³⁵ They included creating Advertising Transparency Center to improve visibility into ads on Twitter and requiring electioneering advertisers to identify as such.^{36,37} (As of this writing, the promised Advertising Transparency Center has not been created.)
- In January of 2018, Facebook announced major revisions to its news feed. The changes were meant to prioritize more meaningful interactions, which means "showing more posts from friends and family [and] less public content, including videos and other posts from publishers or businesses."³⁸ Another, related effort is to help ensure that news on the platform is from trusted sources.^{39,40}

Renewed Research into Disinformation Campaigns and Enabling Platforms

Widespread awareness about disinformation has renewed research into the nature of modern disinformation campaigns, with explanatory and tracking functions. Notable efforts include:

- The Hamilton 68 dashboard, hosted by the Alliance for Securing Democracy at the

German Marshall Fund tracks Russian-backed propaganda on Twitter.⁴¹⁴²

- The Computational Propaganda Project, based at the Oxford Internet Institute brings academic tools and approaches to studying and tracking “junk news.”
- Researchers from New America and Harvard’s Shorenstein Center published a paper, Digital Deceit: The Technologies Behind Precision Propaganda on the Internet which analyzed the “technologies of digital advertising and marketing in order to deepen our understanding of precision propaganda.”⁴³
- The European Commission created a High Level Expert Group on Fake News and Online Disinformation, which released a report on strategies to counter disinformation.⁴⁴

Improving Voter Media Literacy

While it still unclear precisely how false information affects voters, efforts are underway to try to make the public more resilient to false information. (As susceptibility to false information is of concern for many elements of modern citizenry, these efforts are not restricted to the election space.)

- Many organizations are developing workshops, tools, curricula, and messaging, including the National Association for Media Literacy Education, Common Sense Media, and the Center for News Literacy, to name a few.
- Efforts are underway to involve state and local governments in combating false information. These include legislation in Connecticut to establish an advisory council on the topic, and legislation in Rhode Island asking state education officials to work with media literacy organizations.⁴⁵

Fortifying Campaign Infrastructure

The compromise of campaign infrastructure—specifically the Democratic National Committee and individuals connected to the Clinton campaign—raised the prospect that hacking and strategically releasing campaign and private communications may become a routine part of elections in the digital age. Though it was Hillary Clinton’s campaign that was the target of these efforts in the 2016 election, this activity raised bipartisan alarm, leading many groups to improve the cybersecurity defenses of political campaigns. These efforts include:

- The Defending Digital Democracy Project based at Harvard University’s Belfer Center produced the Cybersecurity Campaign Playbook with key steps for campaigns to mitigate their cybersecurity risk.⁴⁶
- In July of 2017, Facebook pledged \$500,000 the Defending Digital Democracy Project at Harvard University’s Belfer Center for Science, which to build a standalone Information Sharing and Analysis Organization (ISAO) for campaigns to exchange timely threat information.⁴⁷
- In October of 2017, Google announced it would offer its Advanced Protection program for high-profile accounts, providing stronger defenses against phishing attacks and other account compromise tactics. Google’s announcement specifically names campaign staffers as an example of those who are at particularly high risk of online attack.⁴⁸

Counteracting the threat of voter manipulation is particularly challenging for (at least) three reasons:

First, the wider political climate created strong disincentives for Republican members of Congress to seriously pursue the matter of Russian influence operations, because the popular discourse often conflated Russian influence operations with the charge of collusion between the Trump presidential campaign and Russia. Many Republican members of Congress concluded that acknowledging Russian

influence on one front would hand a weapon to their political opponents, who could use the focus on Russia to score political points or undermine President Trump's election. These political elements are a further obstacle to an effective and efficient response.

Second, although there is bipartisan agreement on the need to deter future Russian interference by imposing costs on Russia for its actions during the 2016 election, deterrence efforts have been weakened by President Trump, who has intermittently cast doubt on the intelligence community's conclusion that Russia interfered in the election.

Third, no single entity can comprehensively manage the entire response to the voter manipulation threat. The federal government may be best-placed to enact punitive measures to deter future Russian interference; social media companies like Facebook and Twitter play an outsized role in shaping the information environment in which elections occur; different entities altogether—librarians, school teachers, parents—may be best placed to build the long-term media literacy that will enable longer-term resilience to influence operations.

Threat 2. Manipulating Votes

The threat of manipulating votes is the threat of a vote being corrupted after being cast by a voter—essentially, that a voting machine (or vote-tallying infrastructure) will be hacked. While the Department of Homeland Security found no evidence that malicious actors successfully compromised any vote-tallying machines in 2016, reports of several incidents involving Russian hackers and voting systems caused alarm. Among these were reports that Russian actors scanned state election systems in at least 21 states (roughly the digital equivalent of circling a house to look for unsecured points of entry), successfully penetrated the voter registration systems in two states, and targeted a voting equipment vendor that communicates regularly with election officials and systems.⁴⁹

While some of the alarm these reports caused was overblown, and the reports do not support a claim that Russians even came close to successfully changing election outcomes, it is a sobering reality that these activities—poking around in voting systems—are also the markers of a hacker looking to further penetrate a system.

There is a fierce and complex debate over the possibility and probability of voting systems being compromised. It will not be possible to reproduce the debate in its entirety here. Those who are most concerned emphasize the vulnerabilities in our voting systems. They are supported by the work of security researchers who have, over the years, repeatedly compromised voting machines that are used in real elections.⁵⁰ There is disagreement over how easy it would be, under the conditions of a live election, to exploit the vulnerabilities that security researchers have uncovered, and, if so, whether it could occur on a scale big enough to affect a state or national level election outcome. But, the possibility, however remote, that voting machines could be hacked demands that we adopt measures that would make it difficult to compromise a voting machine without detection.

Responses to the Threat of Vote Manipulation

Thus far, the main types of responses have been to:

- Ensure that votes are cast with a paper trail
- Enhance and expand audit procedures
- Improve the cybersecurity of the broader voting ecosystem

Ensure That All Votes Are Cast With a Paper Trail

According to Verified Voting, as of this writing, five states exclusively use voting machines that do not produce a voter-verified paper audit trail: Delaware, New Jersey, South Carolina, Georgia, and Louisiana.⁵¹ Machines that do not produce a voter-verified paper audit trail are currently in

use—though not exclusively—in another nine states: Kansas, Arkansas, Mississippi, Texas, Florida, Kentucky, Tennessee, Indiana, and Pennsylvania.⁵² Many legislative efforts are underway to implement paper trails, both at the federal and state level. Success is often contingent on sustained attention and funding. They include:

Federal Efforts

- The Secure Elections Act, introduced in December 2017, and revised in March of 2018.^{53,54}
- Election Security Act, introduced in the House in February 2018.⁵⁵
- S.A. 656 Klobuchar-Graham amendment to the National Defense Authorization Act of 2017, introduced in July 2017.⁵⁶
- PAPER Act, introduced in the House in September 2017.⁵⁷
- SAVE Act introduced in the Senate October 2017.⁵⁸

State Efforts

- Virginia’s State Board of Elections decertified its paperless electronic machines ahead of its November 7, 2017 election.⁵⁹
- In February of 2018, Pennsylvania Governor Tom Wolf ordered counties that plan to replace their voting machines to do so with machines that produce a paper trail.⁶⁰
- In February of 2018, Kentucky’s State Board of Elections moved to require all future election equipment purchased in the state to provide a voter-verified paper trail.⁶¹

Enhance and Expand Audit Procedures

In addition to ensuring a paper record for every vote cast, it is also important to have procedures to regularly confirm that the digital vote tally and

the paper tally match. There are many types of audits, and not all are created equal. One rigorous method is the risk-limiting audit, which compares a statistically significant portion of the digital tally to the requisite number of paper ballots to provide high confidence that the tallies match. While some states do conduct risk-limiting audits (New Mexico, Colorado, and soon Rhode Island) many states conduct less-rigorous post-election audits, or do not run them at all. All of the federal legislation described above includes provisions on post-election audits. The most effective audit approach is to conduct them after every election—not only closely-contested races—in order to validate confidence in the election systems, but also to act as a deterrent against tampering attempts. In addition to audits that confirm the digital vote tally, procedural audits focus on things like chain of custody of ballot, and other audits focus on the technical infrastructure used in the voting process.⁶²

Improve the Cybersecurity of the Broader Voting Ecosystem

Integrating computerized systems into the voting process—from voting machines, to voter registration system, to election-night reporting systems— inherently introduces cybersecurity risk into the system. Efforts to improve the cybersecurity of the broader ecosystem include:

- The Election Assistance Commission (EAC) is a clearinghouse of information for election officials around the country. They provide resources to election officials on a number of election administration issues, including resources on cybersecurity hygiene and securing voter registration databases.⁶³
- The Department of Homeland Security is vetting state election systems, conducting free threat assessments. These voluntary risk and vulnerability assessments are meant to identify opportunities for states to improve their practices. As of January 2018, three states had been vetted, and 11 more were scheduled.)^{64,65}

- The National Institute of Standards and Technology (NIST) works closely with the Election Assistance Commission (EAC) on a number of aspects of technical voting technical standards.
- The Center for Internet Security (CIS) gathered a broad group of stakeholders to produce a Handbook for Elections Infrastructure Security that takes a best practices approach to election security.⁶⁶
- The Defending Digital Democracy Project (D3P) at Harvard's Belfer Center for Science and International Affairs released a State and Local Election Cybersecurity Playbook, with best practices and technical cybersecurity recommendations in a number of areas of election administration.⁶⁷

In a major contribution to our understanding of state readiness for the 2018 midterm elections, the Center for American Progress conducted a comprehensive 50-state report mostly focusing on mitigating the threat of vote manipulation grading states on several factors, including voter-verified paper ballots and post-election audits.⁶⁸ Their work makes clear that states still have a long way to go to prepare for this threat, and that the capabilities of states vary greatly.

Threat 3. Disruption

The threat of cyber disruption is riddled with unknowns, which makes preparation difficult. A disruptive cyberattack could take a number of forms. An acute disruption could cause chaos on Election Day, where a diffuse disruption could mean smaller disruptive efforts in the period leading up to an election. The former could focus on obstructing voting at a particular polling location, or distributed denial of service (DDoS) attacks on key voter information or news sites, while the latter might slowly wear away at public confidence in electoral processes or outcomes. While it will not be possible (or practical) to capture every disruptive scenario, here are a few key targets:⁶⁹

- E-pollbooks, the digital logs used on Election Day to confirm voters' identities,⁷⁰ are a possible target for disruption. Theoretically, voter logs could be tampered with by deleting or making registered voters' names unrecognizable, which could cause confusion, impactful delays, or disenfranchisement on Election Day. These systems were among those compromised by hackers at DEFCON's summer exhibit.⁷¹
- News media entities that communicate election results are another target for disruption. These entities increase their attackable surface area when they communicate through platforms like Twitter and Facebook.⁷²
- State-run election-related websites that perform functions like providing information about polling locations are vulnerable to cyberattack. A DDoS attack, in which servers are purposefully overwhelmed by traffic, can make a site inaccessible for the duration of the attack. Another concern is ransomware, which could encrypt and make unavailable data that is fundamental to the election process.

The threat model for causing disruption has several features that make it especially challenging to confront, including:

- multiple vulnerable assets
- uncertainty about how vulnerable these assets are
- variability between locations in what is vulnerable
- decentralized control over the various vulnerable assets, and
- prohibitively high costs to securing every potential vulnerable point.

Much like for the threat of manipulating votes, detecting actors scanning voting systems could be a sign they are gauging the possibility of disruptive

efforts. In addition to technical systems, also vulnerable are the non-IT processes that support precinct and state-election board reporting and certification processes.

Responses to the Threat of Disruption

Thus far, the major types of responses fall into the following categories:

- Protecting election-related websites
- Improve the cybersecurity of the broader voting ecosystem
- Improving voter media literacy
- Improving flow of information about threats

Protecting Election-Related Websites

Though it is unclear just how disruptive it would be for an election-related website to go down, the rise of botnet-for-hire services, powerful Internet of Things (IoT) botnets like Mirai, and other innovations make it increasingly easy for hackers to target these sites with DDoS attacks. There are initiatives underway to help make such websites resilient to this and other attacks. Some efforts to protect election-related websites include:

- In December of 2017, Cloudflare launched the Athenian Project. This initiative provides free protection for state, county, and municipal election websites.⁷³
- “Protect Your Election” is a set of tools made available by Jigsaw, a Google subsidiary. The free tools are available to “publishers, journalists, NGOs, and election monitoring sites” and specifically include anti-DDoS protection.⁷⁴

Improving the Cybersecurity of the Broader Voting Ecosystem

As noted earlier, modern voting processes involve computers at many stages—from registering to vote to reporting election results. As a result, some best practices from other areas will also be relevant to election systems. Discovering those best practices and standards, and communicating them with state and local election officials in a way that is sensitive to the particularities of election systems is a major effort. Just as those efforts are a response to the threat of vote manipulation, they are also a response to the threat of disruption. To repeat, key efforts include:

- The Election Assistance Commission (EAC) is a clearinghouse of information for election officials around the country. They provide resources to election officials on a number of election administration issues, including resources on cybersecurity hygiene and securing voter registration databases.⁷⁵
- The Department of Homeland Security is vetting state election systems, conducting free threat assessments. These voluntary risk and vulnerability assessments are meant to identify opportunities for states to improve their practices.⁷⁶ As of January 2018, 3 states had been completed, and 11 more were scheduled.)⁷⁷
- The National Institute of Standards and Technology (NIST) works closely with the Election Assistance Commission (EAC) on a number of aspects of technical voting technical standards.
- The Center for Internet Security (CIS) gathered a broad group of stakeholders to produce a Handbook for Elections Infrastructure Security that takes a best practices approach to election security.⁷⁸
- The Defending Digital Democracy Project (D3P) at Harvard’s Belfer Center for Science and International Affairs released a State and

Local Election Cybersecurity Playbook, with best practices, and technical cybersecurity recommendations in a number of areas of election administration.⁷⁹

Improving Voter Media Literacy

Efforts at acute disruption could come in the form of disinformation. (Imagine a false news story spreading on election night that prematurely named a winner, or falsely reported major disruptions.) To combat acute disruption in the form of disinformation, all the media literacy efforts described above to help individuals discern false stories apply here as well. To repeat, those efforts are:

- Organizations developing workshops, tools, curricula, and messaging. Such organizations include the National Association for Media Literacy Education, Common Sense Media, and Center for News Literacy, to name a few.
- State-level efforts to involve state and local governments in the challenge of combating false information, including Governor Dannel Malloy's (D-Conn.) bill to establish an advisory council on the matter, and Rhode Island bill asking state education officials to work with media literacy organizations.⁸⁰

Improving Flow of Information About Acute Threats

Election security is a national security issue. As in other areas of national security and cybersecurity, timely information-sharing about the specific threats is critical for preparedness and response. The sheer number of election officials and the variation among states in election administration make timely information-sharing a challenge. One challenge is getting actionable technical data (like indicators of compromise) to technical election security staff in time to respond to an attack.

- Before the 2016 election, many state election officials lacked the security clearances that

would allow them to receive classified briefings. The Department of Homeland Security is working to secure clearances for the top election officials in every state. As of March 2018, Homeland Security Secretary Kirstjen Nielsen about 20 of the 150 state election officials had received security clearances to obtain election security intel.⁸¹

- This designation of election system systems as critical infrastructure meant the creation of a Sector Coordinating Council (SCC), and a Government Coordinating Council (GCC). The SCC is an industry-led body that coordinates with DHS and the EAC that is meant to enable critical infrastructure owners and operators to share information. The GCC is the public-sector counterpart through which the Department of Homeland Security (DHS) the EAC, and other relevant entities—including the National Association of Secretaries of State (NASS)—coordinate.
- The Multi-State Information Sharing and Analysis Center (MS-ISAC) monitors state networks for suspicious activity and shares cyber threat intelligence its state and local partners.

Recognizing the critical role of public communications in the case of a cyber incident, the Defending Digital Democracy Project at Harvard's Belfer Center developed two communications guides; one to communicate in the case of a cyber incident, the other in the case of a non-cyber incident.⁸² Going forward, resources like this are especially valuable. Elections face all sorts of non-cyber, small-scale disruptions every year. Building resilience to cyber disruptions is critical, because cyber disruptions may simply be a feature of holding elections in the digital age.

CHAPTER 3

LOOKING AHEAD: UNDERSTANDING FUTURE CHALLENGES

The wide range of responsive activity outlined in the previous section makes it clear that modern elections sit at the intersection of a number of fields: national security, election administration, state and local politics, cybersecurity policy, and many more. This positioning creates opportunities for different sectors to contribute their best energies and expertise. The sprawling nature of this challenge also makes it difficult to organize a coordinated, comprehensive response. With enough sustained attention, key improvements are still possible ahead of the fast-approaching 2018 midterm elections and the 2020 presidential elections.

However, beyond the pressing steps to prepare for the very near-term, we must also make space to consider major questions looming in the medium-term that will impact the future of secure and trusted elections. A satisfactory response would address the most pressing vulnerabilities, but a more complete response would be to prepare for the medium-term while addressing the near-term.

Looking beyond 2020, there are at least three questions we would do well to begin to consider. First, how should we fund the future of voting

reform? Second, how do we maintain public faith in elections? And third, how should we respond to new voting technology?

Challenge 1: Funding the Future of Voting Reform

Of all the efforts discussed in the first chapter, there is broad consensus that two straightforward steps would go a long way towards improving confidence in our election systems in the near-term: first, to replace all voting machines in use that do not produce a voter-verified paper audit trail; and second, to implement mandatory audits that offer a high degree of confidence that the digital tally is correct.⁸³ These are not costly reforms. An estimate from the Brennan Center for Justice places the cost of replacing all paperless machines between \$130 million and \$400 million.⁸⁴ Leading election security expert Dr. Alex Halderman estimates that implementing risk-limiting audits for federal elections would cost under \$20 million.⁸⁵

In late March 2018, Congress passed a spending bill that included \$380 million for election

cybersecurity. While this is approximately the total amount needed to replace voting machines that currently do not produce a voter-verified paper trail, analysis from Verified Voting and the Brennan Center for Justice shows that for 11 of the 13 states using paperless voting machines, funds they are likely to receive will be insufficient to completely replace their paperless machines.⁸⁶

However, the challenge extends beyond these short-term measures. Today's broader voting equipment is in a worrying state. As an extensive report from the Brennan Center for Justice details, 42 states are still using machines purchased over a decade ago, dangerously near the end of their projected lifespans.⁸⁷ As they approach the end of their lifespans, voting machines malfunction more often, which cause nuisance and delay. Older machines can also have their security flaws exposed, which could mean increased vulnerability to hacking. Election officials struggling to maintain outdated machines are sometimes forced to resort to public auctions to purchase replacement parts for machines that are no longer sold or maintained by manufacturers, who may no longer even be in business. An enduring challenge of voting reform in the United States is that no level of government considers it their primary responsibility to pay for voting equipment reform, and funding voting infrastructure will always compete with other budget priorities. Who will pay for the next major round of voting equipment: the federal government, or individual states?

The table on the next page previews the implications of major funding for voting reforms being federal or state-led.

Challenge 2: Increasing Public Faith in Elections

Maintaining electoral integrity depends on more than technical competence. It also rests upon public faith in elections. Public faith—which reflects perception of system integrity, rather than a system's actual or likely integrity—is notoriously

complicated to measure.⁸⁸ Voter confidence is influenced by many factors. The public can have faith in an insecure voting system, and the public can lack faith in a secure voting system. Evidence suggests that voters are significantly more likely to believe that votes were improperly counted when their preferred candidate loses.⁸⁹ Other data show that voter confidence in the United States is linked to how competent voters perceive poll workers to be.⁹⁰

While electoral fraud is as old as elections themselves, the cybersecurity of elections conducted in the digital age presents a new piece of the voter confidence puzzle. In the 2016 election, according to polling from the Cooperative Congressional Election Study, 59 percent of respondents believed that the election was fairly determined.⁹¹ Many voters were “very” or “somewhat” concerned about irregularities affecting the outcome, including 39 percent of voters concerned that an electronic security breach impacted the vote counts.⁹² The same poll showed that voters were similarly worried that a “candidate or party changed the election results to create false or inaccurate vote counts” (38 percent) and even more worried about voter fraud (45 percent).⁹³

To complicate matters, assumptions about what digital security looks like are shaped outside of the voting experience, as most Americans use digital technology in their daily lives, but interact with election technology very infrequently.⁹⁴ As a result, voters may import expectation of what strong digital security looks like from a commercial environment into the voting environment, where the same mechanisms may be unavailable or infeasible.⁹⁵ Being unable to offer a security assurance in the form an individual prefers or expects is different from being unable to secure a system.

Challenge 3: Evolving Voting Technology

Though advancements in voting technologies will certainly have cybersecurity implications,

they are often not motivated purely by cybersecurity concerns. This report has focused on the cybersecurity aspect of elections, but a number of other pressing issues plague election administrators. Election officials and others with interests in election processes have many goals, including increasing voting turnout, minimizing costs, cutting down on wait times, and improving the overall voting experience.

The 2016 election foregrounded cybersecurity concerns in the election discourse, which provoked conflicting reactions to the prospect of exploring new voting technologies. For some, the vulnerabilities that were surfaced in the election were a clear mandate to completely reimagine what the future of secure voting could look like. Many feel that our election infrastructure—so critical to our democracy—should use the best and most secure technology currently available, and that the time is ripe to experiment with and pilot new systems. For others, the urgent lesson from the 2016 election was to move as swiftly as possible to secure our existing infrastructure, which often means expanding paper-based voting systems. For this camp, recognizing that time is short and political attention hard to sustain, conversations about new voting technologies could be distracting and ill-advised.

Internet Voting: Challenge, Opportunity, or Both?

While a full exploration of the various innovations in voting technology and their implications is beyond the scope of this paper, one theme that animates many voting innovations is the idea being able to vote remotely. To some, this is internet

voting. A 2011 report from the Election Assistance Commission clarifies internet voting as, “any system where the voter’s ballot selections are transmitted over the internet from a location other than a polling place to the entity conducting the election.”⁹⁶ This can happen in a controlled environment (on a platform supplied by the administering entity) or an uncontrolled environment (the equipment is supplied by the voter, or any other computer).

Internet voting advocates may be motivated by different reasons. Being able to securely return a ballot remotely could solve multiple problems. For example, depending on implementation, internet voting could reduce resources needed to run in-person polling operations on Election Day, or it could make voting more convenient for a broader population, which could in turn improve turnout.

“Internet voting” is already a reality today. Most of the electronic ballot transmission currently allowed is to accommodate voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), who face challenges in voting from abroad. Today, twenty-one states and the District of Columbia allow some voters to return ballots via email or fax.⁹⁷ Beyond existing practices, many groups are enthusiastic about expanding secure ballot return, including those who champion blockchain’s ability to facilitate secure mobile voting.

	Federal Sources of Funding	State Sources of Funding
Uniformity of Practice	Centrally Established Standards As federal funding to states usually come with strings attached—centrally established standards that states must meet—as well as auditing or reporting requirements, one feature of federally-funded reform could be transparency about the standards to which states are adhering. This could also lead to more uniformity of practice than would otherwise occur. At the same time, centrally established standards and requirements can be onerous for states, especially if they are poorly designed and create unnecessary burdens for states. Alternatively, well-written standards can save states the effort of discovering on their own what the standards should be.	Non-Uniformity States already vary widely in their election procedures. If reform is spearheaded at the local, rather than at the federal level, this is likely to continue. There is some security benefit that comes from non-uniformity. The variety among voting systems means that a potential adversary would need to become familiar with a number of systems in order to execute a successful attack. However, states also vary in their resources. Leaving voting reforms to states may make reforms dependent on a state's financial ability to carry them out. As a result, over time, states with fewer resources or other budgetary challenges may come to have poorer voting infrastructure than do states that are able to prioritize election reform. The security implication of this scenario is that adversaries wanting to influence or cast doubt on elections could direct their efforts towards swing states with the weakest protections
Impact on State Ownership of Elections	States Discouraged From Long-Term Budgeting Voting equipment needs continuous budgetary attention for maintenance and reform. While future innovations may slow down the rate at which equipment needs to be replaced, all hardware will eventually reach the end of its ideal lifespan. The influx of federal funds in 2002 may have suggested to states that major federal funding for voting infrastructure, especially in the wake of an emergency, would arrive. Since HAVA, few states have appropriated substantial funds for voting reform. Another major investment in voting equipment funded at the federal level could discourage state legislatures from embracing the medium- and long-term financial burden of voting equipment maintenance.	Continued State and Local Ownership of Election Administration Considering the proximity of election officials to the populations they serve and the variety in voting behaviors from state to state, state election officials are well-positioned to understand the particular needs and habits of their electorates. Having states be central to reforms may result in reforms best-suited to their constituents. The absence of federal funds may also further incentivize states to build voting maintenance into budgets, which may improve long-term stewardship over voting infrastructure
Risk of Political Tensions	Interference of Federal Partisan Politics Leaving voting reform to Congress makes progress vulnerable to partisan politics. Though HAVA passed with bipartisan support and many of the reform measures currently under consideration have bipartisan support, congressional politics can be unpredictable. The intensity of elections heightens the danger that partisan identities could interfere. From voter fraud to foreign interference, elections are saturated with explosive partisan issues.	Tensions at the State Level Friction between state and local units of government—and between different state branches of government—is also relevant to voting reform. In October of 2017, the Virginia State Election Board decided to decertify a class of voting machines, ordering counties to replace those machines before the 2017 November gubernatorial election. This frustrated many counties, as the decision imposed unexpected costs on some counties that would have to purchase new voting machines on short notice. This dynamic may await other states and localities, if they are left to implement their own voting reforms without federal funding.

CHAPTER 4

LOOKING AHEAD: IDENTIFYING APPROPRIATE RESPONSES

Finding the appropriate response to the challenges facing election security will be key to maintaining the integrity of our system of government. One possible response to new digital threats to voting systems—real or perceived—could be to offer new mechanisms that confirm the integrity of the electoral system. In previous era, glass boxes were introduced in response to the threat of pre-stuffed ballot boxes. What mechanisms could boost voter confidence in the digital age?

Potential Response 1: Expanding and Communicating about Existing Safeguards

As described earlier, the most urgent of the voting reforms—paper trails and post-election audits—could provide high confidence that no vote tampering would go undetected. Beyond implementing these measures, election officials and other public figures could make a directed and concerted effort to broadly communicate about the

specific functions of these backstops, to educate the public about the purpose of paper ballots and post-election audits, which could raise confidence that vote count was not digitally manipulated.

However, this could also heighten the impact of irregularities. Whether or a not a hacker could feasibly tamper with voting machines in a live election is still a matter of dispute. All the same, it is worth considering how the public would respond to an audit that revealed serious discrepancies between the paper and digital tallies. Different states will have their own processes to investigate irregularities, but if the public has come to trust that the paper record will confirm the digital tally and prove that no vote tampering occurred, then any discrepancies that arise could sow public uncertainty. This could be especially damaging if the process of vote reconciliation involved any government actors perceived to be politically motivated.

Potential Response 2: Creating New Mechanisms or Systems to Provide Confidence

The mainstream election security conversation tends to favor expanding paper backstops over incorporating new technology in the short term. However, in some spaces, innovators are asking themselves what would it look like to reimagine secure voting for the twenty-first century? For some, a critical step is to move away from proprietary voting technology and towards open-source election software that can be widely reviewed for flaws. Several jurisdictions are using or are moving towards open-source systems, including New Hampshire, San Francisco, Los Angeles County, and Travis County, Texas.⁹⁸ Proposals like these raise important questions that are worthy of separate debate. But, in addition to questions of feasibility, new mechanisms or systems to boost voter confidence would have other important implications.

First, it could **create evolving expectations for confidence mechanisms**. While new mechanisms or systems meant to raise voter confidence may indeed increase public faith in subsequent elections, creating new mechanisms in response to public demand might also create an expectation for demands to be met in the future. Consider the case of a future public demand for a particular new confidence mechanism. If future election administrators were able to satisfy public demands, it would be an opportunity to repeatedly renew public faith in elections. Alternatively, the public could present demands that outstrip government capabilities, or that impose unrealistic technical or administrative burdens.

Second, it could **create inequality of vote confidence by region**. If new mechanisms are created through any process other than federal action—as seems likely, considering the enormous autonomy of states and localities in election administration—then the uneven proliferation of new confidence mechanisms in one part of the country could affect voter confidence

elsewhere. Voting districts, differently resourced and motivated, could adopt any new confidence mechanisms at their own paces, if at all. If it was believed that one location's confidence mechanism was the gold standard, then this belief could undermine confidence in systems that do not adopt the new mechanism. The result could be inequality between regions in how secure voters perceive their votes to be. For the voting process to retain legitimacy, voters need to have confidence not only that their own votes are counted correctly, but also that results in swing states and district are accurate.

In the wake of the 2016 election, decision makers may be more likely to evaluate new voting technologies primarily through a cybersecurity lens. Advocates of new voting technologies will tend to present the bundle of benefits they believe their innovation offers, which may or may not center cybersecurity. These innovators may be trying to achieve several intermediary goals—providing a more secure voting environment, providing a more user-friendly voting experience—which they believe will in turn fulfill a broader goal, such as increasing overall confidence in the country's voting system. Those who oppose new voting technologies may have similar intermediary goals, and even share overarching goals, but very much disagree on how best to achieve them.

Both sides share at least one common goal—boosting voter confidence—though they may disagree over what is most likely to achieve this goal. This is a complicated matter. Voter confidence can already be difficult to measure, and the factors that make up voter confidence are likely to continue to change as our information environment changes. Regardless of one's stance on whether to experiment with new voting technologies, all sides would benefit from more research in this rapidly shifting area; it is critical to continue to invest in and expand research on how voters form their expectations for election security in the modern age.

CONCLUSION

The long history of U.S. voting is littered with irregularities, malfunctioning technology, contested elections, fraud, coercion, and systematic disenfranchisement.⁹⁹ On top of that turbulent history, the modern era adds a determined nation-state adversary within a changing cyber threat landscape, against the backdrop of an aging physical voting infrastructure. These are stubborn set of facts for the electoral optimist to confront.

However, the pessimist would do well to remember that the long history of voting is also marked by continuous efforts to improve election security, which have resulted in remarkable improvements

over the years. Additionally, though the combination of foreign intervention and digital tools present new challenges, it is worth recalling that electoral irregularities may be the norm, rather than the exception. Our democracy, while fragile on many fronts, has proven resilient to electoral irregularities for centuries.

Whether optimistic or pessimistic, the mandate for the present moment is to sustain the attention and urgency required on this next leg of the long journey towards secure and trusted elections.

Notes

1 This brief history focuses on technological and procedural voting reforms. This period also saw enormous changes in voting access and rights for many populations, and other major electoral reforms. For an expanded history of voting advancements in this period, see Roy G. Saltman's detailed volume, *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence*. (New York: Palgrave Macmillan, 2006).

2 Saltman, *The History and Politics of Voting Technology*, 106.

3 Douglas W. Jones and Barbara Simons. *Broken Ballots: Will Your Vote Count?* (Stanford: CSLI Publications, 2012), Chapter 2, Kindle.

4 "The Board of Aldermen's 1878 report on the Tweed ring scandals estimated that the vote cast in New York City in 1868 was 8 percent in excess of its entire population and that there had been more than 50,000 illegal votes cast." See: Saltman, *The History and Politics of Voting Technology*, 75.

5 Saltman, *The History and Politics of Voting Technology*, 97-102.

6 Ibid., 160.

7 Ibid., 157.

8 Jones and Simons, *Broken Ballots*, Chapter 3.

9 Jones and Simons, *Broken Ballots*, Chapter 5.

10 Roy G. Saltman, *Accuracy, Integrity, and Security in Computerized Vote-Tallying*, National Bureau of Standards, 1988, Pub. (500-158), Washington, DC: Government Printing Office.

11 Ronnie Dugger, "Counting Votes." New Yorker, November, 1988, <https://www.newyorker.com/magazine/1988/11/07/counting-votes>.

12 Saltman, *The History and Politics of Voting Technology*, 3.

13 52 USC 21081: Voting systems standards, 3b.

14 For an expanded discussion of this period, see: Charles Stewart III, "Electoral Vulnerabilities in the United States: Past, Present, and Future," MIT Political Science

Department Research Paper No. 2017-5.

15 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment, January 6, 2017. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

16 Mike DeBonis and Carol Morello, "U.S. 'taking steps' to prevent future Russian election interference, Haley says," *Washington Post*, February 1, 2018, https://www.washingtonpost.com/powerpost/us-taking-steps-to-prevent-future-russian-election-interference-haley-says/2018/02/01/6511d1ee-07aa-11e8-8777-2a059f168dd2_story.html.

17 Carol Morello. "Tillerson has harsh words for Russia's malicious tactics," *Washington Post*, November 28, 2017, https://www.washingtonpost.com/world/national-security/tillerson-has-harsh-words-for-russias-malicious-tactics/2017/11/28/f3136426-d465-11e7-a986-d0a9770d9a3e_story.html.

18 Fiona Maxwell, "McMaster: 'Incontrovertible' evidence of Russian interference in election," *Politico*, February 17, 2018, <https://www.politico.eu/article/h-r-mcmaster-incontrovertible-evidence-of-russian-interference-in-election>.

19 Daniel R. Coats, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Select Committee on Intelligence, U.S. Senate, February 13, 2018. Available at: <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>.

20 Ashley Turner and Tamanna Desai, "Trump has repeatedly cast doubt on Russian interference in US politics - until now," CNBC, February 16, 2018, <https://www.cnbc.com/2018/02/16/trump-has-repeatedly-denied-russian-interference-in-the-us-election-but-not-today.html>.

21 Patricia Zengerle and Doina Chiacu, "U.S. 2018 elections 'under attack' by Russia: U.S. intelligence chief," Reuters, February 13, 2018, <https://www.reuters.com/article/us-usa-security-russia-elections/u-s-2018-elections-under-attack-by-russia-u-s-intelligence-chief-idUSKCN1FX1Z8>.

22 Office of the Director of National Intelligence,

“Assessing Russian Activities and Intentions in Recent US Elections,” Intelligence Community Assessment, January 6, 2017. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

23 Brendan Nyhan, “Fake News and Bots May be Worrisome, but Their Political Power is Overblown,” *New York Times*, February 13, 2018, <https://www.nytimes.com/2018/02/13/upshot/fake-news-and-bots-may-be-worrisome-but-their-political-power-is-overblown.html>.

24 Ashley Deeks, Sabrina McCubbin, and Cody M. Poplin, “Addressing Russian Influence: What Can We Learn from Cold War Counter-Propaganda Efforts?” *Lawfare Blog*, October 25, 2017, <https://www.lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts>.

25 Mike Isaac and Scott Shane, “Facebook’s Russia-Linked Ads Came in Many Disguises,” *New York Times*, October 2, 2017, <https://www.nytimes.com/2017/10/02/technology/facebook-russia-ads-.html>.

26 April Glaser, “Russia’s Election meddling Targeted Activists and People of Color, Too,” *Slate*, November 3, 2017, http://www.slate.com/blogs/future_tense/2017/11/03/russia_s_election_meddling_targeted_activists_and_people_of_color.html.

27 Robert D. Blackwill and Philip H. Gordon, *Containing Russia*, Council on Foreign Relations, Special Report No. 80, January 2018, 6-9.

28 Stephen Blank, “Cyber War and Information War à la Russe,” in *Understanding Cyber Conflict: Fourteen Analogies*, ed. George Perkovich and Ariel E. Levite (Washington DC: Georgetown University Press, 2017), 81-98.

29 United States of America v. Internet Research Agency LLC et al., Criminal no. (18 U.S.C. §§ 2, 371, 1349, 1028A). Available at: <https://www.justice.gov/file/1035477/download>.

30 Office of the Director of National Intelligence, “Assessing Russian Activities and Intentions in Recent US Elections,” Intelligence Community Assessment, January 6, 2017. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

31 “Facebook, Google and Twitter Executives on Russian Disinformation,” C-SPAN, October 31, 2017, [https://www.c-span.org/video/?436454-1/facebook-google-](https://www.c-span.org/video/?436454-1/facebook-google-twitter-executives-testify-russia-election-ads)

[twitter-executives-testify-russia-election-ads](https://www.c-span.org/video/?436454-1/facebook-google-twitter-executives-testify-russia-election-ads).

32 Mike Isaac and Daisuke Wakabayashi, “Russian Influence Reached 126 Million Through Facebook Alone,” *New York Times*, October 30, 2017, <https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html>.

33 “News Release: Klobuchar, Warner, McCain Introduce Legislation to Improve National Security and Protect Integrity of U.S. Elections by Bringing Transparency and Accountability to Online Political Ads,” October 19, 2017. Available at: <https://www.klobuchar.senate.gov/public/index.cfm/2017/10/klobuchar-warner-mccain-introduce-legislation-to-improve-national-security-and-protect-integrity-of-u-s-elections-by-bringing-transparency-and-accountability-to-online-political-ads>.

34 “News Release: Reps. Coffman & Kilmer Introduce Bipartisan, Bicameral Bill on Origins of Online Political Advertising,” October 19, 2017. Available at: <https://coffman.house.gov/news/documentsingle.aspx?DocumentID=2374>.

35 Twitter has also suspended almost 5,000 Kremlin-linked Twitter accounts. See: Twitter PublicPolicy, “Update on Twitter’s Review of the 2016 U.S. Election,” Twitter, January 19, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html.

36 Bruce Falck, “New Transparency For Ads on Twitter,” Twitter, October 24, 2017, https://blog.twitter.com/official/en_us/topics/product/2017/New-Transparency-For-Ads-on-Twitter.html.

37 Twitter PublicPolicy, “Update: Russian Interference in 2016 US Election, Bots, & Misinformation,” September 28, 2017, https://blog.twitter.com/official/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html.

38 Adam Mosseri, “News Feed FYI: Bringing People Closer Together,” Facebook Newsroom January 11, 2018, <https://newsroom.fb.com/news/2018/01/news-feed-fyi-bringing-people-closer-together>.

39 Adam Mosseri, “News Feed FYI: Helping Ensure News on Facebook is From Trusted Sources” Facebook Newsroom, January 19, 2018, <https://newsroom.fb.com/news/2018/01/trusted-sources>.

40 Jonah Engel Bromwich and Matthew Haag, “Facebook Is Changing. What Does That Mean for Your News Feed?” *New York Times*, January 12, 2018, <https://www.nytimes.com/2018/01/12/technology/facebook-news-feed-changes.html>.

41 Available at: <https://dashboard.securingdemocracy.org>.

42 Alliance for Securing Democracy (ASD) Team “Securing Democracy Dispatch,” German Marshall Fund, January 29, 2018, <http://securingdemocracy.gmfus.org/blog/2018/01/29/securing-democracy-dispatch>.

43 Dipayah Ghosh and Ben Scott, *Digital Deceit: The Technologies Behind Precision Propaganda on the Internet*, New America, January 2018, <https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit>.

44 European Commission, *A multi-dimensional approach to disinformation*, Report of the High Level Expert Group on Fake News and Online Disinformation, March 2018. Available at: <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>.

45 Ryan J. Foley, “Spread of fake news prompts literacy efforts in schools,” PBS NewsHour, December 31, 2017, <https://www.pbs.org/newshour/education/spread-of-fake-news-prompts-literacy-efforts-in-schools>.

46 Defending Digital Democracy Project (D3P) “Cybersecurity Campaign Playbook,” Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2017. Available at: <https://www.belfercenter.org/CyberPlaybook>.

47 Joseph Menn, “Facebook funds Harvard effort to fight election hacking, propaganda,” Reuters, July 26, 2017, <https://www.reuters.com/article/us-cyber-conference-facebook/facebook-funds-harvard-effort-to-fight-election-hacking-propaganda-idUSKBN1AB29J>.

48 Dario Salice, “Google’s strongest security, for those who need it most,” Google Blog, October 17, 2017, <https://www.blog.google/topics/safety-security/googles-strongest-security-those-who-need-it-most>.

49 Callum Borchers, “What we know about the 21 states targeted by Russian hackers,” *Washington Post*, September 23, 2017, [https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-](https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers)

[21-states-targeted-by-russian-hackers](https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers).

50 Matt Blaze, Jake Braun, Harri Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, and Jeff Moss, “DEF CON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure.” DEF CON. September 2017. Available at: <https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf>.

51 Verified Voting, “The Verifier - Polling Place Equipment - November 2018” Available at: <https://www.verifiedvoting.org/verifier>.

52 Ibid.

53 S.2261 - Secure Elections Act

54 “Senators Introduce Revised Secure Elections with Burr, Warner’s Support,” March 22, 201. Available at: <https://www.lankford.senate.gov/news/press-releases/senators-introduce-revised-secure-elections-act-with-burr-warners-support>.

55 H.R. 5011 - Election Security Act.

56 S.Amdt.656 to H.R.2810

57 H.R.3751 - PAPER Act

58 S.2035 - SAVE Act

59 Eric Geller, “Virginia bars voting machines considered top hacking target,” *Politico*, September 8, 2017, <https://www.politico.com/story/2017/09/08/virginia-election-machines-hacking-target-242492>.

60 Michael Rubinkam, “Pennsylvania to require voting machines with paper backup,” Associated Press, February 9, 2018, <https://www.apnews.com/b33d9d5fd72642058552662c9c9bf426>.

61 Bradford Queen, “Grimes Leads Board of Elections in Move to Require Voter-Verified Paper Trails in Kentucky,” Kentucky.gov, February 27, 2018, <http://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&pId=156>.

62 National Conference of State Legislatures, “Post-Election Audits” October 10, 2017, Available at: <http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx>.

63 U.S. Election Assistance Commission, “Checklist for Securing Voter Registration Data,” available at

https://www.eac.gov/assets/1/28/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf. <https://www.eac.gov/documents/2017/10/23/checklist-for-securing-voter-registration-data>

64 Tim Starks, “The latest 2018 election-hacking threat: 9-month wait for government help,” *Politico*, December 29, 2017, <https://www.politico.com/story/2017/12/29/2018-election-hacking-threat-government-help-231512>.

65 Morgan Chalfant, “Homeland Security speeds up election security aid to states,” *The Hill*, January 10, 2018, <http://thehill.com/policy/cybersecurity/368348-homeland-security-speeds-up-election-security-aid-to-states>.

66 Center for Internet Security (CIS) “A Handbook for Elections Infrastructure Security” Version 1.0, February 2018, available at: <https://www.cisecurity.org/elections-resources>.

67 Defending Digital Democracy Project (D3P), “The State and Local Election Cybersecurity Playbook,” Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2018. Available at: <https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook>.

68 Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall, “Election Security in All 50 States,” Center for American Progress, February 12, 2018. Available at: <https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states>.

69 Note, electoral disruption occurs—through malicious intent and natural incidents alike—every year. This discussion is limited to those efforts that include cyber means.

70 National Conference of State Legislatures, “Electronic Poll Books,” March 22, 2017. Available at: <http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx>.

71 Kevin Collier, “Personal Info of 650,000 Voters Discovered on Poll Machine Sold on Ebay,” *Gizmodo*, August 1, 2017, <https://gizmodo.com/personal-info-of-650-000-voters-discovered-on-poll-mach-1797438462>.

72 Compromising an official social media account to send a confusing message on election night may be easier than, say, falsifying a video news segment intended to

cause confusion.

73 More information available at: <https://www.cloudflare.com/athenian-project>.

74 More information available at: <https://protectyourelection.withgoogle.com/intl/en>.

75 U.S. Election Assistance Commission, “Checklist for Securing Voter Registration Data,” available at https://www.eac.gov/assets/1/28/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf.

76 Tim Starks, “The latest 2018 election-hacking threat: 9-month wait for government help,” *Politico*, December 29, 2017, <https://www.politico.com/story/2017/12/29/2018-election-hacking-threat-government-help-231512>.

77 Morgan Chalfant, “Homeland Security speeds up election security aid to states,” *The Hill*, January 10, 2018, <http://thehill.com/policy/cybersecurity/368348-homeland-security-speeds-up-election-security-aid-to-states>.

78 Center for Internet Security (CIS) “A Handbook for Elections Infrastructure Security” Version 1.0, February 2018, available at: <https://www.cisecurity.org/elections-resources>.

79 Defending Digital Democracy Project (D3P), “The State and Local Election Cybersecurity Playbook,” Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2018. Available at: <https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook>.

80 Ryan J. Foley, “Spread of fake news prompts literacy efforts in schools,” PBS NewsHour, December 31, 2017, <https://www.pbs.org/newshour/education/spread-of-fake-news-prompts-literacy-efforts-in-schools>.

81 Shannon Vavra, “Nielsen: Election officials don’t have necessary security clearances,” *Axios*, March 21, 2018, <https://www.axios.com/how-secure-are-us-elections-nielsen-state-local-officials-security-clearances-jeh-johnson-eb68ecff-add4-4047-80cd-6df9cb56b6ed.html>.

82 Defending Digital Democracy Project (D3P), “Election Cyber Incident Communications Coordination Guide,” Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2018. Available at:

<https://www.belfercenter.org/publication/election-cyber-incident-communications-coordination-guide>.

83 One such audit procedure is the risk-limiting audit, a statistically rigorous method of comparing a number of paper ballots with the digital vote tally, in order to confirm with high confidence that the paper tally matches the digital tally. For more on these procedures, see: Mark Lindeman, and Philip B. Stark. “A Gentle Introduction to Risk-limiting Audits.” IEE Security and Privacy, Special Issue on Electronic Voting (2012), available at: <https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf>.

84 Brennan Center, “Estimate for the Cost of Replacing Paperless, Computerized Voting Machines,” June 2017. Available at: https://www.brennancenter.org/sites/default/files/analysis/New_Machines_Cost_Across_Paperless_Jurisdictions%20%282%29.pdf.

85 J. Alex Halderman, “Russian Interference in the 2016 U.S. Elections,” U.S. Congress, Senate, Select Committee on Intelligence, Expert Testimony, June 21, 2017.

86 Brennan Center, “Proposed Election Infrastructure Spending,” March 22, 2018, <https://www.brennancenter.org/analysis/proposed-election-infrastructure-spending>.

87 Lawrence Norden and Christopher Famighetti “America’s Voting Machines at Risk” Brennan Center for Justice, September, 2015. Available at: https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

88 For an overview of electoral integrity and the many challenges it faces, see Pippa Norris, *Why Electoral Integrity Matters* (Cambridge: Cambridge University Press, 2014).

89 Michael Sances and Charles Stewart, “Partisanship and Confidence in the Vote Count: Evidence from U.S. National Elections since 2000.” *Electoral Studies* 40 (2015): 176–188.

90 Thad Hall, J. Quin Monson and Kelly D. Patterson, “The Human Dimension of Elections: How Poll Workers Shape Public Confidence in Elections” *Political Research Quarterly* 62:3 (2009): 507-22.

91 Natalie Adona and Paul Gronke, “Election Security and the 2016 Voter Experience.” Democracy Fund, December 2, 2016, <http://www.democracymfund.org/blog/entry/election-security-and-the-2016-voter-experience>.

[experience](#).

92 Ibid.

93 Ibid.

94 According to Fairvote.org, In recent elections, about 60 percent of the voting eligible population votes in national elections every four years, and 40 percent in midterm elections every two years. See “Voter Turnout,” FairVote, available at: http://www.fairvote.org/voter_turnout#voter_turnout_101.

95 There are also structural complications to duplicating security assurances that appear in commercial settings. Crucially, the secret ballot—and expectation that votes cannot be traced to an individual—differentiates voting security.

96 Election Assistance Commission, “A Survey of Internet Voting,” Testing and Certification Technical Paper #2, September 14, 2011. Available at: <https://www.eac.gov/assets/1/28/SIV-FINAL.pdf>.

97 National Conference of State Legislatures, “Electronic Transmission of Ballots,” September 27, 2016, <http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx>.

98 R. James Woolsey and Brian J. Fox, “To Protect Voting, Use Open-Source Software,” *New York Times*, August 3, 2017, <https://www.nytimes.com/2017/08/03/opinion/open-source-software-hacker-voting.html>.

99 For an extensive history of contested elections, see: Edward B Foley, *Ballot Battles: The History of Disputed Elections in the United States* (New York: Oxford University Press, 2016).



This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America's work, or include our content in derivative works, under the following conditions:

- **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit creativecommons.org.

If you have any questions about citing or reusing New America content, please visit www.newamerica.org.

All photos in this report are supplied by, and licensed to, shutterstock.com unless otherwise stated. Cover photo credit: Joseph Sohm / Shutterstock.com.

