FEARS AND FACTS ABOUT ELECTORAL INTEGRITY

Charles Stewart III

Charles Stewart III *is Kenan Sahin Distinguished Professor of Political Science at the Massachusetts Institute of Technology. Since 2001, he has been a member of the Caltech/MIT Voting Technology Project, which applies scientific analysis to questions of election technology, administration, and reform. He has furnished advice to the U.S. Presidential Commission on Election Administration.*

When election integrity became a theme in the U.S. presidential election of 2016, many were surprised. Officials and experts had spent countless hours and billions of dollars since the disputed 2000 election to improve the electoral process, and there was evidence to show that their efforts had been bearing fruit: A growing body of studies confirmed that election performance had indeed been getting better. Yet in 2016, the public was thrown into a panic over the possibility that the November election would be a sham.

During his campaign, Republican Party candidate Donald Trump charged repeatedly that his Democratic Party rival Hillary Clinton was "rigging" the contest, while others sounded alarms about Russian interests "hacking" the race. After the polling, Green Party candidate Jill Stein complained of problems with computerized voting equipment. During the primaries, Trump and Vermont senator Bernie Sanders (officially an independent but running as a Democrat) had accused insiders within their respective parties of having stacked the decks against them through the general design of the nomination process as well as specific actions meant to favor other candidates.

Charges such as these should not have come as such a shock. Since 2000, claims of improprieties associated with the electoral process have become a staple in partisan debates. A review of the scholarship on U.S. elections, however, suggests a more sanguine view than this barrage of allegations might imply.

Three main concerns about electoral integrity have risen to the sur-

Journal of Democracy Volume 28, Number 2 April 2017

face since 2000, and figured prominently in the 2016 race. The first focuses on election administration. Races can be close, and election outcomes can rest on the performance of voting technology and other matters that have to do with how elections are managed. The second centers on the worry that the U.S. system of verifying voter identity at the polls leaves elections open to being overrun by ineligible voters (noncitizens, felons), double voters, and impersonators. The third concern is a fear that growing reliance on computers to manage everything from voter registration through the final reporting of results makes elections vulnerable to computer errors and, still worse, the malice of hackers.

Concerns about election administration tend to be shared across the U.S. political spectrum, and to fuel the other two worries. Republicans and those on the right are more likely to credit theories involving ineligible voters,[1] while Democrats and those on the left are more likely to embrace claims that voting machines can be or have been hacked.

The 2016 election saw the introduction of a fourth concern as well. This consists of worries that not individual voting machines, but rather the larger computerized infrastructure of elections, is vulnerable to attack and disruption. In the political context of 2016, this concern probably had greater currency among Democrats. Yet since the perpetrators of election-focused cyberattacks in 2016 appear to have been Russian, it seems plausible that both parties may take up this theme in the future.

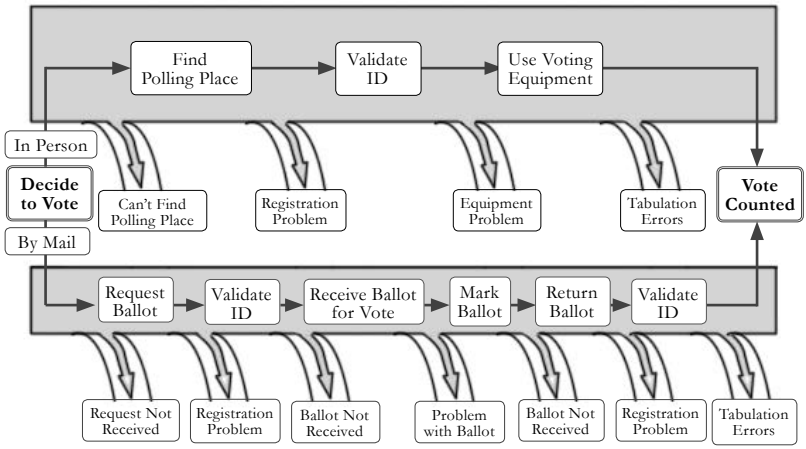
Checking Voting-System Health

The swirl of charges relating to election vulnerability in 2016 was at times overwhelming. To assess how well the 2016 election was managed nationwide, we should first make clear what we are talking about. What is the electoral system that we are judging? How do we measure its quality?

The U.S. electoral process involves an interacting array of distinct, individually complex systems. Voters and scholars alike tend to pay the most attention to the "higher-profile" elements, such as the systems for nominating candidates, financing campaigns, and communicating with voters. Then there are "nuts and bolts" procedural matters—usually gathered under the election-administration rubric—that have to do with how candidates qualify for the ballot, how voters register, and how they cast ballots.

The focus of this essay is election administration. This domain encompasses most of the issues raised since 2000—malfunctioning voting machines, inaccurate voter rolls, confusing ballots, and so on. In 2016, Trump's charge that millions voted illegally and Stein's complaint about voting-machine inaccuracies both concerned administrative matters. Only worries about the hacking of the Democratic National Committee's e-mail servers and charges that Russia was intervening to help Trump fell outside that area.

FIGURE 1—THE "PIPELINE" OF VOTING



Source: Charles Stewart III, "Losing Votes by Mail," *New York University Journal of Legislation and Public Policy* 13 (Fall 2010): 573–601.

In 2001, the Caltech/MIT Voting Technology Project (VTP) looked at election administration in terms of the individual voter's experience.[2] The journey from a voter's decision to vote to the counting of that vote can be likened to a trip through a pipeline (see Figure 1 above). Like a real pipeline, this metaphorical electoral conduit can "leak" at any one of a number of points, causing the voter's vote to be lost. Among these "leakage points" could be 1) a polling place that is hard to find; 2) one that has unfeasibly long lines or other problems; 3) a registration difficulty that confronts the voter at the polling place; 4) voting-equipment problems; and 5) tabulation errors.

The 2001 VTP report estimated that in 2000, long lines or other polling-place problems prevented nearly a million U.S. citizens who wished to vote from doing so. Another 1.5 to 3 million ran into registration difficulties that kept them from voting, and still another 1.5 to 2 million had their votes go unrecorded because machines were not working.[3]

Later research on a topic that the 2001 report omitted—votes lost in the "mail channel"—hinted at another serious source of leakage. Mail-in voting, which is becoming more popular in the United States, presents more chances for votes to be lost than does in-person voting. The number of votes that leak via this channel may rival the number lost on election day.[4] The vote-by-mail process is more complex and lengthy—as well as less closely monitored—than in-person voting. Whether the postal voting is being done as traditional absentee voting or because a jurisdiction (the state of Oregon, for instance) conducts all its elections exclusively by mail, a voter must first request a ballot, which could be held up by administrative delays or even become lost in the mail. And once that ballot reaches the voter, is filled out, and is returned to the cen-

tral voting office, it faces more potential challenges—such as signature verification and vote-counting inaccuracy—than would a ballot that had been cast in person.[5]

In either form of voting—via the mail channel or via a trip to the polls—a vote can "leak" from the electoral process owing to honest human error, deliberate human malfeasance, or administrative practices (such as rules for interpreting voter intent) that can have the effect of excluding ballots from being counted.

The 2000 election's "butterfly ballot" episode in Palm Beach County, Florida, is a good example of human error causing votes to be lost.[6] In that case, the election supervisor was worried that listing in the traditional manner (one after the other in a single column on one side of the ballot) the ten presidential candidates who had qualified to run in Florida would require a font so small that the county's many older voters would be unable to read the names. So she chose a two-page layout that allowed a much larger font, but also sowed confusion about which hole to punch for which candidate.

Human malfeasance can come in many forms, from changing marks on paper ballots to deliberately misrecording vote totals. Of great concern in some quarters since the early 2000s is the possibility of maliciously hacking computerized voting machines so that their touchscreens record the choice of Candidate A as a vote for Candidate B, or their vote-counting software "flips" votes from one candidate's total to another's.[7]

Finally, administrative error may come into play through the decisions and practices of election officials. An example of an administrative decision causing vote leakage would be a rule that disallows a ballot in a recount because the voter failed to follow the narrow requirements of the law (such as indicating a vote with an "X" and not a check mark). An administrative practice might be something such as maintaining voting equipment so poorly that votes are lost to machine failure. It is likely, for instance, that the problem of "pregnant chads" witnessed in the 2000 Florida recount happened because chads from earlier elections had been allowed to accumulate in the punchcard holders. Had officials carefully cleaned the holders after each election, the world might well have been spared the need to learn the term "pregnant chad."[8]

The 2000 controversy's highlighting of administrative and human errors was a big force behind Congress's passage of the Help America Vote Act (HAVA) in 2002. This law allocated US$2 billion to help states and localities buy new voting equipment. In addition, HAVA required all states to have centralized and computerized voter-registration systems, as well as "provisional-balloting" laws to help voters who encounter problems with their registration records on election day.

Overcoming human malfeasance was not a major theme of HAVA. Yet its requirement that any new voter who had registered by mail had to show some form of identification upon voting for the first time—added

at the urging of then-Senator Christopher "Kit" Bond (R.-Mo.)—became the opening salvo in what has grown into a war between Republican and Democratic legislators, at both the state and national levels, over the issue of voter fraud and the need for photo ID.[9] Although impersonation fraud is very rare—seasoned election lawyers report that "inside jobs" to falsify tabulation reports are more likely—this issue has come to dominate discussions of vote fraud among both politicians and the public at large.[10]

Another provision within HAVA that drew little notice at the time the law was passed has become a lightning rod for charges that the U.S. electoral system is vulnerable to hackers who are capable of manipulating vote counts. This provision requires that every U.S. polling place have at least one "direct recording electronic [DRE] voting system or other voting system equipped for individuals with disabilities." Local administrators trying to keep things simple have often taken this as a mandate to replace paper ballots (whether hand-counted or scanned) with DRE voting machines (see Table on p. 58).

The switch spurred complaints about DREs as "black boxes"[11] that would store votes by electronic means alone, thereby making it impossible to follow a ballot's trail from casting to counting. Computer-science professionals spoke out against the spread of such machines, and suggested that any machines used should at least produce a voter-verifiable paper audit trail (VVPAT) to be used in a mandatory postelection audit. Decades before, computer scientists and others had raised these concerns, but these voices were mostly ignored while HAVA was in the works.[12] That has since changed, and the deployment of these DREs is being rolled back. As the topic is highly technical, it has so far escaped politicization.

Research suggests that the types of problems that came to light in 2000 have diminished over time. The machine upgrades called for by HAVA led to a million fewer votes being lost in 2004 as compared to 2000. The improvement carried on through 2012.[13] Similarly, the rate of vote loss due to registration problems seems by my calculations to have halved between 2000 and 2008.

In 2002, the Pew Charitable Trusts began publishing the Elections Performance Index (EPI), which rates how well states do at holding elections.[14] It now runs up through 2014.[15] The EPI was inspired by the work of Heather Gerken, whose 2009 book *The Democracy Index* advocated rating states on objective measures of election administration in order to press low performers to improve.[16] According to the EPI, election administration has been improving from the voter's perspective.

Information Systems and Their Weaknesses

If the 2000 presidential election highlighted the administrative challenges that face the U.S. electoral process, the 2016 race highlighted the role that computers play in election administration—and the vulner-

abilities that they bring. Three news stories loomed large. The first was the hacking of e-mails belonging to the Democratic National Committee (DNC), probably by Russians.[17] The second was the targeting by hackers of voter-registration systems in twenty states, with actual infiltrations occurring in Arizona and Illinois.[18] The third covered doubts raised about the accuracy and reliability of computerized vote-tabulation equipment.[19] Citing these, the Green Party's Jill Stein forced a full recount in Wisconsin—it added 131 votes to Trump's lead in that state—and tried but failed to obtain full recounts in Michigan and Pennsylvania.[20]

These three stories, sadly, became so conflated in many minds that actual election-administration vulnerabilities were often misunderstood, and concerns misplaced. For instance, the hacking of the DNC (and possibly also the Republican National Committee) had nothing to do with election administration as such. Instead, it belonged in the category of old-fashioned political "dirty tricks," albeit with an international cybersecurity flavor. The remaining two stories are related only because both the Internet and vote-tabulating machines rely on electronics and are used in elections.

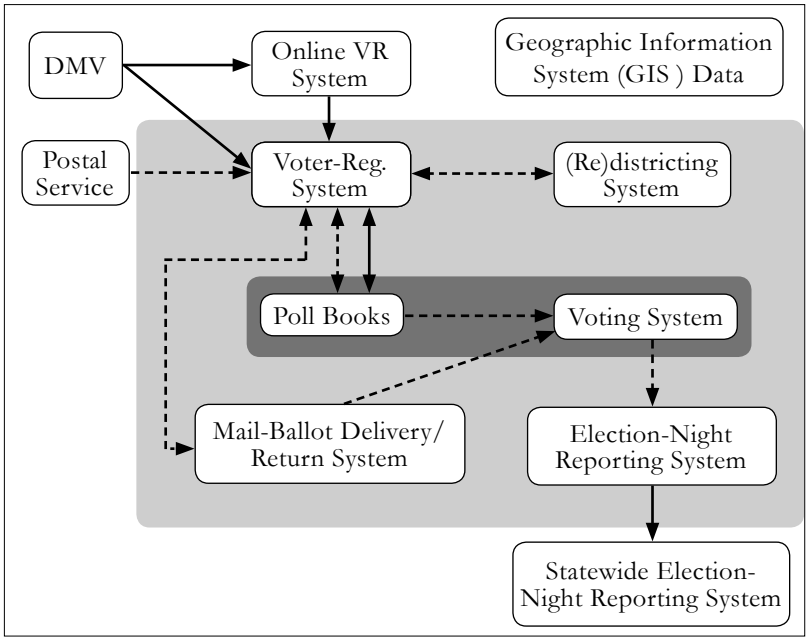
To help place these latter two stories about computer-related election vulnerabilities in context, consider Figure 2 on page 56. Based on the work of Merle King, it illustrates the information-system architecture associated with administering an election.[21] For the sake of discussion, let us call this total system the *election system*. At the core of the election system is the *voting system*. In this system, ballots are defined, votes are cast and counted, tallies are displayed, and the basic information needed to audit (or recount) election results is produced.

Presently, U.S. voters use two types of machines. In one type, votes are captured on paper ballots (often by filling in ovals with a pen or pencil) and then tabulated by optical scanners. In the other, votes are first captured electronically (by means of a touchscreen, for instance) and are then tabulated by the same machine.[22] For the voting system to work in a computerized environment, a ballot must be defined in software. For a paper ballot, this means laying it out and getting it printed, and it also means programming the scanner to correctly interpret marks on the paper. For an electronic ballot, this means laying out the ballot electronically and then loading that ballot image into individual voting machines so that touchscreen touches are interpreted and recorded properly.

Surrounding the voting system are other systems that support the act of voting. "Upstream" systems are in place before the vote is cast. For in-person voting, the voting site will have a poll book of voters who are eligible to cast a ballot at that location. Poll workers consult this book (either in print or on a computer) when voters present themselves to vote.

Behind the poll books is the voter-registration system, which receives information from a variety of sources and manages election-related data. Most new voter-registration information comes either from postcard-

Figure 2—A Schematic View of the Election System



Source: This schematic of voting information-system architecture is based on the work of Merle King. For King's full schematic, see page 14 at *www.nist.gov/sites/default/files/documents/itl/vote/tgdc-feb-2016-day2-merle-king.pdf.*

Note: Arrows depict the direction of information flow between component systems. Solid lines indicate flows that typically rely on the Internet or other networks that are connected to the Internet; dashed lines indicate information flows that typically are "air-locked" from outside networks. The dark box indicates systems that are typically deployed in individual polling places; the light-gray box indicates systems that are typically centralized in a local jurisdictions's election office.

sized forms or via state departments of motor vehicles (DMVs), which under the federal "motor voter" law of 1993 must serve as application points for voter registration (this obligation is shared with certain other state agencies, but in practice most new registrants come in via DMVs). A growing number of states now also have direct online voter-registration portals linked to their DMV databases. Information recorded in poll books—voter histories and address changes, for instance—is also used to update the registration system. Similarly, systems that track postal ballot requests can perform the same updating function as poll books, only in this case for mail-in rather than in-person voters.

Kicking in once votes are cast, "downstream" systems tabulate results and then forward them to a centralized system, which in turn aggregates results from all the voting machines throughout a jurisdiction. Those results then go on to central state-level systems for further aggregation and dissemination.

The shading in Figure 2 indicates where these systems are typically located physically. The two systems in the dark-gray box—the poll

books and voting system—are distributed across a jurisdiction's polling places. The systems in the light-gray box tend to reside centrally within a local jurisdiction (a single state will have many such jurisdictions). The remaining systems outside this box represent information that comes and goes outside the control of the local election jurisdiction.

In addition to identifying the principal election systems and their physical locations, Figure 2 describes information flows among the various component systems, with arrows indicating the typical direction of information flow. Solid lines mean that information flows via the Internet,[23] while dashed lines signal "air-locked" channels such as thumb drives, smart cards, and even paper.

Note that all the information flows for the voting system are drawn with dashed lines. That is because typical practice requires that information moved into and out of these systems be "off the net." Thus when digital scanners are programmed, this is done via thumb drive or smart card. Likewise, voting machines on election day are not connected to outside computer networks.

Examining Figure 2 helps us to see which types of vulnerabilities are associated with the different component systems and, in particular, which are more likely to be subject to *widespread* as opposed to *localized* attacks.[24] Because it is often linked to the outside world through multiple Internet pathways, the voter-registration system is certainly vulnerable to widespread attacks, whether these aim to commit identity theft, to tamper with particular information residing in the system, or to shut the whole system down via the traffic-overload method known as denial of service (DOS). If there is a live, real-time data link between the central voter-registration system and local poll books, the latter will be exposed to a widespread attack. Finally, election-night reporting systems are similarly vulnerable to widespread attacks, precisely because they are publicly accessible online portals.

The voting system itself, including voting machines, is mostly vulnerable to localized attacks. Since machines are individually programmed, offline devices, their vulnerabilities are not "scalable." Each machine would have to be individually corrupted by someone walking up to it and physically inserting (whether on purpose or by mistake) a "bad" thumb drive or smart card that would cause the machine to misread votes or the like.

When it comes to information-system weaknesses, are things better or worse than they were in 2000? Unfortunately, this question has yet to be addressed systematically and objectively, so it is impossible at present to give a comprehensive answer. Still, there are hints at a possible response.

Let us look at the two ends of the system, registration and machines. Right after HAVA passed, local jurisdictions began rushing to replace all their machines, paper or nonpaper, with DREs.[25] Then came the push-

TABLE—USE OF VOTING TECHNOLOGIES IN THE UNITED STATES, 2000–2016

Millions of Voters					
	2000	**2004**	**2008**	**2012**	**2016**
Non-Paper	**28.6**	**49.0**	**47.4**	**38.9**	**40.1**
Mechanical-Lever Machines	17.4	14.8	7.6	0	0
Direct Recording Electronic (DRE)	11.2	34.1	39.8	38.9	40.1
Paper	**66.9**	**61.1**	**77.1**	**83.9**	**91.3**
Punch Card	35.4	14.7	0.2	0.1	0
Hand-Counted	1.6	0.9	0.2	0.2	0.2
Scanned	29.9	45.5	76.7	83.7	91.1
Mixed	**9.6**	**11.7**	**6.8**	**5.8**	**5.2**
Total	**105.1**	**121.8**	**131.2**	**128.5**	**136.6**
Percent of Voters					
	2000	**2004**	**2008**	**2012**	**2016**
Non-Paper	**27%**	**40%**	**36%**	**30%**	**29%**
Mechanical-Lever Machines	17%	12%	6%	0%	0%
Direct Recording Electronic (DRE)	11%	28%	30%	30%	29%
Paper	**64%**	**50%**	**59%**	**65%**	**67%**
Punch Card	34%	12%	0%	0%	0%
Hand-Counted	1%	1%	0%	0%	0%
Scanned	28%	37%	58%	65%	67%
Mixed	**9%**	**10%**	**5%**	**4%**	**4%**
Total	**100%**	**100%**	**100%**	**100%**	**100%**

Note: Column sums are subject to rounding error. "Mixed" counties are those with more than one type of technology. In almost all cases, these are counties that have a combination of hand-counted and scanned paper.

Source: Data on election technology was supplied by Kimball W. Brace, Election Data Services. Election returns were collected by the author (2000–2012) and supplied by David Leip. See David Leip's Atlas of U.S. Presidential Elections at *uselectionatlas.org*.

back from computer scientists mentioned above, so that between 2008 and 2012 the use of DREs began to drop. By 2016, close to 80 percent of all voters were voting on machines that had paper backup. As localities keep trading out non-VVPAT devices for paper-backup machines, that percentage will go up. Moreover, concerns about tabulation accuracy have led more states to require audits. The EPI reports that by 2014, fully 33 states routinely audited their own elections.

At the other end, the rising number of centralized and Internet-reliant registration systems offers more targets for widespread attacks. In 2016, it appears, twenty states suffered unauthorized probes of their voter-registration systems. Although only two systems were actually infiltrated, it is less than reassuring to note that the Illinois penetration came by means of an SQL-injection hack, a long-known threat that is easy to defend against.[26] Backup expedients such as provisional ballots can blunt the effects of registration hacks, whereas the damage sown by wide-

spread voting-machine failures (especially if discovered only after polls have closed) would be far harder to fix.[27]

Threats and Failures: Potential versus Actual

Focusing on the administration of the electoral process itself, and viewing things from the perspective of the voter, the election of 2016 was a surprisingly positive experience. The 2016 Survey of the Performance of American Elections, which was designed specifically with the quality of the voter's experience in mind, reveals few reports of election-day problems. It also reveals that voters felt about the same average level of confidence that votes were being counted accurately as they had reported feeling in 2008 and 2012, respectively. And despite President Trump's persistent claims that millions of fraudulent votes were cast in the election, diluting the votes of legitimate voters and diminishing his mandate, no more than a handful of potentially plausible cases of illegal voting have been verified.[28]

Viewed from the perspective of information-system integrity, the actual conduct of the 2016 election ended up being anticlimactic.[29] No widespread disruptions related to voter registration were reported. Nor were widespread problems with vote tabulation discovered—the meager results of the Wisconsin recount underscored this. And though it is impossible to prove a negative, it is worth pondering that across the approximately thirty states that performed postelection audits, no evidence emerged of anything beyond local tabulation anomalies.

The 2016 election was distinct by dint of the ferocity of the campaign and the winner's startling claims that the results had been marred by fraud. It is important to recognize, though, that sniping by rival campaigns over the quality of election administration has now become a fixture, complete with hard-wired partisan positions. In this climate, scholars must do all they can to distinguish between *potential* threats to the health and integrity of election administration and attacks and failures that actually occur.

The U.S. election-administration system currently has safeguards—and local, state, and federal efforts since 2000 have enhanced its defenses. Yet more can be done. With partisan attention sharpening and cyberthreats growing in sophistication, election administration needs to become more transparent and more open to independent verification. Efforts such as the Elections Performance Index can help. All states should mandate timely election audits, and localities that still use voting machines with no paper trail should retire them as soon as possible in favor of machines that produce a VVPAT record. Given the voter-registration system's inherent vulnerability, states must find ways to audit their voter rolls for accuracy, and let voters know the results whether good or bad.

Finally, there is the matter of the U.S. electoral system's radical de-

centralization, which is rooted in federalism. At present, as FBI director James Comey has noted, this helps to guard U.S. elections against widespread cyberattacks.[30] In the future, however, the system's dispersed nature could make it harder for state and local election officials to organize against highly sophisticated cyberattacks. The federal Department of Homeland Security's declaration that the nation's electoral system is "critical infrastructure" has been met with skepticism by election officials at all levels of government.[31] Republican lawmakers' lingering distrust of a federal role in elections has led one U.S. House of Representatives committee to endorse a bill abolishing the Election Assistance Commission, the federal agency with the most practical expertise on issues of election security.[32] The question of the federal government's role in ensuring the health and security of the electoral process is one that will likely rise in prominence as time and technology move on.

NOTES

1. R. Michael Alvarez, Thad E. Hall, Ines Levin, and Charles Stewart III, "Voter Opinions About Election Reform: Do They Support Making Voting More Convenient?" *Election Law Journal* 10 (June 2011): 73–87.

2. Caltech/MIT Voting Technology Project, *Voting: What Is,What Could Be,* July 2001. The discussion of this framework follows the discussion in Charles Stewart III, "Losing Votes by Mail," *New York University Journal of Legislation and Public Policy* 13 (Fall 2010): 573–602, which uses the analogy of a pipeline.

3. These estimates were derived from studies by the Census Bureau and by analysis of official election statistics reported by the states.

4. Stewart, "Losing Votes by Mail."

5. According to the U.S. Election Assistance Commission, in 2012 at least ninety-thousand postal ballots were rejected due to signatures that were missing or that failed to match. U.S. Election Assistance Commission, "2012 Election Administration and Voting Survey," September 2013, Table 33a. See also R. Michael Alvarez, Dustin Beckett, and Charles Stewart III, "Voting Technology, Vote-by-Mail, and Residual Votes in California, 1990–2010," *Political Research Quarterly* 66 (September 2013): 658–70.

6. Jonathan N. Wand et al., "The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County, Florida," *American Political Science Review* 95 (December 2001): 793–810.

7. Bev Harris with David Allen, *Black Box Voting: Ballot Tampering in the 21st Century* (Renton, Wash.: Talion, 2004); Douglas W. Jones and Barbara Simons, *Broken Ballots: Will Your Vote Count?* (Stanford: Center for the Study of Language and Information, 2012).

8. Douglas W. Jones, "A Brief Illustrated History of Voting," updated 2003, *http://homepage.divms.uiowa.edu/jones/voting/pictures*.

9. Charles Stewart III, "What Hath HAVA Wrought? Consequences, Intended and Not, of the Post-*Bush v. Gore* Reforms," in R. Michael Alvarez and Bernard M. Grofman, eds., *Election Administration in the United States: The State of Reform after* Bush v. Gore (New York: Cambridge University Press, 2014), 79–101; Richard L. Hasen,

The Voting Wars: From Florida 2000 to the Next Election Meltdown (New Haven: Yale University Press, 2012); Daniel R. Biggers and Michael J. Hanmer, "Understanding the Adoption of Voter Identification Laws in the American States," *American Politics Research* (online January 2017, forthcoming in print), *http://journals.sagepub.com/doi/full/10.1177/1532673X16687266*.

10. Lorraine C. Minnite, *The Myth of Voter Fraud* (Ithaca: Cornell University Press, 2010); Mark Braden and Robert Tucker, "Disputed Elections Post *Bush v. Gore*," in Alvarez and Grofman, eds., *Election Administration*, 3–31.

11. Harris with Allen, *Black Box Voting*.

12. Roy G. Saltman, *Effective Use of Computing Technology in Vote-Tallying: Final Project Report* (Washington, D.C.: U.S. Department of Commerce, National Bureau of Standards, 1975); Saltman, "Accuracy, Integrity and Security in Computerized Vote-Tallying," *Communications of the ACM*, October 1988, 1184–91, 1218; Saltman, *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence* (New York: Palgrave Macmillan, 2006).

13. Charles Stewart III, "Residual Vote in the 2004 Election," *Election Law Journal* 5 (June 2006): 158–69; Stewart, "The Performance of Election Machines and the Decline of Residual Votes in the United States," in Barry C. Burden and Charles Stewart III, eds. *The Measure of American Elections* (New York: Cambridge University Press, 2014), 223–47.

14. Pew Charitable Trusts, "Elections Performance Index," 9 August 2016, *www.pewtrusts.org/en/multimedia/data-visualizations/2014/elections-performance-index*.

15. A further update for 2016 is in the works.

16. Heather K. Gerken, *The Democracy Index: Why Our Election System Is Failing and How to Fix It* (Princeton: Princeton University Press, 2009).

17. Tom Hamburger and Karen Tumulty, "WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations," *Washington Post*, 22 July 2016; David E. Sanger and Eric Schmitt, "Spy Agency Consensus Grows that Russia Hacked D.N.C.," *New York Times*, 26 July 2016.

18. "U.S. Official: Hackers Targeted Voter Registration Systems of 20 States," *Chicago Tribune*, 30 September 2016.

19. J. Alex Halderman, "Want to Know If the Election Was Hacked? Look at the Ballots," Medium, 23 November 2016, *https://medium.com/@jhalderm/want-to-know-if-the-election-was-hacked-look-at-the-ballots-c61a6113b0ba#.v1f6g27fp*.

20. Matthew DeFour, "Completed Wisconsin Recount Widens Donald Trump's Lead by 131 Votes," *Wisconsin State Journal*, 13 December 2016, *http://host.madison.com/wsj/news/local/govt-and-politics/completed-wisconsin-recount-widens-donald-trump-s-lead-by-votes/article_3f61c6ac-5b18-5c27-bf38-e537146bbcdd.html*.

21. For King's full schematic, see page 14 at *www.nist.gov/sites/default/files/documents/itl/vote/tgdc-feb-2016-day2-merle-king.pdf*.

22. In 2016, 91.3 million votes were cast on paper systems (71 percent of all votes), almost all counted by scanners, and 40.1 million were counted on electronic voting machines.

23. "Internet" is not strictly the right term to be used here, because some of the computer networks are internal and proprietary.

24. I define a widespread attack as one that is centrally implemented and can be ac-

complished simultaneously in a geographically distributed fashion. A localized attack targets a specific piece of machinery or a system component in a specific location.

25. Information about voting-technology usage is based on data provided by Kimball W. Brace of Election Data Services. Turnout data for 2016 was gathered by the author from official sources and David Leip's Atlas of U.S. Presidential Elections at *http://uselectionatlas.org*.

26. Sean Gallagher, "Officials Blame 'Sophisticated' Russian Hackers for Voter System Attacks," Ars Technica, 30 August 2016, *https://arstechnica.com/security/2016/08/officials-blame-sophisticated-russian-hackers-for-voter-system-attacks*.

27. Because the legal system places such a priority on the finality of elections, courts have been very reluctant to order election reruns even when faults in the original running have been proven.

28. President Trump's insistence that millions of illegal votes were cast in 2016 highlights yet another instance of confusion flowing from a failure to distinguish between potential threats to election integrity and the actual success of those threats. Trump's charges seem to be based on reports, such as one from the Pew Trusts, that estimate the numbers of those who are registered in multiple states plus dead people who remain on voter rolls. See *www.pewtrusts.org/~/media/legacy/uploadedfiles/pcs_assets/2012/pewupgradingvoterregistrationpdf.pdf*. About 2 percent of registered voters move across state lines each year, so roughly three-million people are at least double-registered, especially as no law says that voters must tell their old states that they have moved. But what matters is how many such people actually vote in the same election in multiple states. Often overlooked is that the Pew report helped to spur the formation of multistate compacts to reduce multistate registrations. One of these is the Electronic Registration Information Center (ERIC). As of November 2016, twenty states belonged to ERIC. By then, it had already removed the outdated registrations of more than a million cross-state movers from voter rolls (*www.ericstates.org/statistics*). The existence of ERIC and programs like it indicates that to the degree President Trump is basing his charges on hard evidence, it is four years old and does not reflect efforts since 2012 to cut multistate registrations. See also National Conference of State Legislatures, "Voter List Accuracy," *www.ncsl.org/research/elections-and-campaigns/voter-list-accuracy.aspx*.

29. Derek Willis, "Voters Encounter Problems, But Not the Ones Most Feared," ProPublica Electionland, 8 November 2016, *https://projects.propublica.org/electionland/national/what-didnt-happen*; Jessica Huseman and Scott Klein, "There's No Evidence Our Election Was Rigged," ProPublica, 28 November 2016, *www.propublica.org/article/theres-no-evidence-our-election-was-rigged*.

30. As FBI director James Comey noted, the fifty-state voting system is so sprawling that it is hard for hackers to affect it decisively. Devlin Barrett, "U.S. Voting System So 'Clunky' It Is Insulated from Hacking, FBI Director Says," *Wall Street Journal,* 8 September 2016.

31. Chase Gunter, "DHS Vague on Rules for Election Aid, Say States," *FCW,* 14 February 2017, *https://fcw.com/articles/2017/02/14/what-does-dhs-mean-by-critical.aspx*.

32. Deborah Barfield Berry, "House Panel Votes to Close Election Assistance Commission," *USA Today,* 7 February 2017, *www.usatoday.com/story/news/politics/2017/02/07/house-panel-votes-close-election-assistance-commission/97603326*.