The Ohio State Technology Law Journal

PROTECTING THE PERILOUS PATH OF ELECTION RETURNS: FROM THE PRECINCT TO THE NEWS

STEPHEN PETTIGREW* & CHARLES STEWART **

CONTENTS

* Director of Data Sciences at the University of Pennsylvania's Program on Opinion Research and Election Studies and Senior Analyst for the NBC News Decision Desk and Data Analytics Lab.
** Kenan Sahin Distinguished Professor of Political Science, Massachusetts Institute of Technology; MIT Director of the Caltech/MIT Voting Technology Project.
This essay was prepared for presentation at the symposium on Elections in the Era of Technological Threats and Opportunities, Moritz College of Law, The Ohio State University, January 17, 2020. We are grateful to the five election officials who shared the details of how their states' election-reporting systems work, and who shared candidate assessments about vulnerabilities inherent in those systems, along with possible responses.

I. Introduction

For observers of technology and democracy, the use of computers to administer elections has always been seen as a mixed blessing. Computers promise to help achieve two goals that are at the core of a well-run election: speed and accuracy. Computers also introduce unseen complexity[1] that can be challenging to manage. Trading off the values of speed and accuracy against the costs of unseen complexity has been at the core of election administration for over a century.[2]

In recent years, attention to this accuracy-complexity tradeoff has focused on voting systems, by which we mean the systems, usually computerized, that record and tabulate votes. Less attention has been paid to the systems that take over after the tabulation has been accomplished. Among these are the "election night reporting" (ENR) systems that disseminate the tabulated results to the public. In principle, there is no reason to exclude these computer systems from the larger discussion of the accuracy/complexity tradeoff in elections.

The accuracy/complexity tradeoff of ENR computer systems is just the start of an examination of the role of technology in disseminating election results to the public. Once election results have reached ENR systems—sometimes through the Internet, which raises additional concerns—into "the wild," they are subject to dissemination through pathways that include the traditional and social media. What are the perils in these pathways?

---

[1] The adjective "unseen" is key to the trade-off we describe. The complexity we have in mind is unseen in at least two salient ways. First, the inner workings of computer systems used in elections are often hidden from direct scrutiny by the public, and even the election administrators who purchase and use them. This contributes to the second way in which computer-induced complexity in elections is unseen: because computer systems in elections function seamlessly in the experience of voters most of the time, the degree of complexity in these systems, including the possibility that they may fail, may be underappreciated.

[2] We time the beginning of this tradeoff before the introduction of electronic computing because the introduction of mechanical means of automation, particularly mechanical lever machines, also introduced unseen complexity into what had previously been a purely manual process.

In this paper, we consider the role technology plays in disseminating election results to the public, including the possibility that the larger system might serve as a conduit for mis- or disinformation. We classify vulnerabilities facing the election-return-reporting system into two major categories, *static* and *dynamic.* Static vulnerabilities pertain to potential weaknesses in the system that arise because of the short-term functioning of the system, such as tendencies toward being "hacked" by actors with malicious intent. Dynamic vulnerabilities arise out of the fact that election returns are released over time, not instantaneously. The dynamics of election return reporting, even when they are not compromised, leave them open to being used for disinformation campaigns that can call the legitimacy of an election into doubt. Technical fixes can certainly be applied to the election-return reporting system to harden it against malicious attack or protect it against simple errors. But technical fixes are not enough. Some vulnerabilities are rooted in inherent qualities of election-result reporting. Thus, policy responses must be based on social responses, such as public education and more nuanced coverage of election results by the media.

II. Cyberattacks on Election Systems: Knox County and Ukraine

Our argument rests on a premise that at the most general level, there are two ways in which computer technologies can play a major role in undermining what the public learns about the vote count. The first is that the computer systems themselves can be overtaken by malicious actors. The second is that even correct information can be the fodder for disinformation campaigns, made even more potent by the operation of social media platforms.

To help illustrate the first role for computer technologies, we highlight two important cases where election-result-reporting systems have endured cyberattacks. The first, in Knox County, Tennessee in 2018, was a distributed denial of service (DDOS) attack on the county's ENR

system.[3] The second was a more comprehensive attack on the ENR system in the 2014 Ukrainian presidential election.[4]

a. Knox County, Tennessee

Probably the most visible domestic attack against the computer system of an American election authority was unleashed against Knox County, Tennessee during its May 1, 2018 primary.[5] Investigations of the incident suggest that an attack was directed to the Election Commission's website as a cover for a much more extensive intrusion into the county's computer systems.[6] Nonetheless, the attack on the election commission itself reveals the nature of the vulnerabilities that local election authorities face, and the capacity of malicious actors to potentially manipulate reported election results.

The Knox County event began with a DDOS attack against the county election-reporting website a few minutes before the system was due to

---

[3] A DDOS attack is one in which a malicious actor attempts to overwhelm a computer server with a huge amount of traffic, thereby preventing legitimate web traffic from communicating with the server.

[4] Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers,* CHRISTIAN SCI. MONITOR (June 17, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers [https://perma.cc/F643-2U5J].

[5] Oishimaya Sen Nag, *The 10 Biggest Cities in Tennessee*, WORLD ATLAS, https://www.worldatlas.com/articles/the-10-biggest-cities-in-tennessee.html [https://perma.cc/9NVW-CSMV] (Knox County, Tennessee is the home to Knoxville, the third-largest city in the state); *QuickFacts Knox County, Tennessee*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/knoxcountytennessee [https://perma.cc/M9GJ-8TP7] (Knox County itself, with a population of over 465,000, is Tennessee's third-largest county); s*ee* Brittany Crocker, *Mayor Burchett: Cyber-security Contractor Will Investigate Election Night Attack, K*NOX NEWS (May 2, 2018, 11:19 AM), https://www.knoxnews.com/story/news/2018/05/02/knox-county-officials-investigating-election-night-cyberattack/572236002/ [https://perma.cc/79R4-D9V8] (news accounts indicate that the county had "11 security experts" who worked to resolve the election night problems that are described below).

[6] Tyler Whetstone, *Knox County Election Night Cyberattack Was Smokescreen for Another Attack,* KNOX NEWS (May 17, 2018, 4:54 PM), https://www.knoxnews.com/story/news/local/2018/05/17/knox-county-election-cyberattack-smokescreen-another-attack/620921002/ [https://perma.cc/64L9-69T5].

start reporting the incoming precinct election returns when the polls closed at 8:00 p.m.[7] The attack, which appeared to emanate from IP addresses in approximately 65 countries, made the election board's website unavailable for an hour, as IT workers scrambled to diagnose the nature of the problem and to bring the system back up.[8] While the server was down, it appears that intruders were able to examine the data files behind the public facing server, but not to change them.[9]

In the aftermath of the incident, county officials, along with the outside cybersecurity consulting firm that was hired to investigate the attack, emphasized that the original data displayed on the publicly facing results server—located on electronic storage cards that stored the vote counts from the DREs used in the election—was stored in a way that established a physical gap between the website and the raw vote results.[10] In other words, had the results been changed on the web server, they could have been restored by reference to these original memory cards.

Events in Knox County highlight many themes that come up repeatedly in anticipating possible attacks against the election-reporting system. They start with the basic architecture of the larger election-result reporting system, about which we say more below. They include statements from officials that the issue with these attacks was not whether election results could be fraudulently manipulated, but public confidence in the results in light of reports about the attack. Ultimately, because there is no known way to guarantee against all DDOS attacks, nor to resist all intrusions into a computer system, the focus for most administrators is on "resilience," that is, guarding irreplaceable assets

---

[7] SWORD & SHIELD ENTERPRISE SECURITY, ROOT CAUSE ANALYSIS: KNOX-COUNTY-ELECTION-WEB SITE-5-8-2018, 4 (2018),), https://media.wate.com/nxs-watetv-media-us-east1/document_dev/2018/05/11/swordandshield_1526059177836_42308769_ver1.0.pdf.

[8] Benjamin Wofford, *The Hacking Threat to the Midterms is Huge. And Technology Won't Protect Us*, VOX (Oct. 25, 2018, 5:00 AM), https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting [https://perma.cc/5QZJ-Z368].

[9] *Id*.

[10] SWORD & SHIELD ENTERPRISE SECURITY, *supra* note 7, at 4.

and responding quickly to the attacks that do occur.[11] In light of that, it is unsurprising that Knox County Deputy Election Administrator Chris Davis was quoted as saying in the days after the attack, "[f]rom our perspective, everything went according to plan. . . . All the results came in on time. We just could not release them out on the web because of the cyberattack. Otherwise, everything went smooth [sic]."[12]

Finally, the incident provides a glimpse into the decision-making that goes into deciding how to respond to attacks of these sorts. On the one hand, the presence of several security experts on hand at the time of the cyber-attack indicates that the county—admittedly a fairly large one—had directed significant staff resources to the issue of computer security. On the other hand, press accounts also noted that the county had recently focused its attention on guarding against ransomware attacks, in light of a recent high-profile, massive attack against Atlanta, Georgia. (The Atlanta attack had shut down many of the city's mission-critical computer systems for days, costing it $17 million to respond to a $50,000 ransom demand.[13]) Considering the alternatives, it appears that DDOS attacks against the servers communicating election results to the public could be classified among the "normal accidents" of election administration.[14]

b. Ukraine

---

[11] James P.G. Sternbenz, et al., *Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines*, 54 COMPUTER NETWORKS 1245, 1245 (2010), (resilience can be defined as "the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation").

[12] Crocker, *supra* note 5.

[13] The Atlanta ransomware episode has been widely covered. *See* Benjamin Freed, *One Year After Atlanta's Ransomware Attack, The City Says It's Transforming Its Technology,* STATE SCOOP (Mar. 22, 2019), https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/ [https://perma.cc/2YH8-ZSFZ]; *see also* Theo Douglas, *What Can We Learn from Atlanta?*, GOV'T TECH. (Oct./Nov. 2018), https://www.govtech.com/security/What-Can-We-Learn-from-Atlanta.html.

[14] CHARLES PERROW, NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES 13 (1984).

A more troubling real-world case involves Ukraine and its presidential election in 2014, when a "three-pronged wave of cyber-attacks aimed at wrecking Ukraine's presidential vote—including an attempt to fake computer vote totals—was narrowly defeated by government cyber experts. . . ."[15] The attacks rolled out from May 22 through May 26. They began ahead of the election, when Ukraine's security service discovered that the computer system of the Central Election Commission had been infiltrated, that malware had been installed, and that key files had been deleted.[16] The next day, the hacktivist CyberBerkut, which has been identified as a pro-Russia organization, credibly took credit for destroying Ukraine's election computer infrastructure.[17] The damage was reported as having been repaired before the election had begun. Yet, within 40 minutes before election results were scheduled to be reported on Sunday, May 25, a virus was removed from the election commission computers that would have caused the ultra-nationalist Right Sector party leader Dmytro Yarosh to be announced the winner with 37% of the vote.[18] (Yarosh instead actually received less than 1% of the vote.[19]) In particular, the removed virus programmed the election system to display a graphic reporting Yarosh's victory, rather than affecting the vote tabulation directly. That same image was broadcast on Russia's Channel One in a news bulletin, despite the fact that it had never appeared on the election commission's website, indicating that the hacker(s) had supplied the image to Channel One.

To top everything off, a DDOS attack was directed against the vote-reporting system in the wee hours of the morning following the election,

---

[15] Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers,* CHRISTIAN SCI. MONITOR (June 17, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers [https://perma.cc/F643-2U5J].

[16] Tim Mauer, *Cyber Proxies and the Crisis in Ukraine*, *in* CYBER WAR IN PERSPECTIVE: RUSSIAN AGGREGATION AGAINST UKRAINE 81 (Kenneth Geers ed., 2015).

[17] Benjamin Jensen et al., *Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist,* 42 J. STRATEGIC STUD. 212, 227 (2019).

[18] Clayton, *supra* note 15.

[19] *Id*.

knocking the system out for two hours.[20] Despite the challenges related to the "hostile security environment," the joint Office for Security and Cooperation observer group observing the election declared it to be "genuine."[21]

Something akin to the Ukraine episode is certainly what election officials and other election experts consider to be a worst-case scenario for election reporting. Of course, the situation would have been worse had the malware not been discovered, and false election results had been communicated to the Ukrainian public, rather to a Russian audience.

Nonetheless, the episode shows what is possible with a determined, and apparently well-resourced, hacker adversary. Imagine such an attack being waged against the state election division of a battleground state in the upcoming 2020 United States presidential election. And, imagine that instead of planting a virus that caused an implausible victor to be declared ahead of the vote count, the wrong leading candidate was announced holding a large, yet plausible, lead. Even when corrected, such an announcement could both undermine public confidence in the administration of the election *and* provide aggressive social media purveyors of disinformation with the raw material to rile up credulous followers.

The Knox County and Ukrainian cases illustrate the range of challenges that face the ENR system. For Knox County, it is not even clear that the attack was directed at the elections commission for the purpose of disrupting the election; it could have been part of a larger attack to plant ransomware in the larger county computer system, or even steal more lucrative information about residents and businesses in the county. Nonetheless, the attack illustrates at a minimum that local election systems are a target, as are all local government systems. For Ukraine, the case illustrates that well-resourced malicious actors can wreak havoc on a highly visible system.

---

[20] *Id*.

[21] OFFICE FOR DEMOCRATIC INSTITUTIONS & HUMAN RIGHTS [ODIHR], UKRAINE, EARLY PRESIDENTIAL ELECTION 25 MAY 2014, at 3 (2014), https://www.osce.org/odihr/elections/ukraine/120549?download=true.

Two points must be made before moving on. First, in both Knox County and Ukraine, the official vote count was not compromised because of these attacks. The official tabulation process occurred in parallel with, but still separate from, the computer systems that were compromised. Election officials could provide a good-faith assurance to the public that the correct results were eventually certified. Second, while one can see how attacks such as these *could* undermine confidence in the election, there is no evidence that they *did.* Americans in general have become aware of the dangers lurking in the Internet, and Ukrainian citizens are certainly aware of the barrage of pro-Russia cyberattacks directed their way every day. As far as we know, there has been no scientific research into how the public reacts to attacks such as these. It is reasonable to suspect that they become more worried about the integrity of the election. It is also quite possible that the reassurance of officials, especially local officials, works, and that the swift action of local government workers in responding to such attacks reassures voters. Because answering questions such as these are important intellectual and public policy questions, it is incumbent on political science to direct its considerable capacity to study public opinion in this direction.

III. How Election Results Are Reported

Knox County and Ukraine provide a glimpse into what types of attacks are possible on the computer systems that report election results. Yet, news and other reports of these incidents leave out an important piece of evidence that would help place these attacks in context, and to assess just how similar attacks could be successful.

To gain a full appreciation of where the vulnerabilities lie in the reporting of election returns in the United States, it is helpful to sketch out with some precision how information about votes cast in polling places is communicated to the public. In the grossest of terms, there are two major information channels to consider here. The first is the formal communication of information about election results from the polling place to the authorities who are responsible for certifying election outcomes. The second channel is the reporting of election results informally via the mass media, which is how most Americans receive

information on election night. While the latter information channel is more likely to be subject to mis- and disinformation activities, the integrity of the former helps to bound the degree to which incorrect information is communicated to the public.

a. Reporting election results formally

State laws and regulations govern how information about election returns is transmitted from polling places[22] to the authorities who are responsible for certifying the results of the election. We have not conducted a systematic review of state laws and regulations to characterize how this occurs across the states. Rather, in this section we rely on our professional experience, direct observation, and interviews conducted with five state election officials, who were asked to describe how their states' ENR process work, and to reflect on where vulnerabilities in their processes might lie. [23]

We have constructed a generic, ideal-typical[24] ENR system and describe it in reference to Figure 1. Along the top are the three physical locations where the information moves within and between the polling place, the local election authority, and the state election authority. Along the bottom is represented the means through which the flow of official information is conveyed to the public.

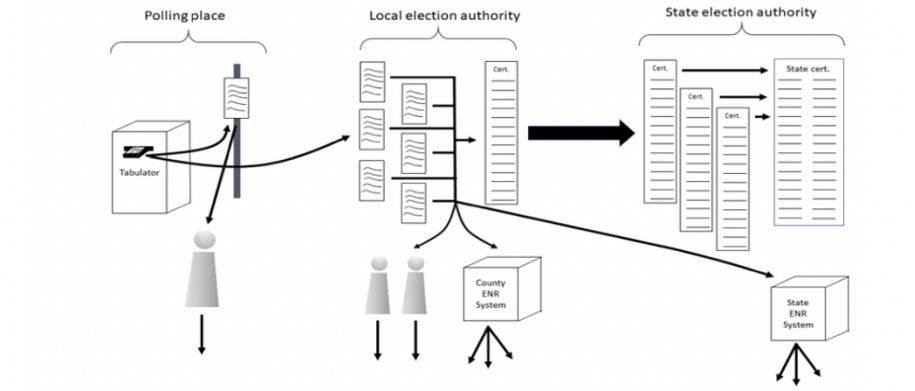
---

[22] For the purposes of this discussion, we treat absentee ballot tabulation precincts as polling places, even though the ballots are marked in a location removed from where the ballots are tabulated. The important thing is that in absentee ballot precincts, scanners (or possibly, hand-counters) tabulate a collection of ballots in a particular place.

[23] No claims about randomness or representativeness of these five states are made here, other than that they were chosen because they represented a mix of centralized and decentralized systems, in-person dominant and mail dominant, and scanner dependent vs. DRE dependent.

[24] Sun Ho Kim, *Max Weber,* STAN. ENCYCLOPEDIA OF PHIL. (AUG. 4, 2007), https://plato.stanford.edu/archives/win2019/entries/weber/.

Figure 1. Schematic view of election return information flows.



The chain of events starts in the polling place, where votes are tabulated and initially reported.[25] In 2016, 98% of votes were tabulated with a computer.[26] Virtually all tabulators, whether they be scanners or DREs, produce a paper-tape report at the closing of the polls that is posted immediately outside the polling place—often near the door of the polling place—once it has been attested to by the polling place officials. Multiple copies of this report are made, to be included in the packet of materials that is physically delivered to the local election authority on election night.[27]

---

[25] Some local election jurisdictions tabulate in-person Election Day ballots centrally, rather than in the polling place. The fundamental processes we describe here pertain to these situations, too.

[26] Data and Stata do-files necessary to reproduce this statistic are available from the author. Total votes cast by local jurisdiction were taken from the United States Election Assistance Commission's Election Administration and Voting Survey (EAVS). Voting method use was taken from Verified Voting's online voting technologies. A small amount of missing data from the EAVS was collected from state election returns.

[27] Most states require that election materials such as election return records be returned to the local election authority immediately upon the close of polls. Election officials do not allow official election return records to "sleep over" at the home of the local election judges, even when this is allowed before the election. One of the authors of this paper has witnessed a local election director dispatch a sheriff's deputy to the home of an election judge to retrieve election returns when the judge, claiming fatigue, went home to bed rather than deliver materials as required.

Tabulators also typically contain electronic memory devices that record the vote-total information that was printed out. These memory devices are removed from the tabulator and are included with the bundle of documents that is delivered to the local election authority for further processing.[28]

Official records of the election returns—including memory cards, paper-tape vote reports, and forms accounting for all of the ballot that had been delivered to the polling place—are then physically delivered to the local election authority. In many jurisdictions, when the materials are received at the local-jurisdiction office, the memory cards from the tabulator units are inserted into a card reader that is attached to a computer that uploads the data and imports it into the election-management software that manages the accumulation of vote reports from the distributed polling places.

From our experience, it is common practice for these central computers to be dedicated to the task of receiving election returns from polling places and readying them to be transferred to the outward facing ENR server. As the memory cards are read and ingested into the vote-counting software, at regular or irregular intervals, the election returns that have been received are transferred to another physical memory device. That physical memory device is then taken to a computer where data from the device are uploaded and incorporated into the software that ultimately manages the dissemination of results to the public.

In some states, the polling places will communicate election returns directly with the local authority, by phone or modem, to report election

[28] In polling places that have multiple computer tabulators, one of the tabulators will often serve as an "accumulator," which receives the tabulation data from the other machines, and then produces a single consolidated vote report for the polling place. This is most common when the polling place has DREs, which are commonly deployed in multiples in polling places. When an accumulator is used, the various machines are networked together in a "daisy chain," which allows information to flow among the machines. This network, while internal to the polling place, and possibly involving electronic poll books, is not connected to computer systems outside the polling place.

returns ahead of the delivery of the official record of election results to the election office. If by phone, staff in the local election office write down the election returns and hand-enter them into the software that reports election returns for immediate dissemination to the public.

At this point, the local office undertakes a short-term process related to informing the public of election results in that jurisdiction. This process is two-pronged. The first is communicating directly with the public. Many large jurisdictions and some small ones handle this communication primarily through a Web-based ENR system that can contain both traditional human-readable reports and automated data feeds that can be directly ingested into media-based election-return-tracking systems. Most small jurisdictions handle this communication by making available printed reports that summarize the returns from that jurisdiction. The major news organizations typically assign an employee to ensure that information concerning election returns is delivered as soon as possible to those organizations. The employee might be a beat journalist, a "stringer," or even the local election official who has been contracted to supply the information to the news organization. The emphasis on speed is such that sometimes the information fed to news organizations through this human-based network scoops the information displayed on the Web-based ENR system.

The second reporting process of the local office is communicating with the state. As returns come in on election night, the local jurisdictions are in communication with the state election office concerning the unofficial results they are receiving. This communication can take a variety of forms, ranging from phone calls to a networked reporting solution that connects all of a state's local ENR systems to the state system. This communication can also take on a variety of levels of detail, from comprehensive precinct reports to simple summaries by office.

Finally, the election-night information reported from the local jurisdictions is reported by the state. States are less heterogeneous in how they report than local jurisdictions, but there is still interstate variation. At one end are states that maintain sophisticated ENR websites that display results by varying degrees of geographic

aggregation and graphical sophistication.[29] Some of these systems are home-grown, but some vendors have entered this arena and provide a product that is largely standardized across states.[30] At the other end are states such as Massachusetts, that do no centralized election-night reporting at all. As with local jurisdictions, media organizations often hire individuals to cover state election-result reporting.

For the most part, the election-night reporting system just described is entirely unofficial. It is conducted both for administrative reasons—to give election officials an initial sense about how the election was conducted in their domain and whether any special circumstances need to be addressed immediately—and because candidates, other election officials, and the public demand it.

Calling this the "election-night reporting system" can be a misnomer, because some of the information may flow in the days immediately after Election Day. In addition, previously-incorrect information might be corrected. We return to this point below.

Whether and how election officials should operate a public-facing program of election-night reporting is subject to discussion and debate among election officials themselves. The main issue is whether election officials should maintain Web-based ENR systems that communicate returns directly to the public. Election officials often remark that the look-and-feel of these systems is "official," even when statements appear on the web sites indicating the results are unofficial and preliminary. Some officials believe that this causes credibility problems when the numbers inevitably change before final certification. By this reasoning, relying solely on media organizations to report preliminary results makes it clearer, though not 100% clear, that the results are unofficial. Furthermore, not engaging in election-night reporting, beyond posting paper reports of vote tallies, removes an administrative

---

[29] *See, e.g.*, *November 6, 2018 General Election*, GA - ELECTION NIGHT REPORTING, https://results.enr.clarityelections.com/GA/91639/Web02-state.221451/ [https://perma.cc/ET8R-Q7H9].

[30] The largest of these vendors is Scytl, a Spanish firm. In the 2018 election, we observed 11 states that appeared to be reporting election-night results using the Scytl system.

expense and reduces potential administrative headaches. Several election officials with whom we talked echoed the sentiment of the one official who said, "our ENR system is our largest and most vulnerable threat surface to cyberattack. I would prefer not to do it at all."

On the other hand, election officials are increasingly responding to the mis- and disinformation environment by redoubling efforts to have all queries about election administration come from official sources. This has been most visible in recent months in push-back observed by state election officials against civic-tech groups that have begun pushing email and text notices to voters containing information related to how to vote. Election officials claim that this information is often inaccurate and misleading to voters, causing administrative headaches to election officials and potentially disenfranchising the voters that the civic-tech groups are aiming to help. The same principle can be applied to election returns, however. If one is concerned about the public receiving incorrect information about elections, and is bent on encouraging the public to get election information only from official sources, then states and localities have no option other than to maintain highly visible Web-based ENR systems.

To let the "antis" have the final say, the last point has been rebutted by some election officials we spoke with, with words to the effect, "if we can't trust the Associated Press to report election results accurately, we're in big trouble." The media organizations that report election-night results place a premium on achieving both accuracy and speed simultaneously. The presence of multiple organizations reporting the same information increases opportunities to spot errors and spreads risks about mistakes or malicious activity leading to inaccurate reports.

b. The canvass

This tour has focused on the election-night reporting process, but there is a related process that unfolds at a slower pace. We refer here to the canvassing process that leads eventually to certification of results by the responsible authorities, at both the local and state level. The canvassing process is designed to build on the election-night results, by checking that those results were correctly collected and recorded. In addition,

disputes are resolved over provisional ballots and outstanding absentee ballots during the canvassing process.

The canvass is relevant here for at least two reasons. Most obviously, the canvass is the process that produces the official results that are ultimately certified and result in the winner taking office. Canvassing occurs under a less hectic timeline than election-night reporting, although in some cases, it may nonetheless finish up by Friday of election week.[31] An important difference between the canvass and the election-night count, however, is that it often takes place out of the direct scrutiny of the public. Thus, as the election-night count is updated because of new information uncovered during the canvass, it may not be clear why those numbers have changed. It is this quasi-mystery through which ballots can be "found" and counts adjusted that can provide fodder for conspiracists or those who would sow discord and confusion of the legitimacy of the count.

Virginia is one state—perhaps the only state—that tries to counter the problem of the "post-election-night-mystery" by making it as transparent as possible.[32] Since the state election of 2005, the Virginia board of elections has posted a "change log" file that accounts for every change to the publicly reported vote totals after election night, for every election in the state.[33] We will revisit this innovation in our conclusion.

The process we have just described is highly stylized, and would need to be adapted to local circumstances in order to describe any given state accurately. Part of the process we have elided in this discussion has been the counting of mail ballots. For purposes of discussing Figure 1, we can treat the place where mail ballots are counted as just another precinct, at least in states where they are counted separately.

---

[31] *See, e.g.*, OKLA. STAT. tit. 26, § 26-7-136 (2017).
[32] *See* Edward Foley & Charles Stewart III, Explaining the Blue Shift in Election Canvassing, 22 (MIT Political Science Dep't, Research Paper No. 2015-21), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2653456.
[33] *Results/Reports*, VA. BD. ELECTIONS, https://www.elections.virginia.gov/resultsreports/ [https://perma.cc/AXA5-ZFTT].

c. Mail-ballot election results

Two features of mail-ballot election returns bear mentioning. First, in some states mail ballots are counted outside the view of the public. In at least a few states, localities are allowed to open and process mail ballots before the polls close, and even sometimes scan and tabulate them. When the tabulation occurs before the polls close, the process must proceed under strict secrecy. Part of that secrecy, by its nature, excludes public observers. Second, the pre-processing of mail ballots allows local jurisdictions that do it to begin announcing partial election returns the instant the polls close. (The same can be said when votes from early voting centers can also be tabulated ahead of the close of polls on Election Day.)

To the degree that absentee and early in-person voters may have different voting patterns than Election-Day voters, this can set up a situation in which the earliest vote tallies released to the public can bear little resemblance to the final vote totals announced by a local jurisdiction, either on election night or in the certified totals. Indeed, in the 2016 presidential elections, Democratic-identifying voters were slightly more likely to vote by mail than Republican-identifying voters.[34] Naïve observers in states that allow absentee ballots to be counted before the polls close may be in for a big surprise as they follow election-night returns.

In addition, the immediate release of mail and in-person early votes can cause inaccuracies in communicating just how many votes remain to be counted. News accounts of election-night returns regularly include a statistic to track "percent of precincts reporting." However, there is no commonly agreed-upon method for calculating this statistic; it is often based on nothing more than counting up the number of precincts from which votes have been released—even if all the ballots associated with the precinct have not be counted—and dividing by the number of precincts in a jurisdiction.

Many counties that release initial reports of tabulated mail and in-person

[34] Foley & Stewart, *supra* note 32, at 15.

early votes as soon as polls close, and do not allocate those votes back to the precincts where voters reside, resulting in a confusing eventuality of perhaps hundreds of thousands of votes having been reported but with 0% of precincts reporting. Alternatively, some counties do allocate those early votes back to the local precincts, creating the potential for it to appear that 100% of precincts have reported, even though each precinct has reported only a partial count of votes.[35]

d. The press reports election results

In the previous section, we reviewed the flow of information about election results from the polling place to the state elections department, with the intermediate stop in the local election jurisdiction. At every stage of the process, there is an opportunity for the public to observe the data being reported, and to take part in disseminating it. While there are political junkies who hang out at county courthouses and local polling places on election night to be the first to see the election returns roll in, for the most part, "the public" is actually "the media." Therefore, it is valuable to consider the role of the media in reporting election results, on election night and the days beyond.

National and local media organizations deploy a highly decentralized information-gathering and dissemination system whenever a federal election is held.[36] Because our empirical interest lies mostly with federal and top state offices, we focus here on the systems that are deployed for biennial federal elections. We further focus on national systems, leaving aside state-specific networks that might be developed to gather and disseminate information about state and local election returns.

Between 2003 and 2016, all the major news networks (Associated Press, ABC, CNN, CBS, Fox News, and NBC) joined forces under the

[35] We return to this point in our conclusions and recommendations. There is no obvious best way to report an estimate of the number of votes waiting to be counted; any plausible way can be misunderstood or misrepresented.

[36] Of course, analogous systems are deployed for smaller-scale state and local elections.

umbrella of the National Election Pool.[37] Under this arrangement, Edison Research conducted exit polls and helped provide information necessary to "call" particular races; the Associated Press aggregated data about vote tabulations.[38] This consortium broke up in 2017, yielding two separate coalitions of media players. These are organized around Edison, which added vote-tabulation to its portfolio, and the Associated Press, which formed the nucleus of the second major coalition.[39] Edison provides the vote tabulation data for the National Election Poll, which in 2018 included NBC, ABC, CBS, and CNN. In 2018, the Associated Press led group included Fox News, *New York Times,* Politico, *Wall Street Journal,* and *Washington Post.* Despite this schism, these new coalitions operate in a manner similar to the old regime, so for this discussion we will use language that is compatible with the media landscape in 2016.

The purpose of these national data-gathering systems is to assist news organizations covering the unfolding election on election night and beyond. To that end, the National Election Pool was responsible for feeding three major streams of data to the reporting organizations: exit polls, election returns, and supporting data, such as past vote returns, demographic information, and election laws.[40] It was (and remains) the job of the various news network "decision desks" to take these data streams and process them into information that was useful for covering the returns. The most visible activity, and the one most relevant to this paper, is "calling" a race in favor of a candidate, in light of the information received. But the data are also used for other important

---

[37] Michael Mokrzycki, National Election Pool (NEP), *in* ENCYCLOPEDIA OF SURVEY RESEARCH METHODS (Paul J. Lavrakas ed., 2008).

[38] *Election Polling*, EDISON RES., https://web.archive.org/web/20161110154555/http://www.edisonresearch.com/election-polling/ (last visited Jan. 9, 2020). Edison began exit polling in 1996. The year 2002 represented the creation of the NEP, which combined Edison's exit polling operation and the AP's vote-tabulation collection efforts.

[39] Steven Shepard, *Is this the Beginning of the End of the Exit Poll?,* POLITICO (Dec. 9, 2017), https://www.politico.com/story/2017/12/09/exit-polls-election-day-frustration-287913 [https://perma.cc/VC9U-ZMLV].

[40] *Election Polling*, EDISON RES., https://web.archive.org/web/20161110154555/http://www.edisonresearch.com/election-polling/ (last visited Jan. 9, 2020).

purposes, including reporting about demographic, geographic, and other trends that help interpret election results and round out the broader election story.

The exit poll information comes from surveys conducted in hundreds of precincts from around the country. In a presidential election year, precincts may be chosen from every state, although economic constraints have sometimes limited geographic coverage in recent years to a subset of more electorally competitive states. In addition, because more ballots have been cast before Election Day, by mail and in early-voting sites, the exit poll now has a component that samples early voters from administrative data. In 2018, the exit poll sampled approximately 700 precincts, garnering 80,000 interviews from 32 states.

National exit poll results are embargoed from public view until 5:00 p.m. Eastern Time, and are never used to "characterize" a particular race before the polls close in that state.[41] Although data from the exit polls can be used to help call the outcome of an election, its primary utility is to help understand turnout dynamics and to explore the policy and issue attitudes of voters. The media members of NEP were also provided with election returns in real time on election night.[42] This information was primarily at the local jurisdiction level—county or municipality, depending on state—but sometimes at the precinct level, when available.

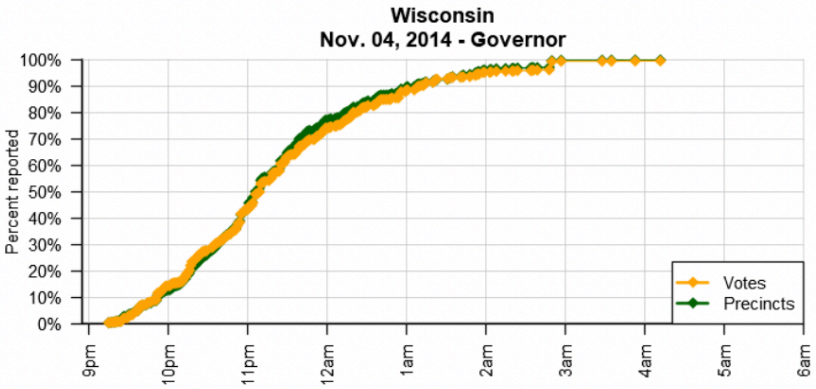
The election return information on election night is received by the news organizations soon after the polls close. Figures 2 – 4 help to illustrate the recent pattern in Wisconsin.

---

[41] Peter Marks & Bill Carter, *The 2000 Elections: The Network Predictions; Media Rethink an Urge to Say Who's First,* N.Y. TIMES, B1 (Nov. 9, 2000), https://www.nytimes.com/2000/11/09/us/2000-elections-network-predictions-media-rethink-urge-say-who-s-first.html [https://perma.cc/SP7A-H6C4].
[42] *Id*.

Figure 2. Time path of receipt of vote-return report from Wisconsin, November 2014 gubernatorial election (Source: Associated Press)

a. Cumulative percentage of votes received and precincts reported.



b. Democratic vote margin.

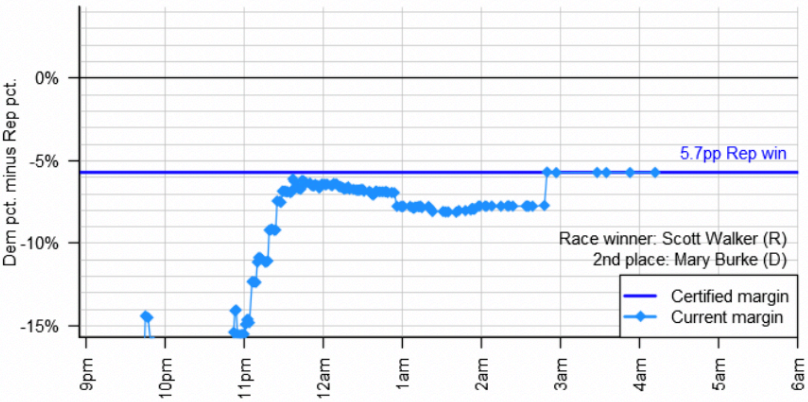
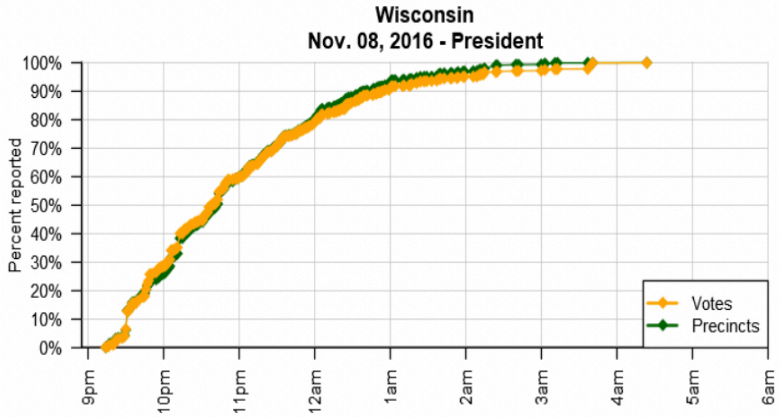


Figure 3. Time path of receipt of vote-return report from Wisconsin, November 2016 presidential election (Source: Associated Press)

a. Cumulative percentage of votes received and precincts reported.



b. Democratic vote margin.

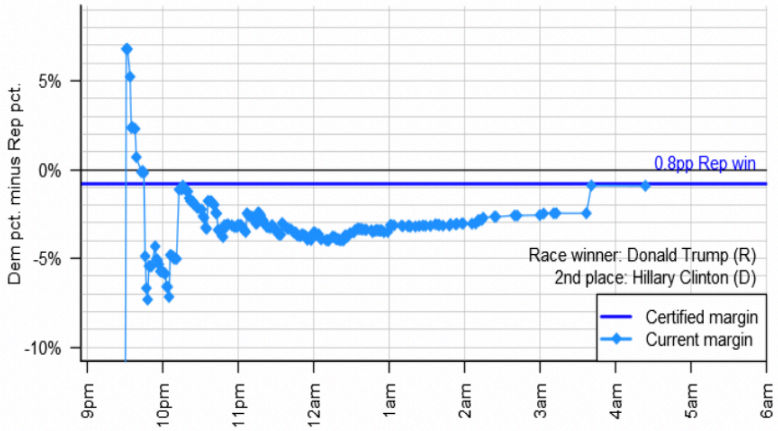
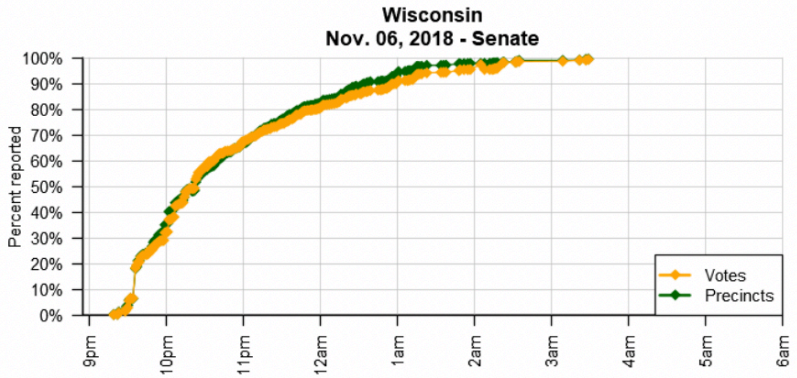
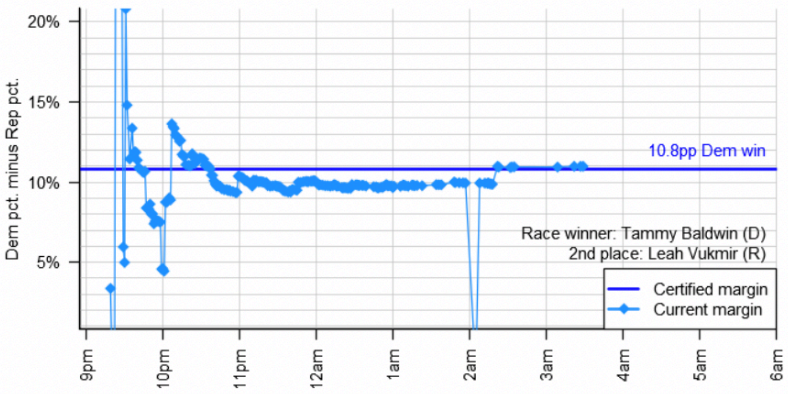


Figure 4. Time path of receipt of vote-return report from Wisconsin, November 2018 U.S. Senate election (Source: National Election Pool)

a. Cumulative percentage of votes received and precincts reported.



b. Democratic vote margin.



Looking at the top half of each figure, there are clear patterns in how often updates are received and how quickly the votes are counted, even across election cycles. The polls in Wisconsin close at 9:00 p.m. Eastern Time.[43] The first report of votes is usually received between 9:15 p.m. and 9:30 p.m. Wisconsin typically finishes counting by around 3:00 a.m. Wednesday morning. The two lines, one showing the cumulative proportion of votes (using the final, certified vote count as the denominator) and the other the cumulative proportion of reported precincts suggests that the mix of precincts reporting throughout the night tends to mirror the distribution of precinct sizes in the state. In other words, "small" precincts do not report at one time of the evening and "large" precincts at another.

The bottom half of the graphs shows the margin between the Democrats' and Republicans' vote percentages at each point in the night. The solid, horizontal dark blue line shows the final, certified vote margin. Once again, there are stable patterns in the vote margin across elections, even though the overall level—high, indicating the Democrat is doing well, or low, indicating the Republican has the advantage—may change. In the first hour or so, the vote percentages tend to be volatile, because the number of votes reported is so small. The volatility tends to dissipate when around fifty to sixty percent of the eventual election-night vote has been counted, which typically occurs in Wisconsin between 10:30 p.m. and 11:30 p.m Eastern Time.

There is also a pattern to their stabilization, in that once the volatility has resolved, the series stabilizes around a percentage point or two of the final certified total, in favor of the Republican candidate. The reason for this pro-Republican tilt in the vote, compared to the final certified total, is that Democrat-heavy Milwaukee County tends to report its mail-in absentee ballot numbers much later than the results in most of the rest of the state. This abruptly shifts the vote margin in a pro-Democratic direction.

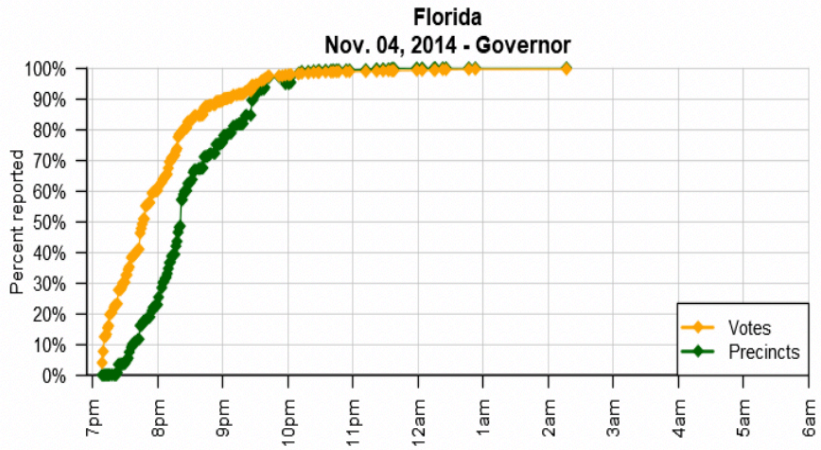
[43] All times are Eastern Time, regardless of the time zone from which the returns originate, because that is the time stamp on the data server.

The 2018 graph (Figure 4) also illustrates how election-night report is imperfect and can be subject to human error. Around 2:00 a.m., the data series spikes dramatically toward the Republican candidate, before being corrected a minute later. The reason for this is that new data was received from Milwaukee County, but the Democrats' and Republicans' vote counts were assigned to the other party's candidate. This error was quickly caught by the quality control procedures that Edison and the networks have in place, and was corrected. Errors in human entry of vote counts tend to be easier to catch when they are large and obvious. A massive shift in the vote percentage toward the Republican candidate in a heavily Democratic county is easily diagnosed to be a data entry error. Such errors are more difficult to diagnose in politically divided counties, where the vote percentages are closer to 50/50. In those cases, it may take longer to correct such an error, since additional steps must be taken to confirm that it is, in fact, an error.

Figures 5 – 7 help to illustrate both the commonalities and differences between states. One commonality is how quickly the initial vote returns are reported. In Florida, half the eventual votes that are counted are reported within the first hour after the polls close at 7:00 p.m. (Florida has two time zones. The closing of the central-time-zone precincts at 8:00 p.m. Eastern causes the discontinuity of the votes-counted part of the graph at that time). On the other hand, the cumulative proportion of *votes* counted rises much more rapidly than the proportion of *precincts* reported in the first hour when the data are transmitted.

Figure 5. Time path of receipt of vote-return report from Florida, November 2014 gubernatorial election (Source: Associated Press)

a. Cumulative percentage of votes received and precincts reported.



b. Democratic vote margin.

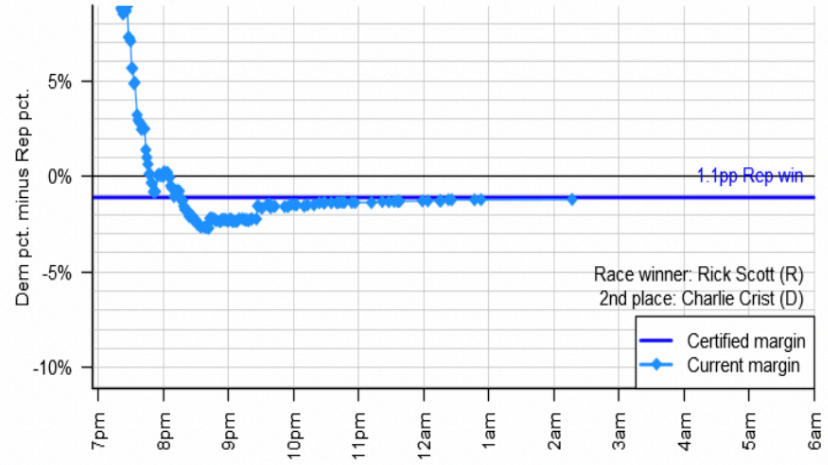
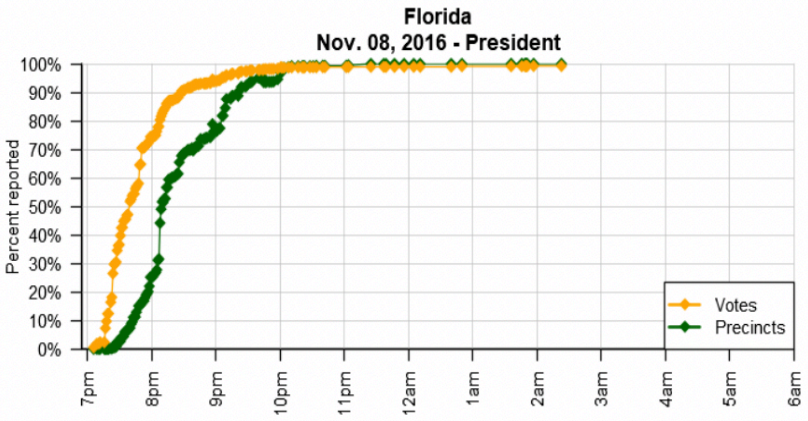


Figure 6. Time path of receipt of vote-return report from Florida, November 2016 presidential election (Source: Associated Press)

a. Cumulative percentage of votes received and precincts reported.



b. Democratic vote margin.

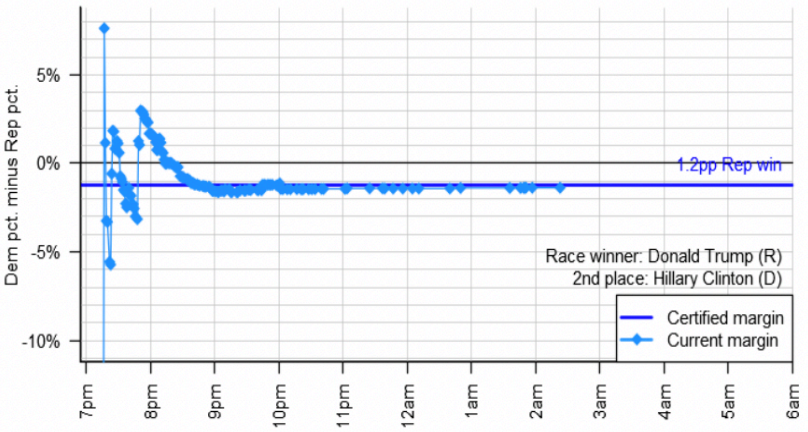
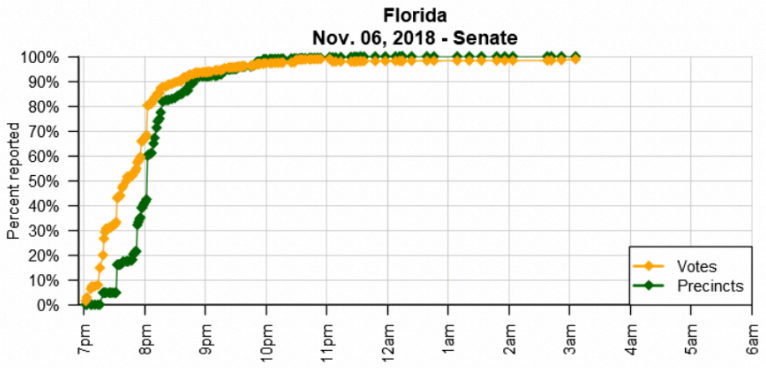
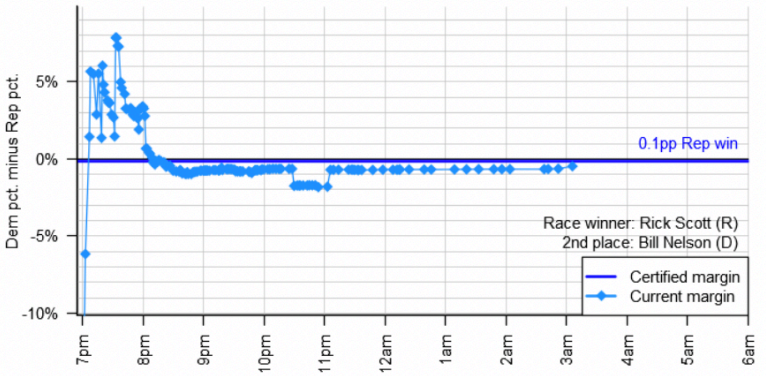


Figure 7. Time path of receipt of vote-return report from Florida, November 2018 U.S. Senate election (Source: National Election Pool)

a. Cumulative percentage of votes received and precincts reported.



b. Democratic vote margin.



This pattern highlights the way in which Florida reports its early in-person votes very quickly after its polls have closed, despite no Election Day votes having been counted. In 2016, there had already been 223,562 votes counted statewide before any county had reported even a single precinct of Election Day vote count data. The data show that because Democrats in Florida were more likely to vote early than Republicans, these initial vote reports were skewed toward Hillary Clinton, despite the fact that she lost the state.

The 2018 graph (Figure 7b) illustrates a different type of data error that can occur. In one county, a transcription error caused the votes of one

candidate to be reported as 320,000, rather than 230,000. This error was not as dramatic as the one we saw above in Wisconsin, but it was still significant, and took longer to be corrected. From the perspective of public confidence in elections, errors like this are extremely problematic, since correcting them requires changing the vote for one candidate but not the other.

Errors like this are also difficult to diagnose and correct because they can occur anywhere in the vote-reporting chain. The error could have been made on the Secretary of State's website. It could have occurred because the reporter taking the election return from the local election official over the phone transposed two digits, or the worker at the central reporting office transposed digits. Correcting an error such as this often requires figuring out where in the chain of communication the error has occurred, which can take more time to complete than simply identifying that the Republican and Democratic vote totals were swapped in a county in which one party is historically dominant.

IV. Counting Votes in Overtime, and the Growing Blue Shift

The process just discussed is most visible on election night, as the national media cover the onrush of election results pouring forth from the states. The counting and reporting of election results do not stop on election night, however. This is most noticeable when the network decision desks declare a race "too close to call" even as the Wednesday following Election Day dawns, such as in Florida in the 2000 presidential race or in Arizona's 2018 United States Senate election.[44] Yet even when the election night results allow the networks to comfortably declare a likely winner within minutes of the polls closing, the counting of ballots continues, as does the verification that any

[44] *See, e.g.*, Dartunorro Clark & Doha Madani, *Democrat Kyrsten Sinema wins Arizona Senate race after nail-biter against Martha McSally,* NBC NEWS (Nov. 12, 2019), https://www.nbcnews.com/politics/politics-news/democrat-kyrsten-sinema-wins-arizona-senate-race-after-nail-biter-n935206 [needs permalink].

original counts were correct. This is the canvassing process that eventually leads to the certification of the election.[45]

Edison and the Associated Press initially track the changing vote totals actively, as legal ballots that had been in hand but not counted on Election Day are incorporated in the count, as newly arriving mail ballots are counted (in states that allow ballots postmarked on Election Day to still be counted if they arrive by a certain deadline), and as provisional ballots are accepted and counted. However, unless a particular race has elicited national interest because of its closeness or because the national networks have not declared a presumptive winner, the public tends to assume that the vote counting has ceased. Of course, for the most part, it has not. Each level of government that has responsibility for overseeing election-result reporting is given a deadline to accomplish its work.[46] Those deadlines for local election jurisdictions range from the virtually instantaneous, as in New Hampshire,[47] to one month after Election Day, as in California.[48] These local certification deadlines introduce the possibility that information about election returns will dribble out over time, and that the quality of the data that dribble out may not be constant throughout the vote-certification period.

This leads to an important empirical fact. For the past two decades, in most states, votes counted and reported in the days following the election have tended to skew more heavily toward the Democratic Party than votes reported on Election Day. This phenomenon has been termed

---

[45] Of course, in rare cases, certification leads to contests and recounts. The principles we are about to discuss apply in those cases, although the numbers are typically very small.

[46] The National Association of Secretaries of State publishes a website that details the canvassing deadlines for every state. *See State Election Canvassing Timeframes and Recount Thresholds*, NAT'L ASS'N SECRETARIES ST. (Oct. 2018), https://www.nass.org/resources/2018-election-information/Canvassing-Timeframes-and-Recount-Thresholds [https://perma.cc4Q67-RSEB].

[47] Although localities typically transmit their results to the state by Friday following Election Day, state law gives them until the following Monday. *See* N.H. REV. STAT. ANN. §§ 659:75, 659:81, 659:84 (2019).

[48] Cal. Elec. Code §§ 15301, 15374, 15500, 15503, 15504 (West 2019).

the "big blue shift" by Edward Foley, who first identified it in print in a 2013 article.[49]

To illustrate the phenomenon, we need two measures. The first is the size of the "overtime vote," which is defined as the number of votes counted after Election Day. The size of the overtime vote is calculated by subtracting the number of votes reported in the presidential election in the Thursday edition of the *New York Times* immediately after Election Day, from the number of votes recorded in the final certified results of the election.[50] The size of the overtime vote is expressed as a percentage of the initial vote. For instance, if the *New York Times* reports results from a total of 1 million votes in a state on the Thursday after Election Day and then the state certifies results with a total of 1.5 million votes, the size of the overtime vote is 50%.

The second measure is the "partisan shift," which is defined as the percentage of the two-party vote received by the Democratic presidential candidate in the final certified count minus the percentage of the two-party vote received in the initial Thursday count as reported by the *New York Times.* For instance, if a state reports a certified vote of 58% for the Democratic candidate but the two-party vote for the Democratic candidate had been reported as 56% on the Thursday after Election Day, the size of the partisan shift is -2 percentage points. The partisan shift measure is constructed such that positive values indicate the Democratic candidate received a larger percentage of the two-party vote than the Republican candidate, and vice versa. Because positive values of the partisan shift are associated with Democratic gains, we sometimes refer to this as the "blue shift," although some states do exhibit a "red shift."

Figure 8 illustrates the blue shift from the past two presidential elections. Because the two measures are heavily skewed, we have plotted values of the overtime vote and blue shift on proportional scales

---

[49] Edward B. Foley, *A Big Blue Shift: Measuring an Asymmetrically Increasing Margin of Litigation,* 27 J.L. & POL. 501, 520 (2013).

[50] The decision was made to use Thursday after Election Day as the baseline instead of Wednesday in order to account for publication deadlines of the *New York Times*, especially in the years before the advent of the Internet.

to aid in legibility. To use 2012 to illustrate how to read the two graphs, focus on Washington state, which is at the extreme "northeast" portion of the graph. Washington's final certified vote count in 2012 accounted for 3,046,066 two-party votes; the initial vote reported by the *New York Times* accounted for 1,885,172 two-party votes. The size of the overtime vote is (3,046,066 – 1,885,172)/1,885,172 = 62%, which is the *x*-axis value for Washington. Washington's certified vote gave the Democratic nominee, Barack Obama, 57.6% of the vote two-party vote; the initially-reported two-party vote share for Obama was 56.4%. The size of the partisan shift (or blue shift) is 57.6% - 56.4% = 1.2 points, which is the *y*-axis value graphed for Washington.

Figure 8. Size of Blue Shift and Overtime Vote, by State, 2012 and 2016

Data sources: Election returns for the initial vote count were taken from the *New York Times* on the Thursday immediately following Election Day. (Data from 2016 were taken from the *Washington Post*.) Final vote counts were taken from various editions of *America Votes*. (Data from 2016 were taken from Dave Leip's Atlas of Presidential Elections, https://uselectionatlas.org/).

As the two graphs in Figure 8 illustrate, it is generally the case that as the size of the overtime vote grows in a state, so does the size of the partisan shift. The proportional scales obscure a second important pattern, which is that for most states, the size of the overtime vote and the magnitude of the partisan shift are relatively small. In 2016, for instance, the median value of the overtime vote was 1.1%; the median size of the blue shift was 0.056 percentage points.

The article by Foley and the working paper by Foley and Stewart provide more detailed analysis about the history and causes of the growth in the overtime vote and the accompanying blue shift.[51] From the perspective of this article, the important thing to note is that the size of the overtime vote has grown since 2004, and the value of the blue shift has clearly favored Democrats since 2008, after a five-decade period in which the partisan shift balanced out between the two major parties, so that the average nationwide value of the partisan shift measure had hovered around zero.

With the size of the overtime vote growing, opportunities grow for there to be controversy over the vote count, especially in races where the initial vote was close and the partisan tilt of the overtime vote was substantial. A good example in recent years was the 2018 United States Senate race in Arizona. At 6:00 a.m Eastern Time, the morning after Election Day, the Republican nominee, Martha McSally, held a 0.87-point lead in the two-party vote over the Democratic nominee, Kyrsten Sinema.[52] However, the initial count only accounted for 72% of all the ballots cast. The overtime ballots remaining ended up favoring Sinema by 11 points. In the end, Sinema defeated McSally, with 51.2% of the two-party vote.

During the period between Election Day and the release of the final count, President Trump tweeted, "Just out — in Arizona, SIGNATURES DON'T MATCH. Electoral corruption - Call for a new

[51] *See* Foley, *supra* note 49; Foley & Stewart, *supra* note 32.

[52] These numbers come from the Election Day vote tabulation calculated by Edison Research on behalf of the National Election Pool (NBC, ABC, CBS, and CNN).

Election? We must protect our Democracy!"[53] The claim about signatures not matching was probably in reference to a lawsuit filed by the Arizona Republican Party over the varying "cure periods" across Arizona's counties for mail ballots (the largest county in the state, Maricopa, allowed five days to cure signature problems with mail ballots. Many of the smaller, rural counties required signature-match problems to be resolved by Election Day). Democrats and Republicans reached an agreement to extend the cure period in the smaller (and more Republican) counties, so the lawsuit was dropped. However, the fact that the results of the election hinged on the counting of absentee ballots, that the absentee ballots were heavily favoring the Democratic candidate, and that Democratic and Republican parts of the state followed different rules about curing signature non-matches gave an opportunity to President Trump to cast doubt on the legitimacy of the election, and to suggest that the election be done over.

In the Arizona case, the Republican candidate herself failed to take the bait, post-election lawsuits were settled through negotiation, and in the end the results were not challenged by the loser. The mainstream Arizona media covered the ongoing counting in a businesslike manner. The Arizona Secretary of State adopted a media strategy that highlighted the regularity of the absentee-ballot-counting process and communicated updates to the vote count on a strict schedule that was announced ahead of time. Thus, the overtime vote count in Arizona was a success story overall. However, one can imagine another candidate not playing the overtime period so coolly, using social media to stoke doubts about the fairness of the process and whipping their followers into a frenzy.

The overtime vote continues the dynamic unfolding of election results witnessed on election night, but on a different time scale. Two things make the overtime vote different from the election night returns in ways that influence the vulnerabilities of the system that reports election results to the public. First, the election night narrative is generally easier

---

[53] Donald J. Trump (@realDonaldTrump), TWITTER (Nov. 9, 2018, 3:33 PM), https://twitter.com/realdonaldtrump/status/1060993836984324096?lang=en [https://perma.cc/SFS4-3UM3].

to tell in terms of regular administrative practice. Polls close, votes are counted right away, and those votes are reported to the public. In contrast, when ballots have yet to be counted in the days following the election, questions arise about why the ballots were not counted on Election Day, and why/how they were "found." Stories about the cure periods of provisional ballots and disputed mail ballots are not as straightforward as the election night stories about the returns coming in.

Second, although there are temporal dynamics to the pace at which the votes are reported on election night, creating a horse-race feel in the few hours right after the polls close, the ups and downs of the candidates as the votes come in are typically explained in terms of well-known political geography—Democratic big cities reporting, downstate Republican counties reporting, etc. The explanation for why the post-election-night count skews toward one party or the other requires reference to more abstract facts, such as the composition of the provisional ballot and mail ballot pools. And, once those votes skew to one party or the other, it encourages supporters of the party on the disadvantaged side to wonder why provisional and mail voters did not vote the way they were "supposed" to on Election Day, or did not follow the rules they were supported to follow.

V. Assessing Vulnerabilities in Reporting Election Results

The previous sections sketch out the processes that result in information about election returns being communicated to the public. Where are the vulnerabilities to be found?

We can identify two general classes of vulnerabilities with the election-reporting system itself, which we term *static* and *dynamic.* Static vulnerabilities are those that pertain to static features of the vote-reporting system. These might include vulnerabilities to Internet-connected components of the ENR reporting system, such as the ones that led to the malicious attacks in Ukraine. Or they might include mundane problems of information transmission, such as mishearing a vote total over a phone line or mistyping a number into a computer.

Dynamic vulnerabilities are those that occur because the information about election returns is not revealed instantaneously, but across a period of time. First, information is revealed across time, and is not revealed randomly with respect to time. It may first be revealed from Democratic-leaning counties right after the polls close and then from Republican-leaning counties later in the evening. Or, Republican-leaning Election-Day ballots may be counted on Election Day and Democratic-leaning mail ballots may be counted in the following days. Second, every state of the data at any general time can be compared to the state of the data at different times, inviting attentive observers to draw inferences from changes themselves, even when they are not biased with respect to parties or candidates.

Attacking static vulnerabilities has been part and parcel of election administration from its inception and have been integrated into administrative practice. The very fact that election results may be incorrectly reported from a polling place, for example, motivates canvassing practices aimed at uncovering and correcting errors. Among these canvassing practices are careful accounting for all ballots used at a polling place, with the total number of votes reported to the local election office. These practices also include comparing results of the current election with past elections. Finally, the movement to increase the sophistication of post-election tabulation audits, such as risk-limiting audits, is motivated by a desire to identify a host of static errors that appear in the tabulation and reporting processes, and to correct them if the outcome of the election seems at stake.

Based on our direct knowledge of the vote-reporting system and interviews with election officials, we know that there is general awareness of information-technology-related vulnerabilities within the vote-reporting system. It is for that reason that *official* reports of vote totals generally are transmitted physically from place-to-place, and pains are taken to ensure that official data are not transmitted via the Internet. Memory cards and tally sheets are carried by hand from polling places to the local election office. Certified local-jurisdiction results are sent to the state capital by courier. A second copy of results may be transmitted electronically, to give officials at the receiving end a "heads up" about what to expect when the official reports are received, and to

serve as an independent source of information against which to compare the official results when they arrive.

The unofficial results are most often transmitted electronically, and are where the vulnerabilities may be greatest. Vote tallies may be uploaded via wireless modem from a polling place to the local election office.[54] A spreadsheet containing election return totals may be e-mailed from a local election office to the state. A jurisdiction's computer system can be subject to a DDOS attack, making the transmission of this information impossible to accomplish.

Although it can rightfully be said that interference with unofficial tally reports does not change official results, it is also the case that the public is paying the most attention to the informal information in the time immediately after an election. For that reason, breaches of ENR systems can be very dangerous to public confidence and legitimacy, even if they have no effect at all on the official vote count.

Dynamic vulnerabilities exist even in the perfect world in which all the static vulnerabilities have been solved. The narrative in this paper identifies four specific forms of dynamic vulnerability that seem particularly important. The first is the "natural" evolution of election results, either on election night or during the overtime period. The lead in the electoral horse race is likely to change in the course of an evening, dramatically at first, less-so over time. Furthermore, different pieces of election information may be reported on different time scales, suggesting that officials are manipulating the returns, even though they are not.

An example of this occurred on election night in 2004 in Ohio, when Cuyahoga County began reporting both precinct-level tabulation totals

---

[54] The use of wireless models to transmit election returns remains one of the sorest points of disagreement between election technology activists, on the one hand, and election officials and vendors, on the other. *See* Kevin Monahan, Cynthia McFadden & Didi Martinez, *Online and Vulnerable: Experts Find Nearly Three Dozen U.S. Voting Systems Connected to Internet,* NBC NEWS (Jan. 10, 2020, 6:36 PM), https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436[https://perma.cc/8L6G-EWXC].

for candidates and estimated turnout.[55] For much of the evening, the number of votes reflected in the tabulation totals for candidates vastly exceeded the turnout levels reported for the precincts, which led some to charges of "ghost voters" in the county.[56] This discrepancy was easily explained by the fact that the accumulation of vote tabulations occurred separately from turnout reports—the same precincts were not necessarily reflected in the two reports, and in any case, vote tabulations were being reported faster than turnout tabulations. Regardless of the benign explanation, for several hours on election night, close observers of Ohio election returns spent considerable time and energy chasing down the charge that election officials were stuffing the ballot boxes in that county.

Related to the dynamic nature of election-tabulation reporting is the second factor, which is the presence and correction of errors. Large, sudden changes to election margins are likely to draw attention. As much as we would like to think that large, sudden changes that return the time-path of the election results back to the previous equilibrium in correction of an error would be reassuring, the correction itself probably draws attention to the error in the first place. Is the correction just a correction, or is it evidence of a struggle over the information to be conveyed to the public?

The third dynamic vulnerability is the blue shift as identified above. Although we have no evidence that the blue shift is due to the manipulation of election results during the overtime period, its persistent size and increasing tilt toward one party invites questions about whether votes are being manufactured by partisan election officials.

The fourth vulnerability comes in considering the role of the exit polls. Currently, exit polls are rarely used by national news organizations to call the winner of a race on election night, except in cases where the exit

---

[55] Jake Tapper & Avery Miller, *Conspiracy Theory Abound After Bush Victory*, ABC NEWS (Nov. 9, 2004, 11:18 AM), https://abcnews.go.com/WNT/story?id=239735 [https://perma.cc/KL22-4FQR].
[56] *Id*.

poll data and prior expectations suggest that the vote spread between the top-two candidates will be overwhelmingly large. In the past, leaked midday results have muddied the waters about the accuracy of the final results, such as in 2004 when three media outlets published exit poll results during the day,[57] not to mention the controversy that arose later on when methodological problems caused the final results to be strongly biased in a pro-Democratic direction.[58]

The vulnerabilities identified here increase the likelihood for voters to be confused or misled by information about election results. The possibility for simple confusion starts with the fact that the public is largely unaware of the dynamic nature of election-results reporting outlined here. That ignorance is reinforced with little apparent knowledge of these dynamics among reporters covering election night.[59] This lack of knowledge is further reinforced by attitudes among candidates that election results should be released instantly, without any mistakes, and that any deviation from these expectations should be treated with suspicion. If the dynamics are covered at all, the starting point is to uncover why things are "fishy," with the most vocal voices inclined to ratchet-up the rhetoric.

The previous paragraph can, in some ways, be considered the best-case scenario. For starters, a significant minority of voters are predisposed to believe that election fraud caused by manipulating vote totals is common. In the MIT module of the 2018 Cooperative Congressional Election Study (CCES), for instance, 6.4% of respondents stated that they believed that stealing or tampering with votes in local elections was "very common;" another 21.3% stated it "occurs occasionally." With

---

[57] Robert Niles, *Exit Polls Bring Traffic Deluge, Scrutiny to Blogs, Slate*, ONLINE JOURNALISM REV. (Nov. 18, 2004), https://www.ojr.org/041105glaser/ [https://perma.cc/34YU-DX62].

[58] *See* MICHAEL W. TRAUGOTT, *The Accuracy of the National Preelection Polls in the 2004 Presidential Election*, 69 PUB. OPINION Q. 642, 643 (2005).

[59] It should be remembered by most reporters covering election results on election night, especially for non-national outlets, who do not normally cover elections as their beat. Even for those who cover elections on a regular basis, election administration is a corner of elections that is rarely covered; election night itself is a small slice of the overall coverage about which few reporters develop expertise.

reference to state elections, these percentages were 7.8% and 21.0%, respectively.[60] These attitudes are affected by partisanship. For the "state" version of the stealing or tampering question, for instance, 21.2% of Democrats said it was either "very common" or "occurs occasionally," compared to 39.6% of Republicans.[61] Furthermore, although no research has been conducted into how the reporting of election results affects attitudes toward fraud, we do know that there is a strong "losers effect" in voter confidence—supporters of losing candidates for president become less confident that their vote was counted as cast once the outcome of the election is known.[62]

Thus, not only do voters lack knowledge about how the vote-count system works, nor are they likely to be enlightened through news coverage, large numbers of voters are predisposed to be skeptical of reports of vote counts; news detrimental to one's favored candidate reinforces that predisposition. This means that raising doubts about vote counts as they are proceeding is ripe for manipulation in the hours and days following the election.

The technology of reporting vote counts is vulnerable to malicious attacks and errors, as are other computerized parts of the voting system. State and local election administrators have taken administrative actions and spent millions of dollars over the past four years to improve the resiliency of the technological component of the vote-counting system.

---

[60] Analysis conducted by the authors. These questions were asked in the pre-election wave of the survey, so were not yet contaminated by reference to a "sore loser" effect. Raw datasets to reproduce this analysis are available on the CCES Dataverse. *See* Charles Stewart, *Cooperative Congressional Election Study 2016 Team Module of Massachusetts Institute of Technology (MIT)*, HARV. DATAVERSE (2016), https://doi.org/10.7910/DVN/TIMWT4.

[61] Furthermore, regression analysis reveals that Democrats were much more likely to believe that vote tampering or stealing was common in highly Republican states, whereas attitudes of Independents and Republicans were unrelated to the partisanship of the state. (Partisanship in this case is measured by the percentage of the two-party received by Clinton in 2016. Regression results are available from the authors upon request.)

[62] Michael W. Sances & Charles Stewart III, *Partisanship and Confidence in the Vote Count: Evidence from US national elections since 2000*, 40 ELECTORAL STUD. 176, 183 (2015).

Because it must at some point come in contact with the Internet, election-night reporting presents the widest threat surface for election administrators. And yet, the technical vulnerabilities may not be the most consequential. The temporal dynamics of election returns, both on election night itself and in the days following, present opportunities for malicious actors—hackers and propagandists—to manipulate voters' understanding of those dynamics in destructive ways. Although we cannot put a firm number on it, it is our sense that this latter set of vulnerabilities, which surround the communication of election returns, is a greater source of danger for the functioning and legitimacy of the American system of election administration.

VI. What Is to Be Done? Protecting against Vulnerabilities

The cybersecurity framework developed by the National Institute of Standards and Technology to help organizations improve cybersecurity practices in order to manage security risks identifies five "concurrent and continuous" functions:[63]

1. *Identify* risks by developing "an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities."[64]
2. *Protect* assets by developing and implementing "appropriate safeguards to ensure delivery of critical services."[65]
3. *Detect* anomalies by developing and implementing "appropriate activities to identify the occurrence of a cybersecurity event."[66]
4. *Respond* to detected incidents.[67]

[63] U.S. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 3 (vers. 1.1).
[64] *Id*. at 7.
[65] *Id*.
[66] *Id*.
[67] *Id*. at 8.

5. *Recover* from incidents through plans that provide for "resilience and . . . restore any capabilities or services that were impaired due to a cybersecurity incident."[68]

We offer these concluding comments in light of these categories in the framework.

a. Identification

Most of this paper has been aimed at identifying the vulnerabilities that lie in the domain of election-result reporting. Those vulnerabilities reside both within the narrow domain of election administration, in the administrative units responsible for conducting the election and reporting the results, and outside of election administration, in the network of institutions and individuals who report election results to the public. Within election administration, the primary challenges are static vulnerabilities that affect whether information will be recorded and transmitted accurately, and whether malicious actors can influence the flow of information within the formal system and between the formal system and the greater society.

The practice of election administration has focused on identifying and remediating vulnerabilities in the tabulation-reporting function for over a century. Decision-makers and policymakers have been slow to recognize the vulnerabilities that lie in the use of information technologies, and the degree to which they constitute threats to be managed. (The history of the use of automation technologies in election administration has emphasized its role in reducing clerical errors and increasing speed; it has taken a long time to recognize the attendant costs and to weigh benefits against those costs.) At the same time, it must be acknowledged that computer professionals and election officials often profoundly disagree over how much risk is created by the reliance on information technologies to manage information flow in election administration. This is especially true as we move away from obvious "computer systems," such as outward-facing servers and other

[68] *Id*.

equipment connected to the Internet, and approach dedicated voting equipment that has computerized components.

Less attention has been paid into identifying vulnerabilities related to the interface between election administration and the public. There is no doubt that there are technological vulnerabilities among the news organizations' computer systems that exist independent of reporting on elections.[69] More fundamentally, though, the vulnerabilities that exist in this area are probably not technical—that is, related to static problems—and more likely to be social. These vulnerabilities include lack of knowledge about the vote-reporting system by news-gatherers and the general public, plus the partisan lens through which the public perceive news about politics, including election returns.

Our own sense is that although it may be theoretically possible to maliciously manipulate election results on election night or in overtime, it is very unlikely. As with most things in American election administration, our assessment on this point starts with the distributed nature of what is being administered. Certainly, with over 100,000 precincts in the United States, averaging approximately 2,000 per state, launching a malicious attack against the returns at the source seems especially unlikely. The likelihood that a malicious attack against central-count tabulation systems would be successful may be higher, but the greater inherent vulnerability of these systems is already dealt with through imposing significantly higher barriers barring physical access to these systems than exist in accessing systems that tabulate votes in precincts and early-vote centers. Using remote electronic means to

[69] One sign that news organizations are part of the ecosystem of election reporting, and that their potential computer vulnerabilities are a matter of concern, is that the Associated Press's elections reporting unit is a member of the Sector Coordinating Council for the Election Infrastructure Subsector. *See* Press Release, Dep't of Homeland Sec., Readout of DHS Meetings with State Election Officials and Other Election Sector Partners (Feb. 19, 2018), https://www.dhs.gov/news/2018/02/19/readout-dhs-meetings-state-election-officials-and-other-election-sector-partners [https://perma.cc/8YQK-TQEQ].

launch a wholesale attack against the *official* returns at the source seems virtually impossible, regardless of the source.[70]

Of course, the vulnerabilities are greater with the unofficial reporting pipeline, since information sometimes goes through unsecured channels. In addition, although there are hundreds of precincts in the average local election jurisdiction, there is only one election office. It may be hard to hack the distributed system, but the single point at which reports from polling places are directed may be a more inviting target for actors with malicious intent.

b. Protection

The "easy" protection solutions—at least to articulate—are those that impose controls over access to the systems that tabulate, record, and disseminate information about vote totals. The core list of protections is relatively short and well-known—strong passwords, multi-factor authentication, firewalls, and air-gaps. Other protections are social, such as having in place systems that provide for independent verification of results before they are released into the wild.

Although there are clearly limits to the utility of public education, it is also clear that education plays an important role in protecting against the vulnerabilities of confusion, misinformation, and disinformation. This education starts with those in the media who cover and report election results.

Related to education are the strategies that the media employ to inform the public about the status of election results at any given time. Attention needs to be paid by the media, first, to how the number of outstanding ballots is reported. Because of the growth of non-traditional modes of voting, such as early in-person or mail-in ballots, the practice of reporting the percentage of precincts reporting needs to be rethought, by both election officials and the media. What should replace it, on the

[70] Of course, fraud has been perpetuated against hand-written election-return records. Nothing we write here is intended to diminish the possibilities of old-fashioned election fraud in any given election. Our point on the matter, however, is that the protections against election tabulation fraud at the source have been designed to combat these older methods of stealing votes.

other hand, is unclear. Expressing the status of the vote count in terms of percentage of ballots cast is conceptually superior to the old precinct-percentage measures, but is also fraught with opportunities for misunderstanding and disinformation. What happens, for instance, when the forecast of ballots to be counted produces an under-estimate, resulting in reports that more than 100% of ballots have been counted, with more to come? Or when the forecast of total ballots is adjusted upward, causing the percent of votes counted to drop?

In 2016, the *New York Times* introduced the "needle" to reflect its prediction of who would win the presidency, and particular states.[71] One feature of the needle, that it fluctuated in proportion to the uncertainty of the forecast, is close to what we have in mind as one implementation of this idea. The *Times* election-night forecasting page had other graphical representations of the uncertainty of their results, which were primarily a function of the number of outstanding ballots in proportion to the estimated margin.[72]

The most direct ways to provide information that guards against premature finality probably require two major activities on behalf of election officials. First, election officials should make every effort to accurately report the number of outstanding ballots left to count late on election night, along with a characterization about where the outstanding ballots are likely to come from. For many local jurisdictions, this will add work on a very hectic election night, but providing this information will help to start communicating with voters the contingent nature of the results that are being reported.

Second, states should consider adopting Virginia's change-log process, to account for changes to election results after election night. Again, this

---

[71] Nate Cohn, Josh Katz & Kevin Quealy, *What is the Election Needle?*, N.Y. TIMES (Feb. 3, 2020), https://www.nytimes.com/2020/02/03/upshot/needle-iowa-caucuses-faq.html [https://perma.cc/336N-PCBV].

[72] *Live Presidential Forecast,* N.Y. TIMES (Nov. 9, 2016), https://www.nytimes.com/elections/2016/forecast/president [https://perma.cc/6D58-B2VM]. Of course, the idea of forecasting the results through a graphical interface that appears "scientific" may also have the negative consequence of suggesting a false sense of precision.

would create additional work for local and state election offices, but it would provide the benefit of proactively managing information about the change in the vote returns after Election Day.

To argue against these proposals, it is possible to argue that to some degree, *less* transparency is called for. (At least the idea should be entertained for further discussion.) By "less transparency," we mean less attention paid by local and state election offices to reporting unofficial election returns via online ENR systems. This would not shut out the public altogether, since the Associated Press and Edison, would still be in the business of gathering election returns themselves and reporting them unofficially. But, this reporting would now be clearly unofficial, providing the public perhaps less reason to regard preliminary figures as definitive.

Finally, a discussion needs to be started about "calling" the outcome of elections before all the ballots have been counted. On the one hand, it is possible that the announcement by media organizations that a candidate is the "likely winner" of a state is heard by viewers as a factual statement, not a forecast.[73] On the other hand, the networks *do* refer to the candidate as the "projected winner." The problem may not be the practice of "calling" states for candidates, as much as it is in communicating that a "call" is contingent on assumptions about the accuracy of the data that the state provided, which could change during the official canvass.

Discouraging networks from identifying candidates as projected winners would accomplish little to reduce the risks associated with election-result reporting. News organizations are unlikely to all agree to restrictions and, in any case, the projections are news that should be

[73] In the postmortems following the 2000 presidential election, news executives engaged in soul-searching over the consequences of prematurely declaring a likely winner and the cascade of events that followed as a consequence. *See* Peter Marks & Bill Carter, *Media Rethink an Urge to Say Who's First,* N.Y. TIMES, Nov. 9, 2000, at B1. We know of no political science research that studies how attitudes are changed when news organizations declare a candidate the "projected winner" of a state. Having research directly on the topic would help to clarify whether declaring candidates projected winners is actually a problem worth addressing.

reported. News organizations should be encouraged, on the other hand, to provide the evidence to the public that has led to the projection at the time the projection is made, and to specify the circumstances that could result in the projection being in error.

c. Detection

Detecting cyber-intrusions into computer systems used in election administration has been one of the chief topics of election security over the past four years, and we have nothing of substance to add to those discussions, especially to the degree that detection is premised on monitoring the nature of the information packets directed to that system via networks, or to the behavior of the computers being used.[74] Considerable attention has also been paid to detecting efforts at pursuing information operations strategies in elections. Nor does this paper have anything directly to add to that discussion.

However, our analysis here does suggest some conclusions about detecting successful intrusions into the system of reporting election results. The methods the national news organizations use to judge the quality of the election data flowing into their decision desks provides an important bulwark against compromising that data, and would likely catch successful attempts to manipulate results that would have a material effect on the election outcome.

The nature of this protection is illustrated above in the time series that recorded election-night election-return dynamics from Wisconsin and Florida. As these two sets of graphs suggest, election-return information flows into the national news operations in streams that follow historical patterns that are distinct for each state. While we have not explored the issue directly, we suspect that these historical patterns pertain to local jurisdictions, as well.

---

[74] The Center for Internet Security hosts a suite of resources that address technical approaches to election cybersecurity. *Election Security Best Practices*, CTR FOR INTERNET SEC., https://www.cisecurity.org/elections-resources/ [https://perma.cc/7RUK-ANJL].

The wholesale malicious manipulation of reported vote totals would have to follow these patterns quite closely, or else be flagged for investigation. Keep in mind, as well, that vote-total data now originate through two independent news-gathering channels and are fed simultaneously to a half-dozen national media operations. Through 2016, all major television and print media outlets used the vote-count data from the Associated Press. In 2017 and 2018, ABC, CBS, CNN, and NBC received their vote-count data from Edison Research, while Fox News, the *New York Times, Washington Post,* and other (traditional) print media received their data from the Associated Press. These independent vote-count operations allow for both real-time and post-election auditing of informal vote reports. For a variety of reasons, the Associated Press and Edison operations are unlikely to be perfectly in sync with each other at points in the night. But, if they do report results that are meaningfully and dramatically different from each other, it would get noticed quickly.

In the moment on election night, anomalies would certainly be noticed by the news operations receiving the data. Each operation supplying the data, the Associated Press and Edison, feeds that data to multiple downstream media outlets. Anomalies are noticed. Many of the separate news operations maintain open communication channels with each other on election night, and share information about election returns that seem amiss.

Finally, an attack on the election returns themselves would have to be sustained throughout election night and into the overtime period. A single successful penetration of the informal reporting infrastructure might be successful in causing a momentary discontinuity in the vote counts, but this would be quickly caught by the automated and manual quality-control processes that are in place. Such an attack would have to be sustained throughout a state in small amounts that would accumulate into a deviation from the actual returns in such a way that fit within historical norms. In other words, a successful, sustained attack that dramatically altered the results in a single county would cause that county's vote results to anomalously stand out when compared to the other counties in the state. In order to mask this, a malicious actor would

have to sustain successful attacks in numerous jurisdictions throughout the state.

These comments pertain to the informal information-reporting process that is centered on news organizations. The formal process tends to have procedures in place to detect attempts to manipulate the results. While these procedures may be circumvented in low-profile races on occasion, it is hard to imagine them being circumvented for high-profile races, like the presidency. One basis for detecting the manipulation of official returns is having multiple sources of information about the election returns. Parts of the canvassing process, especially those that resemble double-entry bookkeeping, require that the same calculation results be produced through independent means.

The primary way that the accuracy of election returns in the formal process is ensured by transmitting them through multiple means. The best protection against manipulation through an attack on computer networks is to communicate those returns physically, on paper and by currier. If there is at least one physical channel to communicate election returns to the next level of aggregation, then that report could serve as a check against the information that was communicated via an electronic network, either the Internet or the telephone network. Any difference between the two forms of communication would have to be investigated back to the source. We have not done a systematic survey of state and local election officials, but based on our discussions with many election officials, we believe that most states rely on communicating formal information about election returns through at least two channels.

d. Respond

We assume that in the 2020 election, as in every election, some anomaly in the vote-count will emerge in some jurisdiction. Such an anomaly will require the responsible officials to respond by reconstructing what the true election count is, and by demonstrating to the public that the correct results have been included in the official tally.

Although anomalies in both the informal and formal vote tallies will probably create doubt among the public in whether the vote count is

correct, and officials need plans to respond to both, in the end, the most important vulnerabilities to respond to are those that infect the official vote process. The manipulation of official vote tallies has the potential to install the wrong person into office. For that reason, it is important that among the responses to anomalies that are available to election officials is the ability to overturn the presumed results of an election, in light of evidence that the original count was fraudulent or based on a counting error.

If the manipulation or error is discovered during the canvassing period, or even the period in which challenges to election returns are possible, all is not lost. However, many states, if not most, time their post-election-audit processes to occur after the results have been certified, and make no explicit provision for revisiting the results of the election if a serious, material anomaly is discovered. These types of post-election auditing procedures are flawed.

The new kid on the block with respect to post-election auditing is risk-limiting audits (RLAs). RLAs are designed to be implemented before the certification of the results, and to inform election officials whether they should be confident in the results—or if they should bump the audit up to a full recount.[75] RLAs conducted as part of the certification process currently provide the best mechanism through which the manipulation of election returns at the precinct level can be detected and, most importantly, remedied. State legislatures should not only adopt RLAs, they should write legislation that includes RLAs as part of the canvass.

e. Recover

Recovery in the cybersecurity context is related to learning from the intrusion and restoring the system to a functioning level, presumably with new safeguards in place to overcome prior security deficiencies. The United States has not yet experienced a serious large-scale attack

---

[75] *See generally Knowing Its Right: A Two-Party Guide to Risk-Limiting Audits*., DEMOCRACY FUND (May 22, 2020), https://democracyfund.org/idea/knowing-its-right-limiting-the-risk-of-certifying-elections/ [https://perma.cc/XL9U-8FK6].

on the system that reports election results, either formally or informally, so it is difficult to speculate with any certainty about the ability of the system to learn from intrusions in such a way that makes the system more secure.

The United States *does* have experience with situations that are adjacent to the vote-reporting system, and we might learn from the responses to those experiences. Among these are the controversy over Jimmy Carter's early concession on election night 1980, based on preliminary election results, and news organizations reporting election results before the polls are closed statewide in states that straddle time zones. As a result of the controversy surrounding Carter's concession, national media organizations agreed that they would not "call" any state until all precincts had closed there.[76] Efforts, already noted, by the *New York Times* to visualize the uncertainty of preliminary election results through the "needle," is another example of the system learning and trying to adapt.

The negative side of the ledger has entries, too. The nation's slow and uncoordinated response to the known cyberattacks on election infrastructure in 2016 should give one pause in considering whether and how the nation would respond to a malicious attack on the vote-reporting system. However, any attack against the formal vote-reporting system would be an attack against state and local systems, not a system run by the federal government. This gives us optimism that the response to a cyber-attack against the vote-reporting infrastructure would be led by the response of local election officials, and other state and local actors, and would not be as slow to respond as the most recent federal response to election security has been.

---

[76] Reginald Stuart, *Congress to Debate a Uniform Schedule for National Voting*, N.Y. TIMES, Jan. 18, 1985, at A1, https://www.nytimes.com/1985/01/18/us/congress-to-debate-a-uniform-schedule-for-national-voting.html [https://perma.cc/8CK6-75LQ].

VII. Conclusion

The election-reporting infrastructure in the United States is distributed between formal and informal actors, and knits together a highly decentralized set of players. Like all aspects of election administration, the decentralization of the system creates both advantages and disadvantages in the struggle against error and actors with malicious intent. Unlike most other areas of election administration, the reporting of election results occurs through formal and informal challenges. The two challenges both reinforce each other and provide an opportunity to audit, in real time, the information flowing through the system.

In every challenge to the system of election administration since 2000, there has been a tendency to try and identify a technological magic bullet to solve the problem identified, whether it be voting machines or voter registration. In the case of reporting election results, there is likely to be no technological silver bullet. Technology itself opens up vulnerabilities. But, even if we leave technological vulnerabilities aside, election returns by their nature are subject to manipulation when they are communicated to the public. In thinking about how to ride out the cybersecurity storm of 2020, it is important to consider both the technological and social aspects of how election returns are communicated to the public if the country is to protect against efforts to undermine the legitimacy of the election.