Voting Systems: How They Work, Vulnerabilities, and Mitigation

By Duncan A. Buell and Steven Rosenfeld

Voting Systems: How They Work, Vulnerabilities, and Mitigation

Produced in partnership with the Independent Media Institute's Observatory and IMI's Voting Booth project.

For media inquiries/interviews, please contact the authors at:

buell@acm.org (Duncan A. Buell)

steven@ind.media (Steven Rosenfeld)

Cover photograph: Election worker Hazel Rountree explains how to place a ballot in the optical scanner on the first day of early voting in Ohio in October 2020. Photo © Sue Dorfman / Zuma Press. All rights reserved; used with permission.

Contents

1.0. Introduction

The world of running elections is little understood and widely politicized. Partisans who do not understand the stages of the voting and counting process have been quick to criticize elections as illegitimate when their candidates lose. These critics have made unfounded claims about the operations of voting systems and actions of election workers. Their accusations ignore many of the checks and balances that catch administrative mistakes and are intended to ensure accurate results.

Still, election systems, like any large electronic infrastructure composed of subsystems, are not without vulnerabilities that can impede their operation or be exploited by individuals seeking to tarnish the process. One of the biggest problems shadowing the national update of voting systems (following Russian meddling in the 2016 election) has been procedural lapses that caused incorrect vote count results to be released soon after Election Day. These errors were not quickly acknowledged but propelled much of 2020's election disinformation.

More specifically, the lapses were failures by election officials and their contractors to verify that the information and data in their systems have been accurately programmed and synced. This involves configuring the ballot layouts, the scanners that analyze the ink marks on ballots and assign votes, and the tabulators compiling subtotals into vote counts. When this information has been incorrect or uncoordinated, the unofficial results released immediately after Election Day have wrongly assigned vote totals. In most of the cases we know of, the errors were caught and corrected before the winners were certified. But these errors have fueled great partisan rancor.

When programming errors occurred in 2020's presidential election in Antrim County, Michigan, a rural expanse with fewer than 24,000 residents, Donald Trump's supporters claimed the initial incorrect tally reflected an untrustworthy election across the state. These partisans launched an investigation that reveled in stolen election clichés and which revealed a lack of factual knowledge of how election systems work. But because most voters do not know how elections are run, these and other false claims have lingered. As of fall 2022, tens of millions of voters still believe that President Joe Biden was not legitimately elected.

This report explains how the vote-counting pathways in the latest generation of

election systems works, their technical vulnerabilities, and some remedies. Its authors have spent years studying elections in complementary spheres. Duncan A. Buell is a lifelong computer scientist and more recently a county election official in South Carolina. Steven Rosenfeld is a national political reporter who has specialized in election administration and voting rights.

The authors believe the public is best served by understanding the interrelated mechanics behind voter registration, casting votes, detecting votes on ballots, and compiling results. Today's voting systems are layered and complex, and like the people who run them, they are not error-free. Thus, it is important that mistakes, where they occur, are understood, contextualized, and not exploited.

Today's voting systems can produce an extensive evidence trail of every operation that follows the voter and their ballot. Not all of the data sets accompanying these steps are public records in every state. But many crucial records often are. Additionally, many election officials are not always comfortable with sharing the powerful data they possess—data that could attest to results and pinpoint and rectify problems. However, this report describes and deconstructs election infrastructure as transparently as possible to steer disputes to reality-based factors and evidence.

1.1. How Did We Get Here?

Today's systems and many of the protocols surrounding vetting voters and counting ballots date to the aftermath of the 2000 election when Florida experienced technology and procedural failures. In response, Congress passed the Help America Vote Act of 2002 (HAVA), which provided millions to states to modernize their election equipment. At the time, such modernization led many states to acquire costly paperless electronic voting systems. These computers replaced paper ballots marked by hand, punch card ballots marked by computers, and older mechanical lever voting machines.

The paperless systems were generally bought between 2004 and 2006. This is when South Carolina bought a paperless system for use statewide. This occurred when Duncan Buell was chair of the computer science department at the University of South Carolina (2000–2009); later (2019–2021), Buell served as an election official in Richland County, where the state capital, Columbia, is located.

By 2018, the HAVA-era systems were aging. Starting around that time and in the three or four years that followed, most states and counties have been replacing them.

Sometimes, the replacements have been a somewhat improved version of a computer from the same vendor. For example, South Carolina used paperless voting computers from Election Systems and Software (ES&S), the iVotronic model. In 2019, it acquired newer computers from the same vendor that print a filled-out paper ballot card after a voter uses the touch screen to make their choices. In other instances, state and local officials acquired computer systems built around hand-marked ballots. (Russian hacking during 2016's election hastened the national return to paper ballots, whether marked by computers or by hand.)

The use of computers in the polling place has been controversial for years. In the mid-2000s, Maryland bought a system from Diebold (now Dominion Voting Systems). Professor Avi Rubin of John Hopkins University (and/or his graduate students) discovered online some of the source code for the Diebold system, and in 2004, they publicized what they saw as code written to a low-quality standard. This code detects and assigns votes to candidates, and then starts the process of preparing the subtotals that are compiled, like bricks in a pyramid, into the overall results. Rubin flagged security, transparency, and verification issues. The newest voting computers address many of these concerns. But there are new issues, such as accurately configuring the overall system.

In what follows, the authors refer to "voting computers" and not to "voting machines." This is intentional. When people think of a "machine," they often think of something that almost always works as expected. When people think of a "computer," we believe their expectation that it always works drops, which is appropriate in this circumstance.

For years, the authors have investigated allegations of fraud and malfeasance in elections. As a computer scientist, Buell has done extensive analysis of voting system data, but has never seen deliberate efforts altering results. As a journalist, Rosenfeld also has looked for such evidence, which he has not seen with the newest voting systems. (Such abuses, if they occurred, would likely be confined to

little-scrutinized local races, as regional contests have too many data sets and observers to go unnoticed.) But the authors have observed many errors. When the system has not been designed and written to make it hard to make errors, it will be (and has been) easy to make errors.

Most election officials and vendors will say that the mistakes are "human errors"—by voters or poll workers—and not the fault of the technology. But if the system cannot be used as intended, including by officials, their contractors, and election workers, then it is the system that is at fault in its design and implementation.

The national media does not cover elections at this level of detail. Influential outlets like the New York Times tend to summarize or trivialize key election administration tasks. For example, an August 2022 report called the system configuration mistakes in Antrim County "a minor clerical error… [that became] a major conspiracy theory." Clerical errors are typos when entering surnames and birthdays, not setting up countywide computer systems. Yet it is at this level of operation where errors occur that feed disinformation and partisan anger and undermine public trust in elections.

Since 2020, a new threat has emerged. Until very recently, most election officials, and the authors, maintained that the civil servants running elections seemed sincere and well-meaning. Yet among the nation's 8,000-plus local election officials, a handful have departed from their role as fair-minded referees and granted unauthorized access to voting computers to aggrieved partisans—who copied and shared computer drives, software, and data. While these actions have not changed any results, they have fed narratives that elections cannot be trusted and pose security risks (from more competent actors) in future elections.

Disclaimer: Much commentary comes from Buell's analysis of statewide election data from South Carolina from 2010 through 2018, with limited analysis after that, and his experience from March 2019 to March 2021 on the Board of Voter Registration and Elections of Richland County, South Carolina. Access and analysis of a state's voting system data for five biennial cycles is unprecedented in election circles. Rosenfeld's reporting augments trends and observations in recent cycles across the country.

In both instances, what we say is substantively correct, but readers should be aware

that each state has unique laws, procedures, and infrastructure. That said, let's begin to look at the architecture of running elections. We will start with some general comments about elections, why they are hard to administer, and why the process—the stages, subsystems, steps, and safeguards—is important.

1.2. General Issues With Elections

- Election Day is a distributed event. It is staffed by volunteers and conducted at any number of different venues (firehouses, schools, community centers, county headquarters, sporting venues, etc.).
- It's going to be chaotic, especially in high-traffic moments. Thus, contingency plans, and backups to the backups, are necessary.
- We will never know "ground truth" about results unless we carefully count every ballot by hand at least twice. But that is not going to happen, given millions of ballots cast in many states and time constraints. Thus, the *process* by which elections are conducted is everything.
- The candidates and the media expect the results available within nanoseconds of the polls closing on Election Day.
- Elections are a niche commercial market with little competition, where key steps are privatized.
- Most elections are a government responsibility and operation, and thus are almost certainly underfunded.

1.3. Specific Issues With the Use of Technology in Elections

- We often observe what Buell calls "a shortage of skepticism and an excess of hubris."
- Many officials, vendors and policymakers seem to believe that computers and data networks always work. We should instead use them but then be pleasantly surprised when they do actually work.
- Federal certification of voting systems requires testing by approved labs. The vendor pays for this, so tests are only done occasionally. This process is not as frequent or expedient as updating one's personal digital devices.

- The small market means few vendors and little leverage for improvement, especially when vendors lobby for sales and maintenance contracts.
- Relatively few election officials will know how the technology works. All but the largest jurisdictions are unlikely to have robust IT support, and what support exists will come at government salaries. This is the backdrop in a world where computer security is perhaps the biggest issue in computing, and the most competent people work in the private sector.

2.0. Basics: Terminology and Standard Examples

Before we begin a close look at elections, we will go over some standard terminology. The terms we use will not be applicable everywhere, but we trust that it will be simple to replace our terms with the terms used in other parts of the country.

It is best to think of voting as a series of stages where eligible voters are vetted, receive their ballots, and those ballots are counted and compiled electronically for the unofficial results released after Election Day. Similarly, it's best to think of election officials and workers as overseeing those discrete steps, which consist of different *subsystems*, each with rules, protocols, computer systems, and data sets.

For example, take voter registration. In every state except North Dakota, eligible voters must register. Some states do this automatically. Others require that residents file forms and meet deadlines. That starting line is well known. The voter registration system has its own data. This database contains address, citizenship, age, mental fitness, and other records, as well as a digital image of a signature. This is used to verify one's eligibility to vote, to assign voters to precincts, and, further downstream, to vet returned mailed-out ballot envelopes before opening them. That data set is not the same as what is used when other voting system software reads and analyzes individual ballots and then compiles vote subtotals and overall results.

When parsing the terms and examples that follow, think about how these relate to your experience voting and add up to an overall process and system. These terms and examples refer to what you will see at polls and election offices and begin to describe what is going on inside the computers used as the process unfolds.

2.1.0. Terms

Here are some definitions of terms that are used later in this report and are useful in understanding the voting and counting process. We start with who runs elections and how the correct ballots are prepared and delivered to voters. That is followed by computers that detect votes on those ballots and start compiling vote totals.

2.1.1. Jurisdictions

A jurisdiction is the administrative unit under which elections are conducted. In most parts of the U.S., these are counties. In some parts of the country, however, elections are conducted at an administrative level smaller than a county. (Michigan and Wisconsin are leading examples, owing to political districts with roots in the 19th century.) There's no jurisdiction larger than a county that is responsible for the detailed operation of elections.

In some states, such as Georgia, Louisiana, and South Carolina, the state mandates a single election system must be purchased from a vendor. In most states, however, counties can choose their own system, usually from a list of approved systems.

2.1.2. Precincts/Polling Places

We refer to polling places as the locations where voters come to vote. Polling places are not the same as precincts because, in some situations, a polling place may contain more than one precinct. Precincts are based on geographical boundaries. The critical point is that election officials know exactly which voters reside in which precinct. From that information, they determine what contests the voters are eligible to vote in, which, in turn, relates to the ballot the voter receives. Also, knowing which (and how many) voters are in each precinct and polling place lets officials allocate resources, from computers used to poll workers.

In some jurisdictions, the polling place will accept voters from all precincts. In others, the poll will have different areas set up for specific precincts. Increasingly, the practice of using "vote centers," where any voter in the jurisdiction can vote, has become popular. When vote centers are used, it becomes harder to predict how many voters will show up and know what resources to allocate. One version of a vote center is early voting sites, where people vote in person before Election Day. (There are three ways to vote: early and in person, early using a mailed-out ballot, and on Election Day in person.)

2.1.3. Election Offices/County Headquarters

The jurisdictions holding elections are typically overseen by a regional government office, usually county-level election departments. County departments manage the

general aspects of the distributed event that is an election, and are an intermediary between local governments and state authorities. In contrast, there is the setting for what gets done on Election Day, which we will refer to as "county headquarters." Often, this can be a warehouse-like facility for handling ballots, computers, etc.

We would expect that most election management activities are done at county headquarters. But there are some counties that conduct tasks at other sites, perhaps for lack of sufficient space. Detroit, for example, processes returned mailed-out ballots at a downtown convention center.

2.1.4. Configuring an Election

There are many aspects of setting up an election that must be accurately done and synchronized for votes to be correctly counted. These steps, which are discussed in greater detail later in this report (see 4.2.), begin with listing all of the contests and candidates on each paper ballot card (or on a computer screen on a paperless voting system). It continues with programming the scanners that detect and compile precinct-level votes, and additional computers that compile jurisdiction-wide totals. When seen from a county-level perspective, hundreds of computers and related devices—or more—must all be properly programmed, set up and synced to hold an election.

2.1.5. Ballot Style

The ballot style is the name given to the specific ballot with all of the contests for voters who reside in that precinct. As one goes from statewide races to more local contests, the candidates and contests will change due to the precinct. In Maricopa County, Arizona, where Phoenix is located, there were more than 800 ballot styles among the 2.1 million ballots cast in 2020's general election. Those styles do not include non-English ballots and braille ballots for the blind.

The ballot style becomes important in programming precinct and central office ballot scanners/vote tabulators (these can be separate computers or combined). The style is to be distinguished from the ballot's physical form. Ballots can be a hand-marked paper card, a computer-marked card, or a paperless electronic record on a touch screen computer. In 2022, more than 90 percent of registered voters will use hand-marked or computer-marked ballots that are scanned by counting systems.

Paperless voting stations are mostly used for people with disabilities.

When setting up the voting system for an election, each ballot style is implemented with what is called a "ballot definition file," which contains details used by the counting software. More on that is described later (see 2.1.14.).

2.1.6. Chain of Custody

Chain of custody is an inventory control term that has different applications with various aspects of running elections. Most commonly, it refers to the handling of ballots to ensure that they are properly logged, copied (if damaged or a voter errs), scanned, counted, batched, and secured. (Accounting for every ballot is a foundational part of verifying an election's accuracy.) The chain of custody also refers to the protocols surrounding the transfer of electronic ballot style and vote count data, such as portable drives used to program the computers used. (These devices include ballot-marking computers, scanners, and tabulators.)

2.1.7. Direct Recording Electronic (DRE)

A DRE is a computer that allows a voter to make choices on a touch screen and then saves the choices internally in its memory or directly to a flash memory card. The ES&S iVotronics used in South Carolina from about 2006 to 2019 were DREs. Some DREs added to their hardware a printer that would print the voter's choices on a paper tape that could be observed (not always easily) by the voter.

2.1.8. Ballot-Marking Device (BMD)

The successor (for the most part) to the DRE is a BMD. A standard example of a BMD is the ES&S ExpressVote. This is a touch screen computer. But instead of storing votes in memory in the computer, the BMD prints a paper ballot card that prints the voter's choices in a readable format for observation by the voter, as well as in a barcode (such as the ES&S ExpressVote) or QR code (Dominion Voting System's BMDs) for tabulation purposes. A scanner reads that code and starts compiling subtotals for the results in each contest.

2.1.9. Voter Verifiable

A ballot is voter verifiable if the choices that will be tabulated can be verified by the voter to be the choices that the voter made. We do not believe this term should

not be used for any of the BMDs or DREs that tabulate votes based on something that the voter cannot actually "verify."

For example, if a barcode or QR code is used for tabulating, then unless the voter has a cheat sheet to be able to read and understand the barcodes, whatever the voter can in fact view and understand (such as text that allegedly lists their choices) is actually irrelevant to the ensuing electronic tabulation. It is thus a misnomer to say that the voter can "verify" the choices made.

A hand-marked paper ballot, with ovals filled in, is voter verifiable. The voter can clearly see the names of the candidates and the ovals that have been filled in and can verify that the ovals correspond with their choices. There do exist BMD models that fill in the ovals. In that case, there is no real difference between a BMD-marked ballot and a hand-marked ballot (as long as the voter verifies the printout is correct).

2.1.10. Barcode/QR Code

A barcode is similar to the SKU code (stock keeping unit) with which we are now very familiar when checking out at a retail store. Barcodes are usually done, even in elections, using a standard encoding process. But in elections, the process of decoding is only understood by the election system software. Buell, for example, once scanned a barcode from a ballot using a barcode-reading app on his phone. That particular barcode, as a retail goods barcode, was a Fram oil filter. If decoded by the election software, however, a candidate choice or choices would have been indicated.

Barcodes are linear, one-dimensional, and read as bars and spaces left to right. A QR code is a two-dimensional analog. QR codes are used because they can encode more information in essentially the same physical space, but they are substantively no different from barcodes.

2.1.11. Hash Function/Hash Value/Hash Code

We will occasionally refer to a "hash." This comes up in discussing cybersecurity. It is standard practice in computing, and not a deep mystery to those who write the relevant software, that when things such as legal documents go back and forth over the internet, a hash value is transmitted. This makes it computationally impossible

for one party to change the terms of a contract (like the dollar value, say), without having the hash values fail to match.

In elections, like electronic commerce, this is accomplished by use of a hash function. When applied to the document, it produces a hash value or hash code. A long document of many pages could be hashed into a 256-bit (32-character) hash value, say, that represents an authentication signature for the document.

In elections, administrators and vendors could use hash codes to notarize the voting system's settings and data as part of preelection tests. After Election Day, they may (or may not) use hash codes to verify that the settings have not been corrupted before the results are certified.

Many of 2020's erroneous stolen election claims emerged in locales where different ballot definition files were mistakenly used at different stages in the process—causing configuration and counting errors. The use of hash codes would detect in advance if such problems exist and allow correction before incorrect results were published.

The U.S. Department of Commerce maintains national standards for hash functions.

2.1.12. Connection to the Internet

It is virtually always the case that election officials will claim that the voting system is "not connected to the internet," to attest to its security and accuracy. This assertion is often a misstatement and needs to be acknowledged as such. We do not want voting systems connected to the internet because that is a potential pathway for corrupting or disrupting the information used by the computers and the flow of data in an election.

In what follows, we will discuss how voting systems are configured. The process starts with precinct and ballot information that is usually taken from an online database, via flash drives or similar media, and used to program a county-level central tabulation computer. Since a flash drive is in fact "a computer," creating a flash drive from a computer that is connected to the internet, and then plugging that flash drive into a different computer is, in fact, a connection to the internet. Connection of a computer to the internet can occur either with a cable into the

wall, or via a wireless connection—or by a flash drive that has previously been connected. This security risk needs to be understood and accepted.

This risk is not a minor thing. In the early 2000s, when Buell was a University of South Carolina department chair, the FBI came to a meeting of the chairs to urge the faculty not to go to conferences and permit other attendees to plug in a flash drive to download their presentations. The FBI's concern at that time seemed to be industrial espionage—bad actors who could take control of computers used for technology research could enhance their own research programs at low cost and effort.

2.1.13. Digital Ballot Image

In most cases, a voter's paper ballot is not manually counted. Instead, each side of a ballot card is put through a computer scanner that immediately creates a digital image of that page.

You may notice dashes or grids printed along the margins of a ballot card. Those markings help the scanner software (preprogrammed with ballot definition files) to impose a grid that correlates the marked ovals—the voter's choices—with the tabulation system. The tabulation software compiles the results for that ballot, the precinct, and the jurisdiction. The original ballot, ballot image, and final database of every vote cast are key elements of ascertaining the accuracy of voting systems.

2.1.14. Ballot Definition File

A ballot definition file (BDF) helps the scanner search for ink-marked ovals, and the BDF assigns a vote to a candidate based on the location of that oval on the page. For example, J. Random Candidate could be in column one and in the fourth half-inch box going down from the top of the page. The BDF is like a cheat sheet that will say that column one, fourth box, is J. Random Candidate.

(With precinct-based vote counts, what is usually used at county headquarters is not the raw data from each voting station, but rather the precinct's combined subtotals for the candidates based on the cheat sheet that is the BDF. It is rare that a county processes raw data from precincts. It simply adds the precinct totals to its master count.)

2.1.15. Cast Vote Record

All of the votes, from all of the ballots, are compiled into larger databases called the cast vote record. (Different vendors don't always use this term the same way.) What's important is that the final version of this database is built from subtotals and is the basis for the official results. Each ballot can be a row in this spreadsheet, and each vote (or the absence of a vote) can be a separate column. The cast vote record (CVR) is often a large data file that cannot be easily read, due to its size, by software like Microsoft Excel.

The CVR is important in one other regard. It is the only election record that tells you which candidates did not receive votes. After the 2020 election, for example, analysts using this database found that tens of thousands of Arizonans voted for most GOP candidates on their ballot, but not for Donald Trump. The CVR not only revealed that split-ticket voting pattern, but it also showed where it occurred via the voters' precincts.

2.1.16. Central Tabulation Computer

In what follows, we describe how elections typically are administered. Inherent in this example will be a central tabulation computer at the county headquarters. This computer is used to configure the election and to total the votes from all of the sources of votes. (Officials and vendors often call this computer the "EMS," or election management system. Usually, it is located in a separate room with restricted access and video surveillance.)

2.2. A Typical Example of an Election Process

Here is one example of how election infrastructure operates based on the authors' firsthand experiences. This overview will not fit exactly with many counties, but we believe voters will be able to modify what's presented to fit their state's laws and practices.

- In South Carolina, the election system is standardized statewide, and the configuration of elections (that is, ballot styles in the various polling places) comes from the state. The state and county also cooperate with maintaining voter rolls, although the most up-to-date information tends to reside at county headquarters (from engaging with voters).

- South Carolina has early in-person voting, Election Day in-person voting, and early voting by mail.
    - Mailed-out ballots are returned to the county and are opened and tabulated using a centralized scanner (in Richland County), which is a higher-speed scanner than the scanners used in neighborhood polling places. (That centralized scanning operation is more efficient.) Some smaller counties only use polling place scanners.
    - All voters who vote in person use ExpressVote BMDs, both for early voting and for Election Day voting at polling places. These BMDs produce paper ballot cards that are scanned at the polling place. The local totals from the scans are brought back to the county headquarters on flash drives. Each BMD also has a flash drive that stays inside the computer during Election Day, and is brought back after polls close with the flash drives from the scanners. That BMD flash drive also will have on it the event log for the events that occurred on that computer. (The event logs trace every operation, from ballot paper jams to recording the votes cast.)
- The totals from precinct scanners are accumulated after polls close at county headquarters using a central tabulating computer. These totals are combined with totals from the headquarters' central scanner that has processed the returned mailed-out ballots.
- At intervals throughout election night, intermediate results are extracted from the central tabulating computer and are posted to the internet for the candidates, press, and public. (In many states, those results are published by county or state officials on their websites.)

2.3. Variations

- In counties that use hand-marked paper ballots (not BMDs or DREs) for most voters, there will still be scanned local subtotals for each precinct (assuming that the scanning is done at the polling place and not only at the county headquarters). Those subtotals will be essentially the same as what one would see from a BMD system. They become building blocks of the

overall cast vote record.

- Sometimes the scanning and tabulating systems are combined in one device. The ES&S ExpressVote XL voting computer allows for both marking ballot cards and tabulating votes, thus making the scanners unnecessary. This device doesn't change the basic nature of processing the data, except to change the number of computers from which partial information might be used to compile the results.

  One might imagine a polling place (such as Buell's precinct in South Carolina) with 10 ExpressVote voting computers, but only one scanner. That polling place's subtotals would come from the single scanner. Were this site using all ExpressVote XL computers, the subtotals would come not from a single scanner, but from each of the 10 voting station computers.

3.0. Corruption Versus Disruption

In considering security, vulnerabilities, and mitigation, it is important to distinguish corruption of an election from disruption of an election.

Corruption of an election means that the tabulation of votes has been altered by malice or malfeasance so the vote totals are not what they should be. In mid-20th-century America, one could conceivably corrupt an election in which the votes are tabulated at county headquarters by exchanging a box of ballots that are on their way from a polling place to county headquarters with another box of ballots with different choices made.

Disruption of an election means that something has happened in the process of conducting an election that makes the vote count sufficiently suspect that we might expect a different outcome in the absence of the disruption. When such intrusions occur, it is key to understand what has occurred, when and why it occurred, and the disruption's magnitude. That is, did it affect 10, 100, 1,000, or more votes—or a contest's outcome?

3.1. Disruption by Corrupting the Voter Registration Database

Theoretically, one could change the information of thousands of voters in jurisdictions where one would expect a particular partisan slant (such as Democratic-leaning urban centers). Voters who showed up would be told that they were either not registered, or registered at a different address, and thus could not vote at that site except with a provisional ballot. (That ballot would not count unless they presented more identification at county headquarters in the next few days, which most provisional voters don't do.)

Has this happened? In 2016, the scrambling of voter registration information was seen as a possibility after Russian agents infiltrated these databases in a handful of states. At the time, officials said that no voter information was altered. A related example can be seen in states that have conducted large voter purges using imprecise government records (data not sufficiently updated for vetting registration credentials). False positives have led to delisting thousands of voters, prompting lawsuits to restore their status.

Some conservatives charge that voter rolls are rife with illegal voters. The truth is

voter rolls always are in flux as people register, move, and die—and officials try to catch up via a range of list maintenance protocols. But voter fraud, or impersonating another voter or illegally voting, is very rare, and is usually detected by workers who vet voters at polls and county headquarters.

For example, in February 2022, Ohio Secretary of State Frank LaRose, a Republican, announced that his office had found 31 noncitizens who were registered to vote. None of these voters should have been registered. But none actually voted. There were four individuals who voted illegally prior to 2020, he said, and 27 people who voted illegally in the 2020 election. Those 27 individuals constituted 0.0005 percent of Ohio's nearly 6 million ballots cast in 2020's general election.

3.2. Disruption by Locally Allocating Insufficient Resources

Other forms of alleged disruption involve shortchanging voting and computer resources in specific polling places, leading to delays that would cause voters to leave and not vote.

During the November 2012 election in Richland County, South Carolina, long lines at polling places resulted in some people waiting up to seven hours to vote. Many conspiracy theories emerged about shortchanging polls in locales that might have opposed a sales tax. Buell was hired to analyze what had happened. He found no bias to support the conspiracy theories. Instead, his findings showed that a new election director had badly erred. A third of the voting computers were left in a warehouse during a high-turnout presidential cycle—in a jurisdiction that is half African American with then-President Barack Obama on the ballot. Almost all of the polls were shortchanged by almost the same fraction, and then computer failures further exacerbated the problem.

Lines and wait times were as long or longer in Miami, Florida, during the same election. The delays led Obama to appoint a Presidential Commission on Election Administration, co-chaired by Democratic election lawyer Bob Bauer and Republican election lawyer Ben Ginsberg. Among the commission's recommendations were longer polling place hours and more days of early voting. In 2016 in Maricopa County, Arizona, there also were big delays across Phoenix when new vote centers replaced longtime neighborhood polling places.

3.3. Disruption by Procedural Error

A different kind of disruption occurred in the GOP's 2008 presidential primary in Horry County, South Carolina (Myrtle Beach). When voters went to the polls on a Saturday, it was discovered that their new iVotronic voting computers had not been closed after testing earlier in the week. When poll workers tried to open the computers, the computers responded by saying that they already were open and had votes cast on them. The problem, as Buell recalls, was compounded because the one person who really knew how to fix the problem was home sick. It took some locations until mid-afternoon before technicians could get to the polls, close and flush the computers, and reopen them for accepting votes.

The political impact that could have occurred was that, since the Republican nominee, John McCain, had very strong support in Horry County, had McCain lost statewide, he might have had a legitimate claim that he lost due to loss of votes in Horry over the ensuing confusion. As it happened, McCain won statewide.

A different kind of disruption involving procedural errors occurred in Antrim County, Michigan, during the 2020 general election. It is an example of how administrative mistakes can morph into a conspiracy theory that undermines public trust. Antrim officials did not notice that some tabulators had been incorrectly programmed and had left out one race. The wrong ballot definition file had been used. The omission scrambled the preliminary results on election night—because the tabulator assigned votes to the wrong candidates in the database that compiled the results. (The mistake was fixed before the results were certified.)

However, the errors led Trump supporters to accuse Democrats and Dominion Voting Systems of rigging Michigan's presidential election. Trump allies and analysts, who claimed to be cyber experts but had no prior experience with voting systems, issued an error-filled report, including misreading computer event logs. An investigation by Alex Halderman, a University of Michigan computer scientist hired by the state, found the programming and configuration errors and cited the misreading of the system's logs.)

3.4. Disruption From Inadequate Electronic Support

Another disruption that has happened repeatedly and is likely to recur concerns

electronically checking in voters at polling places. Jurisdictions are increasingly fond of using so-called electronic poll books, or e-poll books, which are often wirelessly connected to a centralized voter registration database. (This electronic system replaces the old-style paper sign-in books.)

E-poll books permit online updating of a database in jurisdictions that offer same-day registration, and thus would prevent a voter from fraudulently registering and voting in several places on Election Day. They also permit early voting up to the last possible time, by recording the early vote and preventing that voter from also voting on Election Day.

However, these systems have failed repeatedly for different reasons. During the 2018 general election in Johnson County, Indiana, the county had insufficient bandwidth back to the central computer, and check-in of voters stalled. Similar problems occurred in the 2020 presidential primary in Los Angeles, California, when e-poll books had trouble connecting to the statewide registration database. A similar failure occurred after early voting opened at an Atlanta sports arena in 2020's general election.

(Another facet of potential e-poll book snafus concerns state rules surrounding their use. In some states, poll workers must obtain verbal approval from county officials before updating a voter's information at the precinct. That requirement can delay voters and voting. In other states, poll workers have more discretion, and there is no such requirement.)

3.5. Questions to Be Asking

- At each stage of the process, who is in charge? The state? The county?
- Where does the most current voter roll data reside?
- How many polling places are there, and how many voters are going to each? What is the distribution of these counts?
- What's the law regarding the maximum number of voters per polling place? What's the law regarding the number of voters per device/voting station?
- What's the plan for tech support on Election Day?

- Who configures the election—the jurisdiction? Or is this contracted out to a private company?
- If the county is using BMDs that produce barcodes or QR codes, what is the "official" ballot? Is it the text that the voter might be able to read and verify? Or is it the computer-printed code?
- Is the entire election system on a separate computer network that is not connected to the internet through either cabled or wireless means? (This would be good.) Or is it just firewalled with gadgets and software? (This would be bad.)
- What is the level of technical expertise in the election office? Are there people who really know the equipment? Or does the jurisdiction rely heavily on contractors?
- Does the jurisdiction use e-poll books? If so, are they connected to the voter registration database on Election Day? If so, how is it determined that adequate bandwidth exists?
- What's the law regarding mailed-out ballots? Where can they be returned in early voting and on Election Day? (The answer may not be the same.)
- When can the outer ballot return envelopes be opened? When can the inner envelopes containing the ballot be opened and the votes tabulated? When must election officials receive them?
- Are election data sets public records in your county and state? If so, when are they available? In what format is the data? And what cost is incurred in getting those records?

4.0. Looking Closer: Subsystems and Data Sets

One way to look at an election system is to follow the path that the data takes. Different data sets accompany various stages in the process of voting and counting. This data comprises the most direct evidence of legal voters, legal ballots, and vote counts. They also pinpoint vulnerabilities or errors at key junctures.

4.1. The Voter Registration Database

Voter rolls are not just the starting line of the process for individual voters. They also are the starting line of creating precincts and ballot styles and programming the various computers used in voting and counting.

This database is managed at both the local and state level. In most jurisdictions, a voter can look up and update their information in the voter registration (VR) database. In South Carolina, the lookup is done to the version of the database maintained by the state. In contrast, in Franklin County, Ohio, (Columbus) the lookup is done through the county's website.

How secure is VR data? If the database where lookups take place is online, it is susceptible to corruption. Tom Schedler, Louisiana's ex-secretary of state, confirmed this in a panel presentation. The version of the database where one could do a lookup in Louisiana was not the "official" VR database, he said; that information was offline with safeguards.

Many officials, nonetheless, believe that using firewalls or similar tools means that they can claim that their election system is not connected to the internet. This is wrong. Not connected means not connected. The bottom line is that a pristine, known-good copy of the VR database needs to be kept offline. Updates to the online database that voters can access must be monitored using tools whose validity can be verified.

Furthermore, updates from the online version to the offline version need to be made using software and procedures that ensure the official (offline) version is not corrupted. The offline version should be used to configure ballot styles and ballot definition files.

4.2. Configuring an Election

Configuring an election is an extremely consequential and underappreciated process.

From administrative, vulnerability, and disinformation perspectives, we contend that configuration problems are behind most of the known vote-counting meltdowns that have occurred with the newest election systems. Simply put, every voter has to be given the correct ballot. The voting system's analytics must be correctly programmed to assign that ballot's votes to the selected candidates and compiled into the correct precinct subtotals and jurisdiction totals. This is not simple.

To start, voters must receive the correct ballot. Voters assigned to a polling place may not all live in the same districts for all of the elected offices. In Richland County, South Carolina, there are precincts with voters who live in the city of Columbia and voters who do not live in the city. There are precincts with voters who live in one of two different congressional districts.

This backdrop requires different ballot styles be used. It is not a trivial matter to determine all of the ballot styles that will be needed for a particular polling place, and to ensure that the various computers used in each polling place are configured properly to accommodate all of the voters sent there. The issue is further complicated when vote centers are used, which often happens in states with early voting at a few locations. Vote centers must have all possible ballot styles on tap.

We need to think about what it takes to configure an election. South Carolina, for example, has about 2,300 polling places. In Richland County, with 280,000 registered voters and 140 polling places, there were about 400 different ballot styles for the partisan primary of June 2020. It is a huge challenge to configure an election so each voter, when they arrive at the polling place, gets the correct ballot.

Getting that ballot to voters is not done by typing in the configurations by hand. This process is done by a software program at some level (state or county) that produces computer files (called ballot definition files) that contain the ballot's configurations.

The ballot definition files are used by the county to configure the other computers

used in the polling places. That equipment can include on-demand ballot printers, ballot-marking devices, scanners and tabulators, thumb drives and storage media, and paperless stations for people with disabilities.

The setup typically occurs by sending a computer-readable file (on a flash drive, or a DVD disc) to the county headquarters. That computer file will be loaded onto the voting computers (often in secure staging areas) and will be available on any e-poll book. Election officials, vendors, and contractors don't like to talk about the configuration process. We would hope their programming information comes from an offline, pristine, known-good database and is delivered on physical media and not sent online.

4.3. Distributing Configurations to Polling Places

What occurs next is that the voting system's computers have to be set up properly. Various procedures exist around the country.

In some jurisdictions, all voters vote on a ballot-marking device (BMD). In some jurisdictions, voters mark paper ballots in the polling place and then feed the paper into optical scanners. In some jurisdictions, the paper ballots are brought back from the polls to a central location for scanning. In all of these situations, it is necessary that the BMDs and/or the scanners are configured to tally votes correctly. That means the ballot styles and configurations that are present on the county's central computer must be distributed to the devices used at the polling and the scanning places.

This task usually is done using flash drives or similar electronic voting cards. The ES&S ExpressVote, for example, has no internal memory (according to the documentation), and it runs using a flash drive configured for that ExpressVote computer at that polling place in that election. On Dominion Voting Systems' BMDs, a flash drive is programmed by poll workers with the correct ballot style, and that is inserted into the front of each ballot-marking computer. After a voter makes their choices, a paper ballot is printed with the votes in human-readable text and a QR code that's read by the scanner/tabulator.

Before polling place voting begins, the computers are put through "logic and accuracy" tests to ensure the configurations are correct. Part of the testing includes

creating hash codes (an encrypted sequence based on the underlying data used) to lock down—or notarize—the configurations. A hash code created at the end of the process can be compared to the earlier one to confirm that there has been no meddling (or even just a change due to something like redistricting). How much attention is paid to this part of the process is an open question. During the 2020 election in Antrim County, Michigan, officials initially did not spot their configuration errors.

4.4. Returning Polling Place Data to the Central Tabulation Computer

At the end of Election Day, data from the polling places needs to be brought back to the central tabulator. Typically, scanners at voting sites will analyze ballot cards and will compile their respective results, which are subtotals in the jurisdiction's overall count. However, there are instances when ballots are brought back to a central location for tabulation. Either way, the precinct-level results need to be compiled into a total count for the entire jurisdiction.

At this stage, chain of custody protocols take on added importance. If paper ballots are returned to be scanned at a central location (such as after each day of early voting), the number of ballots is noted, as that inventory is a baseline to ensure that the correct number of ballots are counted. There also are chain of custody protocols concerning the computers and flash drives. Poll managers put these items in bags or containers that are sealed, and whose movements are logged.

In the case of ES&S ExpressVotes, for example, each scanner at the polling place will have stored totals on a flash drive. That drive is returned to the central location, and the local totals are accumulated into a global (jurisdiction-wide) total. In the case of hand-marked paper ballots scanned at the polling place, the same process would hold. Subtotals would come from the scanners at the polling places, and they would need to be consolidated by the central tabulation computer.

4.5. Posting Intermediate Results

It is invariably the case that candidates, the media, and the public want to know the results instantly. It is usually the case that intermediate results are taken from the central tabulation computer and posted to a website, or to the state office, or to the media. When Buell was on the Richland County, South Carolina, Board of Voter

Registration and Elections, the state election office preferred that intermediate results were posted about once every hour.

Since the central tabulation computer is not supposed to be connected to the internet, this would probably be done by writing the intermediate results to a flash drive and then plugging that drive into a computer that was connected to the internet.

Obviously, then, that flash drive should only go in one direction—from the tabulation computer to the internet. That flash drive should then absolutely not be reused and plugged back into the tabulation computer; this would be yet another indirect way to connect the tabulator to the internet.

During the one and only time that Buell was permitted as an election official to watch this process, he observed that a flash drive that had been written by the central tabulation computer and then plugged into the internet-connected computer was then immediately plugged back into the central tabulator. When Buell pointed this out, the technician's reaction indicated he was more annoyed at the criticism than he was concerned about the fact that he had violated one of the commonsense rules of how to stay unconnected from the internet. In today's disinformation environment, following security protocols could not only lessen the prospect of intrusion by bad actors but also remove a target for partisan attack.

5.0. What Errors Have Been Seen?

Election officials will tell you that they hope for elections with large margins so that any problem will not be seen as having impacted the results. However, since the 2020 general election, a cadre of self-appointed "experts" have emerged and attacked the legitimacy of elections whose result they don't like—starting with Donald Trump's defeat.

One common tactic involves pontificating about imagined scenarios or technicalities that have little or no bearing on the factual mechanics or relevant vote count data. But because the public is not well-versed in how elections are run, these theatrics earn undue and uncritical attention. Small errors are portrayed as mountainous infractions. Election officials know procedural mistakes are inevitable. But many officials don't like to say so publicly. What follows are recurring programming and setup errors, some of which occurred in 2020's election and were mischaracterized as having rigged the results.

5.1. Insufficient Backup Plans in Case Things Go Wrong

Stepping back, one of the ongoing complaints about the process for running elections in South Carolina was that the process, as presented by the state to the counties, assumed that everything would work perfectly. Based on Buell's decade-long analysis of election data and observation of polling places, and from his experience serving on the Richland County election board, it didn't seem that South Carolina's required processes had sufficient contingency plans, and then backups to the backups. Poll managers were unable to figure out what to do when things went wrong.

Many of the errors that Buell observed stemmed from the state's election administration's lack of a good checklist to make sure that all has gone well. Ensuring that all of the voting computers were properly closed, or verifying that vote totals make sense, should be among standard directions to poll managers. Yet, it seems that this was not the case in South Carolina. (This same pattern was repeatedly seen in 2020's primaries when new systems were first deployed.)

5.2. Polling Place Configurations Differ From Central Count Configurations

An error that has been seen in at least four states is that the computers used at the

polls were given different configurations of what the ballot looked like—compared to the configurations used by the central tabulation computer at county headquarters.

We have examples from South Carolina, using the previous ES&S iVotronic direct recording electronic (DRE) voting computers; from Northampton County, Pennsylvania, using the newer ES&S ExpressVote XL computers; from Antrim County, Michigan, using hand-marked paper ballots and optical scanners from Dominion Voting Systems; and from Dekalb County, Georgia, which also used Dominion computers.

5.3.0. Four Examples

These examples, spanning the previous and current generations of voting systems, underscore the persistence of configuration errors.

5.3.1. South Carolina

We were first alerted to the configuration problem when analyzing the 2010 data in Beaufort County, South Carolina. In Bluffton 2C precinct, there should have been two county council contests on the ballot, but the configuration on the ES&S iVotronic computers had only one contest, while the configuration at county headquarters had both. Since the vote totals from the polling places were added into a spreadsheet based on their position in the precinct spreadsheet, and not based on matching up candidate and contest, the effect in this case was that almost all of the rows of vote counts (from the precinct in question) were shifted up one row in the county's spreadsheet and added into the wrong contest and candidate.

This configuration problem gave rise to an anomaly that apparently no one noticed. With 725 votes cast in the precinct, there were no votes reported for any candidate for County Council District 10 (the missing contest on the ballot) and no votes for or against constitutional question 4 (the last item on the ballot). Usually, configuration errors, if caught, can be corrected by manual adjustment.

In 2018, the same error occurred and went undetected in two different counties in South Carolina. It resulted in miscounted votes from the contest where the configurations were incorrect all the way down to the end of the ballot. Fortunately, no incorrect outcomes were certified.

5.3.2. Northampton County, Pennsylvania

A curious problem occurred in Northampton County using the newer ES&S ExpressVote XL computers in November 2019. In Pennsylvania, candidates who were endorsed by more than one party would have their names appear once for each party on the ballot, with the total votes being aggregated at county headquarters. Northampton County was informed by the state that this practice was contrary to state law and that candidate names were to appear only once, with the parties listed below the name. Northampton configured the ExpressVotes to comply with the law, but then added an informational box on the computer's screen to inform voters that they were seeing a different presentation of candidates from what they would have seen in the past.

After Abe Kassis, a leading candidate for a judgeship, got a few hundred votes and his competition received more than 20,000 votes, an anomaly was decided to be likely. News reports speculated about the cause, but did not suggest that it was a system configuration error. It turned out that the information box had received some 25,000 votes, as an ES&S executive reported five weeks after Election Day. The candidate expected to win actually did win once the anomaly was resolved.

5.3.3. Antrim County, Michigan

Essentially the same problem happened in Antrim County, Michigan, in November 2020, using not ES&S devices but rather Dominion Voting Systems hardware. Again, there was an update to configurations, but there was a different version of the x-y coordinates for the candidate ovals on the paper ballot at the polls from what was present at county headquarters. The result was that votes were shifted up one line in the totals, and in the first reporting, Joe Biden won in a county where he was expected to lose substantially. (As of summer 2022, pro-Trump candidates for statewide office in Michigan were still citing the Antrim County incident as their "evidence" that Biden did not win the state in 2020.)

5.3.4. Dekalb County, Georgia

In 2022's spring primaries for county commissioner, one candidate received no Election Day votes in all but seven precincts. Several factors led to configuration errors. One of the four candidates dropped out of the race. The computers in five

precincts had not been updated after the district's boundaries had changed after redistricting. A question only appearing on the Republican Party's ballot was not properly appearing on touchscreens—and the state's attempted fix (as it provides programming data) left most scanners expecting to see votes from four candidates. As a result, votes initially were misallocated. The results were corrected after a recount. (Georgia purchased Dominion systems for the state in 2019.)

5.4. Why Does This Happen?

This particular problem seems almost endemic in voting systems, given that it has been observed in ES&S systems and in a Dominion system.

Part of the problem is inherent complexity. The central tabulation computer, also used to configure the devices to be used in the polling places, is a single computer running a particular operating system, probably an older version of Windows. The devices (BMDs, scanners, etc.) are independent from the central tabulation computer, are almost always running on a different operating system, and are being configured over some days of preparation time.

In Richland County, South Carolina, for example, there was one central computer but about 1,100 ExpressVote voting computers, and about 160 scanners, each of which needed to have a flash drive configured individually. We would expect to see some coordination problems when so many devices are used. Moreover, today's voting system software *does not* verify that everything is in sync.

While most local election workers are dedicated, nonpartisan, and fair-minded, their systems are complex and have many parts. In the South Carolina data, for example, this particular coordination error was noticed in perhaps five precincts statewide in every biennial election cycle. Detection of many such errors could indicate malfeasance (or colossal error), but a small number of such errors in 2,300 precincts never seemed like anything other than a random user error (or perhaps a bug somewhere in the software).

There are standard ways to ensure that the configuration used in the central computer is the same as what is used at the polling places. (These would be variations of hash codes to ensure that electronic documents on different devices are the same.) But these checks and balances are apparently not built into today's

election software.

5.4.1. Transcription Errors by Humans

Most election systems will permit election workers at headquarters to make manual adjustments to vote counts. Most commonly, this is done by county workers who scrutinize digital images of the sloppily marked ballots to determine the voter's intent. Dominion's computers, for example, flag and segregate these ballots. (This process, called adjudication, can be controversial if it's done without political party observers present and agreeing with the decisions.) The best new systems, however, create multiple records of the changes made.

But it can happen that election workers accidentally type in the numbers incorrectly. In Antrim County, Michigan, some of the manual "corrections" to earlier incorrect electronic tallies were still incorrect, a post-2020 report by University of Michigan computer scientist Alex Halderman found. Although it is probably necessary with any system to allow for manual adjustment, this does, of course, lead to understandable opportunities for error.

5.4.2. "Add Votes" Versus "Replace Votes"

In the 2010 election in South Carolina, neither the state nor the county was ever able to produce the correct vote totals in Colleton County. Working from the data, Buell and a professional colleague were able to produce the correct totals. One of the main problems appeared to be that after an initial miscount, votes from some voting computers were counted twice.

A close look at the voting computer showed that the screen display for adjusting vote totals by *adding* in votes was visually almost identical to the screen for adjusting vote totals by *replacing* one set of votes with another. It appeared that double counting had happened by adding votes instead of replacing votes. (Counting twice can also occur when local officials do not pay attention to chain-of-custody issues, such as when paper ballots get jammed in a scanner and are rerun through the same computer.)

5.4.3. Double Counting of Votes

Although the public never sees this, ballots are processed in batches as they are

counted in precincts and centralized counting sites. It can happen that batches of votes, or sometimes the votes of entire voting computers, are counted twice. Adding votes instead of replacing votes can cause this. We have also seen this occur when voting computers malfunction as they are used (and are sidelined) and vote tallying needs to be done in alternative ways.

In Marlboro County, South Carolina, in the 2018 primary election, one of the voting computers failed in the Wallace precinct. The normal procedure was that vote totals were collected on a handheld device, and then those totals were combined at county headquarters. The voting computer that failed had five votes on it. Since the iVotronic keeps a cast vote record on an internal memory card, it is possible to count votes from the memory card instead of in the usual way. However, in the Wallace precinct, the 148 votes from the four other voting computers were tallied in the usual way and then also from the memory cards, resulting in those 148 votes being counted twice.

Another example of votes being counted twice occurred in Mesa County, Colorado, in the 2020 general election and sparked conspiracy theories—which were compounded when the county clerk allowed Trump supporters to make unauthorized copies of the computer drives and data. The county's election manager made several errors using Dominion's adjudication system, including initially double-counting more than 20,000 votes because she stopped the computer and did not properly reset it, an investigation by Mesa County's prosecutor found in May 2022. (Among other things, his report had screenshots taken from overhead video of the incident.) The same official made similar mistakes in the April 2021 municipal election, the prosecutor reported. Pro-Trump analysts keep insisting that Dominion's system secretly added the votes.

5.4.4. Problems From Hardware Failures

The aforementioned failure in Marlboro County raises yet another question that we have never seen answered. What happens when the computer's memory fails? In our analysis, we saw occasions when the event log of the iVotronic very specifically recorded a memory failure. If the computer is known to have failed, what should be done with the votes on the computer? (This snafu was a more prevalent issue in paperless voting systems that have largely been replaced. If it

occurred in today's voting systems, it would take some effort to recover the votes.)

5.4.5. Devices That Have Votes but Claim Otherwise

In Buell's time spent observing elections in Richland County, there were three instances where an iVotronic DRE was opened for voting and used to collect votes, but the DRE later declared to a poll worker trying to close the iVotronic that it had never been opened. In November 2018, the problem surfaced again, and several hundred votes were initially not counted.

This is a particularly insidious problem. In large jurisdictions (like Richland County), it was common that a handful of iVotronics, perhaps four or five of the 1,100, would break down sometime on Election Day, and then they would report that they would have no votes cast on them. When Los Angeles County deployed its new voting system in 2020's presidential primary, many precincts had voting stations that froze as they were used and were taken out of service. It was unclear if any votes on those computers were counted.

5.4.6. Failure to Account for All Devices and Data at the End of Election Day

In many jurisdictions, there is a large quantity of computers and gadgets that go out the door before the in-person voting begins. But there may not always be checks in place to ensure that everything is returned safely and is accounted for after the polls close. With the newer ExpressVote (BMD) computers, there is additional hardware. In Richland County, for example, in addition to the more than 1,000 ExpressVotes, each of which has its own flash drive, there is a scanner (usually one, sometimes two in the large polling places) with its own flash drive. Imagine being responsible for keeping track of all of this "stuff," especially if you are a tired poll worker or staffer at county headquarters.

5.4.7. Unreported Votes

Sometimes, votes are missing when officials release election night totals. This is not the same as adding in votes from mailed-out ballots that may be processed in batches after Election Day. In 2011, the county clerk in Waukesha County, Wisconsin, a GOP stronghold, announced that her workers found several thousand votes on the day after Election Day. These votes erased the narrow lead by a Democrat in a high-stakes state Supreme Court race. The clerk said that she failed

to include a spreadsheet with the votes from one town in the election night returns.

6.0. Post-Election Day: Canvass Boards, Recounts, and Audits

Elections do not end on election night, even though the media would like the public to believe that their projections—and desire for candidate concession speeches—are the final word. The preliminary results announced are the first *unofficial* results. The final margins, if they are close, can trigger a recount.

Depending on the jurisdiction and their technology, the post-Election Day process to finalize the results can involve different procedures by election workers, local election boards, and political party representatives, although the overall goals are the same.

In general, with mailed-out ballots, there are steps that are akin to checking in a voter at a precinct. First, the ballot must be received by the county election office on time. Some states accept them after Election Day and others do not. Then, a ballot return envelope must be vetted to affirm the voter's identity—via a signature (usually found in the voter registration database) and other information written on the outside envelope. Only then is the ballot removed and scanned, and its votes are counted by a tabulator.

6.1. Voter Intent

A similar process involves vetting sloppily marked ballots, which are reviewed to determine the voter's intent before being counted. (These ballots can be cast in person or by mail.)

Different voting systems automate some of these processes. For example, when Dominion's system analyzes the digital ballot image of a hand-marked paper ballot and finds a sloppily marked oval, or perhaps marks for more than one candidate in a single contest (called an overvote), the computer will set aside that ballot for later review by an election worker at headquarters. That county worker will visually inspect a digital image of the ballot made by the scanner. If the voter's intent is clear, the county worker will assign the vote to the candidate, which is added to the count's totals. Dominion's system records the voter intent determination and notes its adjudication in the final cast vote record database.

The interpretation of voter intent by election officials can be controversial. In San Francisco County, California, which uses the Dominion system, workers seated

before banks of computer screens review ballot images to make that determination. In states like Arizona and Colorado that use adjudication systems, representatives from political parties or the candidates must be present and agree. If the voter intent review is done in-house by election workers, the jurisdiction's election director may make the final determination or forward the ballot to a canvass board for final scrutiny.

It is unlikely, however, that the physical ballot in question would be retrieved by the worker. That scrutiny might come later before the canvass board or during a recount. Canvass boards (and recount boards), whose roles vary by state, can also review questionable signatures on mailed-out ballot envelopes. They approve the jurisdiction's vote counts that become the certified result. While there is some training associated with these various reviews, there are no standards in most state laws and regulations concerning voter intent and signature matching.

6.2. Verifying Vote Counts

The certification of results happens under different timetables in different states. South Carolina requires that election results be certified no more than seven business days after Election Day—in other words, assuming Election Day falls on a Tuesday (which it usually does), then the results would have to be certified by the Friday of the following week. In other states like California, the certification may not occur for as long as several weeks after Election Day. The varying deadlines limit the scope and specificity of vote count reviews.

Once an election has been certified, losing candidates can file for recounts. Recount thresholds vary by state but usually are margins of less than a half or a quarter of a percent. (A candidate may have to pay for the recount if it is not automatically triggered.)

Recounts involve securing all of the ballots followed by a mix of rescanning and/or manually counting some or all of the ballots. Most states do not provide for manual recounts. (Hand counts take longer and are prone to some degree of human error due to their laborious and repetitive nature.) Election lawyers often say that recount laws are among the least precise in election administration. In 2016's presidential recount in Wisconsin, for example, each county could decide whether to do a hand count or a machine count. In 2022, Florida became the first state to authorize its

counties to use digital ballot images in recounts. (Maryland uses the ballot images to verify the results before certifying winners.)

During recounts, lawyers or representatives of the opposing candidates argue whether specific ballots should be accepted or rejected. These arguments often rely on whether the voter intent was clear or on bureaucratic technicalities, such as how and when a ballot return envelope was postmarked or received. The judges are local boards, which are not always composed of representatives from across the political spectrum.

One question that arises before recounts occur is what is done to double-check results before certifying winners. The answers vary and are little understood by the public.

Some states require that a small sample of ballots, often from preselected precincts, be hand-counted as a way to attest to the overall system's accuracy. Those precincts may not be the best indication of the system's accuracy across the jurisdiction. Officials or their contractors may do other procedural checks, such as creating hash codes on the system's configurations that can be compared to the codes created before voting began. If preelection and post-election codes are the same, it would confirm there was no meddling with the configuration and operation. But not all jurisdictions do this.

On the other hand, some jurisdictions conduct the equivalent of unofficial recounts. The state of Maryland and a handful of counties in Florida and other states do this, but they are the exceptions nationally. These jurisdictions verify their preliminary results using ballot image-based comparisons. Maryland hires an outside firm, Clear Ballot, to retabulate results from the digital images created by ES&S's scanners—their Election Day system. The Florida counties rescan each paper ballot produced on Election Day using different computers and Clear Ballot's software.

These efforts seek to double-check the accuracy of every vote cast and explain discrepancies. Computer scientists worry that digital ballot images could be corrupted—or fabricated by partisans alleging election fraud. But, as of mid-2022, there have not been any breaches of digital ballot images produced on certified voting systems.

Fears aside, the benefits of ballot image reviews are they can be done quickly, they are a full accounting of all of the votes cast, and they provide easily understood visual evidence—the ink marks on the ballots. Conceivably, the original paper ballot, ballot image, and cast vote record database could be compared.

But that fuller process and accounting are not currently done. (Why not? After Election Day, many officials don't want more work. And some states don't treat ballot images as public records, although the U.S. Department of Justice issued guidance in July 2021 instructing states to retain their "digital or electronic" election records for 22 months, which is the standard for paper ballots.)

6.3. Post-Election Audits

What states and counties tend to do, instead, is conduct recounts as prescribed under state law, and then they perform post-election audits after taking a break. Audits do not have the legal weight of official recounts, where judges are present, voters and individual ballots can be challenged and possibly disqualified, and the winner can change. (Election lawyers say that unofficial margins larger than 1,000 votes almost never are reversed.) Instead, audits tend to be quality control exercises that reveal systemic weaknesses and help develop best practices.

There generally are two types of audits, each with variations. The first is essentially an unofficial recount, either conducted by computers or by a hand count. The second type of audit is a statistical review, where a subset of randomly selected ballots is used to estimate the overall accuracy of the election's results.

Under the "unofficial recount" fold, computers rescan some or all of the ballots. These computers can be the same ones used during the election, or an unofficial recount can be done using an independent analytical system—such as ballot-image software. In general, using an independent system, called dual verification, is better than reusing the same system. But vendors have resisted this approach since the Help America Vote Act became law in 2002.

Hand counts, which many pro-Trump partisans are calling for a return to (along with the scrapping of all computers in voting), are far more laborious, time-consuming, and error-prone—due to their repetitive nature. Unlike electronic scanning and analysis of paper ballots in batches, hand counts do not lend

themselves to first confirming the ballot inventory is complete and correct (including duplicates). That accounting is a key controlling factor that sets the stage for comparing vote totals.

In response to these audit approaches, statisticians have developed and promoted what is called a "risk-limiting audit." There are several versions of these. They are all based on randomly sampling ballots to estimate the overall accuracy of the reported results. Usually, an initial number of randomly counted ballots is set to statistically achieve a confidence level—or "risk limit"—of 90 percent or 95 percent.

In elections with wide margins, risk-limiting audits—which do not rely on any electronics but instead are a highly focused incremental hand count—are attractive to officials who want stamps of approval but do not want to manually recount every ballot. However, if the contest in question's margin is close, as was the case in 2020's presidential election in Georgia, it can be simpler to recount every ballot, as opposed to randomly selecting and extracting tens of thousands of ballots in populous counties.

6.4. The 2020 Presidential Election

The fact that the verification procedures were not easily understandable to the public created a vacuum in the 2020 election that was exploited by Trump's supporters. The loudest voices took advantage of the public's unfamiliarity with how votes are cast and counted to put forth accusations about swarms of illegal voters and forged ballots. These narratives, which were conjectures notably lacking factual references, revealed much about the accusers.

But the loudest voices dominated the media. Election officials initially took the posture of nonpartisan referees. They let state and federal courts assess and dismiss virtually all of the false claims for lack of evidence. But when then-President Trump kept saying that the election was stolen, partisan opportunists started to echo and exploit his claims. One result is that as of fall 2022, tens of millions of Republican voters still believe that they are true.

What didn't happen, initially, is worth noting. Election officials in the handful of swing counties in battleground states decried and debunked the disinformation. But

initially, most did not use their voting system's data and analytics to defend their results. Nor did they confirm and seek to explain the small procedural errors that occurred, such as in Antrim County, Michigan, where officials initially didn't spot errors that had been made during the voting system configuration. Only many months later did some elected officials, such as the Republican-led state senate in Michigan and the GOP-led board of supervisors in Maricopa County, Arizona, issue detailed rebuttals to false claims and specific accusations.

There was a notable exception in nongovernment circles. A longtime data analyst for the Arizona Republican Party and two retired voting system technologists used publicly available data sets to debunk several key false claims. On the false charge of massive voter fraud, they used Maricopa County's voter registration database to account for every voter by name. The exceptions were several hundred voters whose names were kept confidential because they were judges, police officers, or crime victims.

They also used the cast vote record to identify how many ballots contained a majority of votes for Republican and Democratic candidates, but *not for each party's respective presidential candidate*. The cast vote record is the only data file that shows which candidates did not receive a vote. That analysis, released in January 2021, explained Trump's loss in the state. It revealed that sufficient numbers of suburban Republican-leaning voters did not vote in favor of giving Trump a second term. Their location could be traced by the ballot styles' precincts. When Georgia's Republican Secretary of State Brad Raffensperger testified before the House Select Committee to Investigate the January 6 Attack on the U.S. Capitol on June 21, 2022, he made the same point. The data showed that sufficient numbers of otherwise loyal Republicans did not vote to reelect Trump.

These factual analyses have not stopped Trump supporters from perpetuating the lie that Biden was not legitimately elected. Indeed, the post-election reviews sanctioned by pro-Trump GOP legislators in Arizona and Wisconsin have succeeded in sowing doubts about the election, although they universally failed to present any proof. However, the election's aftermath has seen the emergence of a new threat: a handful of local election officials and county sheriffs (in Colorado, Michigan, Wisconsin, and Georgia) who are actively supporting the partisans who continue to attack the integrity of the 2020 election.

From an election security perspective, the prospective threat is not from the bumbling pro-Trump activists. Rather, the threat is that by gaining unauthorized access to election systems and posting software online, more technically capable actors could conceivably seek to disrupt or corrupt the actual operations of conducting future elections.

Election officials and vendors do not want to talk about or lend credence to that prospect. They want to convey confidence in election results and restore public trust. Officials also are reluctant to talk about human errors in administering elections—in data entry, programming, configuring, syncing, testing, and verifying—that routinely recur, and have recently been exploited and attacked by partisans unhappy with election results. Nonetheless, there is ample data to document election outcomes.

Today's voting systems have strengths and weaknesses. This report was created to explain how these systems work and to discuss vulnerabilities at key junctures that have been exploited by partisans seeking to sow chaos and doubt about the results.

It is the authors' hope that readers—from voters, to trusted community leaders, to journalists, policy experts, and lawmakers—will better understand how elections are run and how votes are detected and counted and will bring an evidence-based mix of skepticism and realism to this foundational feature of American democracy.

7.0. Questions That Readers Might Ask About Voting Systems

It is invariably the case that we learn more from mistakes than we do from things that work properly. Having seen the mistakes that have been made, using equipment from several vendors and in various jurisdictions around the country, we can formulate questions that address whether these mistakes might be likely in the future.

We have no doubt that election officials will refuse to answer many of these questions, usually on the grounds that the answers would expose security risks. But we quote Carolyn Crnich, former clerk of Humboldt County, California, from a phone call with her in 2012: "I don't ever want to have to tell my voters, 'Just trust me.'"

7.1. Procedural Issues

1. What certification requirements for election computers and systems exist in your jurisdiction? Must the equipment be federally certified? Must it only be certified by the state?

2. What is in fact the precise wording of the laws regarding certification, and is the law being followed?

   In some states, a review of the source code of a voting system's hardware and software is required but apparently has not been done. In some states, an escrow of the source code is required. Has this been done?

3. At what jurisdictional level is the voter registration (VR) database maintained? The state? The county? Is the online version of the database the only copy? What provisions exist for ensuring that corruption has not occurred, and have those provisions been created by the jurisdiction, or are they simply using the reporting and management modules of the database software?

4. What is the process by which ballot styles and the election configuration go from the VR database to the tabulation computer for configuring the hardware? Does this come from a computer connected (whether directly, or indirectly on a network that is only firewalled from the internet) to the

internet? Or is this done from a database that is not connected to the internet? Who does this configuration? Is this done by public employees or by a private company?

5. How are the ballot styles and the election configuration delivered to the devices (DREs, BMDs, and/or scanners)? If this is done with flash drives, what provision is made to ensure that the drives really are clean, and have not been plugged into a computer that has been connected to the internet?

6. What is the process by which intermediate results are uploaded on election night after the polls close? Can we be sure that this is done using (removable) media that are never plugged back into the tabulation computer?

7. What election data sets are available as public records? Do your state public records laws or agency directives include electronic data? Are local government officials preserving these electronic records? Key data includes voter registration, ballot definition files, ballot images, and the cast vote record. When is the earliest that data sets are available before and after Election Day? What format is the data in? What is the cost associated with obtaining the data set?

8. The Presidential Commission on Election Administration report (2013) asserts that people should not have to wait more than 30 minutes to vote. Realizing that this may not always be possible, a rule of thumb applied is that resources in the polling place should be sufficiently adequate that 95 percent of the voters wait less than 30 minutes. What's your jurisdiction's plan for achieving this goal?

9. Long lines can possibly be avoided by a proper layout of the polling places. Queueing theory says that average wait time is minimized if there is one line queueing up for multiple check-in stations. Is this what happens at your polling place?

7.2. Software Issues

1. What software is being used in your jurisdiction (in the polling places and in the central office)? From what vendor? What is the update mechanism, and

who does the update? (In South Carolina, we believe, the update is done by the maintenance vendor, while in Colorado, updates are generally done in the counties by staff from the secretary of state's office.) How are the updates delivered? On discs? On flash drives? Over the internet? From the state?

2. What provisions exist in the central software for ensuring that the obvious errors that could be made will not be made? Is there a checkout/check-in part of the software that verifies what gear gets sent out, what gear might have failed on Election Day, and what gear has been rerturned safely and been accounted for?

3. What is the process for reporting bugs in the software? Is the software thoroughly understood by the election officials, or must they be assisted by vendor staff or vendor maintenance staff?

7.3. Hardware Issues

1. What hardware is being used in your jurisdiction in the polling places? Are the devices DREs or BMDs? What scanners are used to read hand-marked paper ballots? When was it purchased and from what vendor? Who does the maintenance on the hardware? Who is responsible for any updates to firmware in the hardware? Who is responsible for checking on any flaws found in the hardware and then correcting for those flaws (or at least mitigating the effect)?

2. If your jurisdiction uses DREs or BMDs, what is the allocation formula? How many voters per device is considered acceptable?

   (A common assumption among those who study queueing theory is that polls need to have sufficient equipment and supplies so that no resource is more than "half-full" at the end of the day. South Carolina, for example, suggests that voters be given three minutes to vote. The state has a 12-hour Election Day, which is 720 minutes. So, if a device were used nonstop, it would be able to accomodate 240 voters. Election administrators who don't want polling place systems to be more than "half-full" would then deploy enough devices so, on average, each device only accommodate 120 voters.)

3. How is the check-in of voters done? Are the voter lists still paper books? Is the check-in done with e-poll books? From what vendor? Is there a paper backup of the electronic voter roll? And are they required to be connected to a common database on Election Day? If so, who measures the bandwidth needed, and what are the contingency plans should there be connectivity problems?

4. What's the networking of the computers at election headquarters? Is the central tabulation computer electronically disconnected from any network? Or is it just firewalled from internet-connected computers?

5. Some vendors advertise and sell devices (notably scanners) with wireless modems for sending results over the internet back to headquarters, or at least to a collection spot. If your jurisdiction uses scanners, do they have modems? Are the modems used? Is the modem always active? Is it "disconnected" by a software switch, or is there actually a hardware switch that disconnects the modem?

8.0. Bibliography and Other References

1. Andrew W. Appel. "Security Seals on Voting Machines: A Case Study." ACM Transactions on Information and System Security, vol. 14, 2011.

2. David Becker, Jacob Kipp, Jack R. Williams, and Jenny Lovell. "Voter Registration Database Security." Center for Election Innovation and Research, 2018.

3. Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman. "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" Proceedings, 41st IEEE Symposium on Security and Privacy, 2020.

4. Matt Blaze, Jake Braun, Harri Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, and Jeff Moss. "DEF CON 25 Voting Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure." 2017.

5. Matt Blaze, Harri Hursti, Margaret MacAlpine, Mary Hanley, Jeff Moss, Rachel Wehr, Kendall Spencer, and Christopher Ferris. "DEF CON 27 Voting Machine Hacking Village." Report, 2019.

6. Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William P. Zeller. "Source Code Review of the Diebold Voting System." Top-to-Bottom Review for the State of California, 2007.

7. Center for Internet Security. "A Handbook for Elections Infrastructure Security." 2018.

8. Edgardo Cortés, Liz Howard, and Lawrence Norden. "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack." Brennan Center for Justice, 2018.

9. Paul T. Cotton, Andrea L. Mascher, and Douglas W. Jones. "Recommendations for Voting System Event Log Contents and Semantics." 2009.

10. Christopher R. Deluzio, Liz Howard, Paul Rosenzweig, David Salvo, and

Rachael Dean Wilson. "Defending Elections: Federal Funding Needs for State Election Security." Brennan Center for Justice, 2019.

11. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. "Security Analysis of the Diebold AccuVote-TS Voting Machine." 2006.

12. J. Alex Halderman. "Analysis of the Antrim County, Michigan November 2020 Election Incident." 2021.

13. Tim Halvorsen, Larry Moore, Benny White. "Lessons from Maricopa County: Slow Facts Versus Fast Lies in the Battle Against Disinformation." September 2, 2021.

14. Harvard Kennedy School Belfer Center for Science and International Affairs. "The Cybersecurity Campaign Playbook." 2017.

15. Mark Lindeman and Philip B. Stark. "A Gentle Introduction to Risk-Limiting Audits." NIST, 2012.

16. Maricopa County Elections Department. "Correcting the Record: Maricopa County's In-Depth Analysis of the Senate Inquiry." January 2022.

17. Maryland State Board of Elections, "2016 Post-Election Audits in Maryland." Presented at the National Association of State Election Directors' Winter Meeting, February 19, 2018.

18. Matt Masterson, Jennifer Depew, Katie Jonsson, Shelby Perkins, and Alex Zaheer. "Zero Trust: How to Secure American Elections When the Losers Won't Accept They Lost." Stanford University Internet Observatory Cyber Policy Center, 2021.

19. Brian Mechler. "Voting System Examination of Election Systems and Software EVS 6.1.1.0." Office of the Secretary of State of Texas, 2020.

20. Larry Moore. "Visualizing A Close Election Contest and Resolution." August 27, 2021.

21. National Academies Press. "Securing the Vote: Protecting American Democracy." 2018.

22. National Association of Secretaries of State. "Cybersecurity Resource Guide." 2022.

23. Office of the Secretary of State of Ohio. "EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing." 2007.

24. Ronald L. Rivest and John P. Wack. "On the Notion of 'Software Independence' in Voting Systems." NIST, 2008.

25. Daniel Rubenstein, Mesa County, Colorado, District Attorney. "Conclusion of Investigation of Report 3 re: Elections." May 19, 2022.

26. Michael A. Specter and J. Alex Halderman. "Security Analysis of the Democracy Live Online Voting System." 2020.

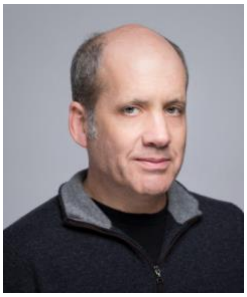
27. Stanford MIT Healthy Elections Project. "The Virus and the Vote: Administering the 2020 Election in a Pandemic." July 1, 2021.

28. Philip B. Stark. "Ballot-Polling Risk-Limiting Audits in Two Pages (±1)." 2012.

9.0. About the Authors

Duncan A. Buell is a visiting assistant professor of computer science at Denison College in Granville, Ohio. In 2021, he retired from the University of South Carolina, where he was a professor in the Department of Computer Science and Engineering and was department chair and interim dean. He served as a consultant to the League of Women Voters of South Carolina on election technology and analyzed Election Systems and Software (ES&S) election data from South Carolina, Pennsylvania, Texas, Kansas, North Carolina, and Colorado. He also was a consultant to Richland County, South Carolina, and Maricopa County, Arizona, on resource needs to prevent long lines at polling places.

Email address: buell@acm.org
Website: http://duncanbuell.org



Steven Rosenfeld is a national political reporter who has covered democracy issues since the 1990s. He has reported for Vermont newspapers, Monitor Radio, and National Public Radio, and many websites including BillMoyers.com, the New Republic, AlterNet, Salon, American Prospect, National Memo, LA Progressive, and others.

Rosenfeld turned to election administration after Ohio's 2004 presidential election. In 2010, he was part of a Pew Center on the States team that designed the Electronic Registration Information Center, which 33 states and the District of Columbia use to update voter rolls and contact eligible voters. Since 2016, he has focused on the evidence trails in elections. He has written or co-authored six books on election topics, including 2021's oral history, "The Georgia Way: How to Win Elections." His reporting is distributed by the nonprofit Independent Media Institute, where he directs its Voting Booth project.

Email address: steven@ind.media
Website: https://votingbooth.media