Perspectives on Electronic Voting

Douglas W. Jones*

I. Introduction

Election managers must consider a number of factors when considering a move to electronic voting technologies. The legislative bodies that oversee the election managers should be aware of these considerations as they craft the laws guiding the shift to new technology. Partisan and independent election observers also need to be aware of these considerations as they observe both the crafting of election laws and the reduction of those laws to practice.

Our focus here is on technologies that stand between the voter and the results of the election. This includes machinery that directly or indirectly attempts to interpret voter intent. Examples of such technologies include:

- Mechanical voting machines, as first developed over century ago.
- Direct recording electronic voting machines, as deployed in some countries since the 1970s.
- Punch-card vote tabulators, such as the Votomatic that was the center of controversy in Florida after the 2000 general election in the United States.
- Optical mark-sense ballot tabulators that scan and tabulate votes from paper ballots marked by the voter.

This section will address two questions that jurisdictions must answer when considering election automation:

- Why pursue voting technologies?
- How to manage the acquisition, evaluation and use of voting technologies?

The very first issue a jurisdiction faces as it moves toward election automation is the fundamental question: why do this? This question needs to be answered before any decisions about election technology are made.

The next issue that must be faced is how to manage the acquisition, evaluation and use of new voting technology. Each technology poses its own problems, but all technologies, from the simplest to the most complex, pose many of the same (or at least similar) problems. These problems can be looked at from a number of viewpoints. Each of these viewpoints brings out different aspects of the problem. Among the most valuable viewpoints are those centering on the election equipment life cycle, the election cycle, the flow of data through the election system, and the chain of custody that carries a vote from voter to the final canvass of the election.

There are many other issues involved in adopting voting technology, including choosing machines, dealing with vendors, working with donor and or legislative expectations, and maintaining public confidence in the election process. However, in this section, the focus is on the decisions of why to adopt voting technology, and how to bring that technology into operation. As a result, this paper discusses election technology without focusing on the specifics of any one technology. Thus, questions about the distinctions between, for example, optical mark-sense voting systems and direct recording electronic voting systems are not at issue.

*This material is based, in part, upon work supported by the National Science Foundation under Grant No. CNS-052431 (ACCURATE). Any opinions expressed here are those of the author and are not endorsed by the National Science Foundation or by the University of Iowa.

II. Why Automate Voting

Votes have been counted for thousands of years without the aid of technology. Ancient Greek democracy, Roman democracy and Swiss democracy did not rest on any technology more complex than shows of hands, stone and metal ballots, or pen and paper. These simple techniques serve to this day in many contexts, so it is useful to ask what drives election authorities to adopt more complex technologies.

Looking through the history of voting technology, there are at least five distinct reasons that, singly or in combination, have driven electoral authorities to adopt complex election technologies:

- To centralize control over the conduct of elections.
- To deal with the complexity of voting rules.
- To increase access to the polls.
- To reduce costs.
- To satisfy a desire for modernization.

The final reasons above are questionable. Whether it is political leaders or the international community, the hope to save money and the desire to show that the election authorities are thoroughly modern tend to lead to decisions that are less likely to be informed by technical and practical realities.

A. Centralized Control

In general, complex technological mechanisms require significant expertise to manipulate. Around the world, election authorities have used this fact to take control of elections away from local election workers and centralize it in the hands of authorities, or rather, the technical staff of the authorities. Election technology can offer significant benefits in jurisdictions where there is widespread fraud at the polling places, for example, where local election workers have routinely engaged in ballot-box stuffing or forgery of election results. On the other hand, centralization creates a risk of centralized fraud if the authorities or their technical staff are less than honest.

There are estimates that close to 30 percent of the ballots cast in some jurisdictions in the United States were fraudulent in the 1880s.[1] Many early developers of voting machines in the United States saw their machines as a defense against such fraud,[2] and reform advocates frequently saw the adoption of mechanical voting machines as an effective defense against fraud.[3]

One can easily infer a similar motivation for the adoption of computerized voting systems in Kazakhstan. Observers in the 2005 presidential election in that country reported widespread problems. While electronic voting would not have prevented reported abuses such as family or group voting, it would have prevented the incidents of ballot box stuffing or the numerous incidents of irregular ballot counting. In polling places where electronic voting was used, the opportunity for some of these abuses was eliminated.[4]

However, it is unfortunately easy for election administrators to overestimate the security they gain by using advanced technology to conduct elections. In 2006, the United States had about 500,000 computer programmers, 800,000 software engineers, and 500,000 computer systems analysts,

[1]Worth Robert Miller, "Harrison County Methods: Election Fraud in Late Nineteenth Century Texas," *Locus: Regional and Local History,* 7:2 (Spring 1995): 111-28. Available at http://clio.missouristate.edu/wrmiller/Populism/texts/harrison_county_methods.htm.
[2]Douglas Jones, "Technologists as Political Reformers: Lessons from the Early History of Voting Machines," presented at the Society for the History of Technology Annual Meeting, Las Vegas, October 13, 2006. http://www.cs.uiowa.edu/~jones/voting/SHOTpaper.pdf
[3]Joseph Harris, *Election Administration in the United States* (Brookings Institution, 1934). See particularly page 60. Available at http://vote.nist.gov/election_admin.htm.
[4]*Final report on the presidential election in Kazakhstan, 4 December 2005*, Organization for Security and Cooperation in Europe, Office for Democratic Institutions and Human Rights, February 21, 2006. See section XIV. Available at http://www.osce.org/item/18133.html.

i.e., a total of around 1.8 million people with significant knowledge of computer programming.[5] The United States has no monopoly on such knowledge, so it is reasonable to double this number to account for professional programmers elsewhere in the world, and to double it again to account for people who can program but do not do so as their primary job. In sum, we can safely guess that there are over seven million people in the world who have the skills needed to carry out technologically sophisticated attacks on computerized systems. Furthermore, some electronic voting machines appear to be vulnerable to surprisingly low-tech manipulation. For example, there are allegations from the spring 2006 municipal elections in the Netherlands that one polling place election official manipulated the controls on an electronic voting machine to fool elderly voters into thinking that they had voted when in fact, they had not.[6]

Centralized control, of course, poses significant risks. Centralization that takes control from corrupt local election officials and puts it in the hands of honest central authorities is good, but the central authorities are not always honest. The history of vote fraud in the United States is dominated by stories of corrupt political machines that controlled counties or occasionally entire states.[7] Decentralization is frequently a strong weapon for dealing with corrupt authority.

B. Complex Voting Rules

When ballots are simple, with a single race on each ballot and only a few candidates in the race, hand counting paper ballots can be fast and accurate. An example of a recommended practice is to divide the ballots into stacks, one stack for each candidate plus one stack for blank or ambiguous ballots. This should be done without access to any pens or pencils in the presence of observers. At least two people representing opposing parties should examine and agree on the interpretation of each ballot, and disputed ballots should be displayed to all interested observers to demonstrate that they indeed contain no legal vote. Once this is done, the count can be completed by simply counting all of the ballots in each stack.

Such relatively simple counting rules do not work where there are many different races on one ballot, as in a typical general election in the United States. Or where there are hundreds of candidates in a single race, as in a parliamentary election in the Netherlands. The more complex the counting rules, the more likely people are to make errors in carrying them out.

Machines, whether mechanical or electronic, do not make clerical errors. They do, however, make other types of errors, and the people who administer machines make clerical errors. Yet as election rules grow more complex, the sheer volume of work involved in counting the ballots can make technology desirable despite these problems.

C. Increased Access to the Polls

Conventional elections require that all voters present themselves at a polling place during a limited time period. Many potential voters may not be able to travel to a polling place during the designated interval. Postal voting, voting by fax machine and Internet voting all offer the opportunity for increased access to the polls. However, each of these poses significant security problems! How can the election authority determine that a ballot received by post, by fax or over the Internet came from a legitimate voter? Numerous technologies have been proposed to accomplish this, some of which do not solve the problem at all (forgery of a photocopy of an ID document is far easier than forgery of the document itself). Other solutions compromise a voter's

---

[5]Occupational Outlook Handbook, United States Bureau of Labor Statistics, 2006-07 Edition. Available at http://www.bls.gov/oco/

[6]Onderzoek naar stemfraude in Zeeland (Investigation of vote fraud in Zeeland), *Brabants Dagblad*, March 21, 2006. Available at http://www.brabantsdagblad.nl/brabant/article188558.ece.
NFI: niet geknoeid met stemmachine Landerd (Netherlands Forensic Institute: no tampering with Landerd voting machine), *Brabants Dagblad*, August 23, 2006. Available at http://www.brabantsdagblad.nl/regios/udenveghel/article594020.ece.
Strafklacht stemfraude in Landerd (Indictment for vote fraud in Landerd), Brabants Dagblad, August 31, 2006. Available at http://www.brabantsdagblad.nl/gemeenteraadsverkiezingen/article613419.ece.

[7]Andrew Gumbel, *Steal This Vote* (Nation Books, 2005).

right to a secret ballot. This is currently a very active area of research.

The problem of reaching a polling place during the voting period is most severe for expatriate voters. The problems of expatriate voters, particularly those in areas with poor postal service, deserve particularly close attention. Many jurisdictions have explored Internet voting to serve the needs of these voters.[8] [9] [10] In many of these cases, it takes one or more postal transactions to obtain the right to cast an Internet ballot. It is reasonable to ask whether it might be more secure to use the Internet to deliver a postal ballot instead of using a postal transaction to deliver authorization to cast an Internet ballot.

In addition, voting on conventional paper ballots at the polling place requires that voters be able to handle a pen or pencil and that they be able to read the ballot. Blind voters, illiterate voters and physically disabled voters are at a clear disadvantage in such a context. There are very low-technology approaches to ballot access for the disabled and illiterate, most notably the tactile ballot.[11] Despite this, today most attention is focused on use of electronic voting machines for this purpose. A new class of devices, known generically as accessible ballot marking devices, is only beginning to emerge.[12] [13] The latter are, without doubt, as technologically complex as electronic voting machines, but instead of recording or tabulating votes, they merely assist the voter in marking a ballot.

D. The Cost of Elections

Elections are expensive. Among the costs to consider are the following items and processes:

- Salaries for polling place election officials, polling place technicians, polling place security officers, security officers at the storage facilities, and technicians required to maintain, test and set up voting equipment (among others).
- Training polling place election officials and polling place technicians.
- Special transportation for voting equipment.
- Printing paper ballots.
- Secure facilities to store paper ballots and voting equipment.
- Climate-controlled storage for electronic voting equipment.

In the United States, it is quite common to find that the total number of election officials exceeds 1 percent of the turnout in a general election. In addition, many election jurisdictions assign law-enforcement officers to protect ballots, technicians to provide support at polling places, truck-drivers to transport ballots, and many other temporary job assignments, so that the total number of people needed to carry out an election approaches 2 percent of the turnout. Every one of these workers must be paid, if not directly, then indirectly through the costs of their lost labor elsewhere in the economy.

Where paper ballots are used, the usual rules call for the number of ballots printed to exceed the expected turnout by a significant safety margin. It seems a pity to print ballots knowing that many of them are destined to be discarded unused. After the election, the law generally requires the

[8]Robert Hensler, "The Geneva Internet voting system, République et Canton de Genève Chancellerie d'Etat" (January 15, 2003). Available at http://www.geneve.ch/chancellerie/E-Government/doc/pre_projet_eVoting_eng.pdf.
[9]David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, "Analyzing Internet voting security," *Communications of the ACM* 47:10 (2004), 59-64. Available at http://portal.acm.org/citation.cfm?id=1022594.1022624.
[10]Organization for Security and Cooperation in Europe, Office for Democratic Institutions and Human Rights (OSCE/ODIHR), *Final Report on the 22 November 2006 Parliamentary Elections in the Netherlands* (March 12, 2007). See section IV.C. Available at http://www.osce.org/item/23602.html.
[11]American Council of the Blind, *Independent, Secret and Verifiable: A Guide to Making Voting an Independent and Accessible Process for People Who Are Blind and Visually Impaired* (2002). Available at http://www.acb.org/resources/votingbook1.html.
[12]The Automark ballot marking device is made by Automark Technical Systems (www.automarkts.com).
[13]Douglas Jones, *System for handicapped access to voting ballots*, U. S. Patent 7134597. Available at http://www.freepatentsonline.com/7134597.html.

storage of all ballots and other records of the election for some time. Paper records are bulky and expensive to store, and in warm moist climates, they may deteriorate quite rapidly.

For more than a century, advocates of election technology have hoped that mechanical and later electronic voting systems would reduce these costs. With respect to personnel costs, fast mechanical or electronic counting can indeed greatly reduce the amount of labor hours required after the polls close. With respect to printing and storage costs, paperless mechanical or electronic voting systems do eliminate the need for printing excess ballots before the election and storing voted ballots afterwards. Unfortunately, starting with the analysis done by Joseph Harris in the early 1930s, it has been clear that these savings can be elusive.[14]

The fundamental problem is that voting technology has costs that are quite different from the costs of low-tech elections conducted with simple paper ballots. Voting machinery must be stored securely between elections, generally in climate-controlled storage. Furthermore, voting machines require skilled technicians for maintenance and trained election workers for operation.

Some voting technologies are indeed inexpensive. The Votomatic and its descendants use mechanical ballot marking templates (the Votomatic machine), inexpensive ballot boxes, and only a single central computer system for ballot tabulation. In contrast, it may be necessary to purchase and store one direct recording electronic voting machine per 50 voters for a general election in the United States, or one per 1,000 voters for a Dutch parliamentary election. The difference in the number of voters a voting machines can handle is largely a function of how long it takes an average voter to work through the ballot, and this, in turn, depends on the complexity of the ballot.

E. The Appearance of Modernity

The electronic voting machines of the late 20th century and the mechanical voting machines of the late 19th century were all close to the limits of what was technologically possible at the time of their introduction. Some people clearly feel that the need to be modern is sufficient justification for using a technology. A typical advertisement for an election technology product promises that it "delivers the promise of the future of voting today!"[15] or "Internet voter registration and voting could be the most compelling issue facing e-government today and could also reinvigorate democracy like nothing before."[16]

However, modernity for its own sake is nothing more than a matter of fashion. Being modern may excite some voters, but the hope that it will reinvigorate democracy is, at best, speculation. As such, arguments for voting technology based on this kind of rhetoric should be discounted. When such arguments dominate the drive toward electronic voting, hard questions need to be asked.

III. Four Views of Voting Technology Management

As mentioned above, four views of the election process will be discussed, and steps related to the use of voting technology will be illustrated through each view.

A. The Voting System Life Cycle View

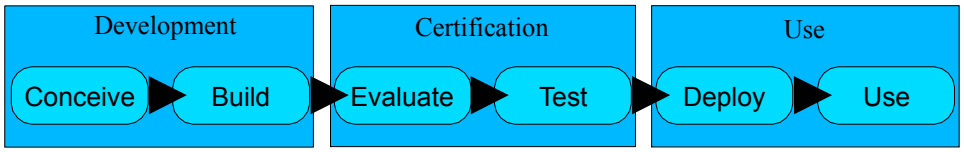
Typically, it takes several years for a voting system to move from conception to use. The cycle may be accelerated for incremental changes to an already deployed system, but even then, it is rare to upgrade a system in less than six months. More rapid system deployment can only be done at the risk of shoddy development, incomplete testing and inadequate training.

---

[14] Harris, p. 61.
[15]Quoted from Toolsmith Consulting, Liberty Election Suite, available at http://www.tool-smith.com/ToolsmithWeb/?t=products/liberty.
[16]Robert S. Done, *Internet Voting: Bringing Elections to the Desktop* (The PricewaterhouseCoopers Endowment for The Business of Government, February 2002). Available at http://www.businessofgovernment.org/pdfs/Done_Report.pdf.

The life cycle of a voting system, from its initial conception to its eventual abandonment, involves three major stages that can be subdivided into several minor stages. These stages bear strong similarities to the stages in the life cycle of safety critical systems such as avionics software or medical devices. The process begins with system development, followed by certification or qualification. Once systems are certified, they may be deployed and used.

Figure 1: The voting system life cycle



Voting system development begins with the conception of the new system. In the case of entirely new systems, this is frequently done by either an election official or an independent inventor. Where the system is an incremental upgrade of an existing system, the conception usually rests on observations of some inadequacy in the existing system.

Once conceived, the voting system must be built. This generally involves considerable labor, so someone must provide the capital needed to fund this work. Some voting systems have been developed at government expense, for example, the Sailau system in Kazakhstan or the SERVE system in the United States.[17] [18] Other systems have been developed with private funds, as with most voting systems sold in the United States. In some developing democracies, donor funds have been used to develop voting systems; in such cases, there is a real risk of disconnect between the actual needs of the developing democracy and the expectations of the donor.

Regardless of who funded the development of the voting system, it is essential that the system be subject to evaluation to ensure that the system, as developed, meets the requirements that have been set for it. A very common model has emerged around the world for such evaluation. Governments designate independent testing authorities (ITAs) to which voting systems are submitted for evaluation. The ITAs then evaluate the voting systems against voting system standards set by the government. This model is old, originating with independent steam engine and boiler testing agencies in the 19th century. Since then, it has spread to many other domains. In 1990, the United States adopted this model for testing voting systems.[19] Kazakhstan and the Netherlands use much the same model.[20] [21]

The need for the testing authority to be independent of the voting system developer or vendor is fairly obvious. It is equally important that the testing authority be independent of the government. When a government has spent large sums on a voting system or has committed itself to installing that system by a particular date, it is very natural for the government to attempt to pressure the testing authority to approve that system regardless of its actual adequacy. This kind of pressure threatens the integrity of the entire approval process.

Typically, the independent testing authority has two distinct functions, design review and testing. Design review involves a study of the design of the voting system, determining whether the system, as designed, meets the requirements set by the voting system standards. Such review applies equally to hardware mechanisms and software. Testing compares the system, as built,

[17]OSCE/ODIHR, *Final report on the presidential election in Kazakhstan, 4 December 2005* (February 21, 2006). See page 9. Available at http://www.osce.org/documents/odihr/2006/02/18133_en.pdf.
[18]Jefferson et al., 59-64.
[19]United States Federal Election Commission, *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems* (January 1990). Available at http://josephhall.org/fec_vss_1990_pdf/
[20]OSCE/ODIHR, *Final report on the presidential election in Kazakhstan*. See section VI.
[21]OSCE/ODIHR, *Final Report on the 22 November 2006 Parliamentary Elections in the Netherlands* (March 12, 2007). See section B. Available at http://www.osce.org/documents/odihr/2007/03/23602_en.pdf.

with both the design and the standards. Black-box testing focuses on functionality, focusing on user manuals and the external behavior of the system. White-box or glass-box testing examines the internal mechanisms of the machinery. Red-team testing involves deliberate attacks on the system in order to evaluate its response to improper or malicious use.[22]

The biggest problem faced by independent testing authorities is that they can only test to the standards that the government has set. If these standards are inadequate, the tests will be inadequate. Some standards are easy to test. For example, voting machines used in the Netherlands require that the buttons used to select candidates be no smaller than 10 millimeters and function when depressed from 0 to no more than 6 millimeters with a force of no more than 4 newtons. Additionally, they must operate on 187 to 242 volts at 49 to 51 hertz.[23] Other standards can be quite difficult to test. For example, voting machines used in the Netherlands must present information that is relevant, clear and clearly perceptible, and they must prevent or limit accidental or incorrect use, so far as is reasonable and technically possible.[24] Such problems are not confined to the Netherlands. Similar complaints have long been made about the voting system standards in the United States.[25]

Once a voting system has been approved as adequate, deployment may begin. At this point, training materials are finalized and training programs begin for election administrators. While preliminary training may have begun during the certification process, certification may require significant changes, and allowances must be made for these in the preparation of training materials. The highest training priority is for election administrators and the technical staff at election equipment warehouses.

Training typically involves using examples of the new voting system, but only a few such examples are needed initially. Large-scale manufacturing of the approved system can typically begin during training, because no large-scale deliveries should be made until trained staff are prepared to accept delivery.

On receipt of voting equipment, it is necessary to conduct an acceptance test to see that the machines, as delivered, are functional and match the designs that were approved. As with any purchase, acceptance testing must be conducted by the customer. A responsible vendor will, of course, conduct quality control tests in order to avoid liability for delivering broken or incorrect equipment, but if the customer does not test, there is no way to know if the vendor is being responsible.

Acceptance testing is as important for low-tech voting devices as it is for computerized election machinery. For example, prior to the 2000 general election in Cook County, Illinois, the ballot tabulating machines were tested, but not the mechanically trivial Votomatic vote recording devices. Unfortunately, as post-election analysis would show, these were defective, with holes that were slightly out of alignment. This error probably disenfranchised about three percent of the voters.[26]

Once the new voting system has passed its acceptance tests, it may be employed for one or more election cycles. During these cycles, deficiencies in the voting system will probably come to light, for example, due to inadequate design or improper use. At some point, these inadequacies will invariably lead to the decision to change the voting system, either by replacing it with an entirely new system or by modifying the design of the current system. Either of these cases involves the initiation of a new voting system life cycle, from development to deployment.

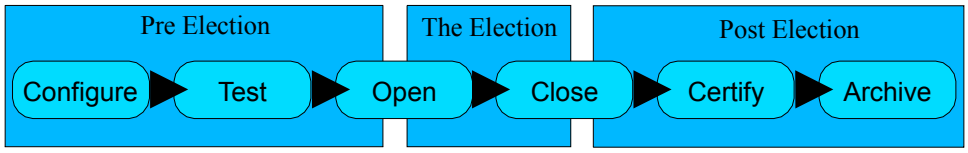
---

[22]Brennan Center Task Force on Voting Security (Lawrence D. Norden, Chair), *The Machinery of Democracy: Protecting Elections in an Electronic World* (Acadamy Chicago Publishers, 2007). See Appendix E, Voting Machine Testing.
[23]Netherlands Ministry of the Interior, "Annex: Specifications for voting machines," in *Voting Machines (Conditions and Approval) Regulations* (1997). See items 9.4 and 12.1.
[24]Ibid. See items 2.1 and 8.6.
[25]Earl Barr, Matt Bishop, and Mark Gondree, "Viewpoint: Fixing federal e-voting standards," *Communications of the ACM* 50:3 (2007), 19-24. Available at http://portal.acm.org/citation.cfm?id=1226736.1226754.
[26]Michael Hites and Bill Ornt, *Testing of Vote Recorders* (Department of Mechanical, Materials and Aerospace Engineering, Department of Mechanical, Materials and Aerospace Engineering, August 24, 2001).

B. The Election Cycle View

Election cycles are seen quite differently by the public and by election officials, and this difference becomes far more complex when elections are carried out using complex technology. The public sees a political campaign that culminates in an election, followed by a brief flurry of activity as the votes are counted and unofficial results are announced in the press. The election official sees a vastly different cycle that begins with pre-election activities, centers on election day itself, and is then finished with post-election activities that must be completed before the next election cycle begins.

Figure 2: The election cycle.



Pre-election activities include voter and candidate registration, but from the point of view of election technology, the story begins as soon as the lists of candidates and referenda that are to appear on the ballot are finalized. At this point, the process of ballot design begins. This process is remarkably similar whether the ballots are to be printed on paper or presented on an electronic voting system. The complexity of the ballot design problem depends very much on the jurisdiction. Ballots for general elections in the United States or parliamentary elections in Holland may involve hundreds of candidates and may differ significantly from one election district to another.

Where ballots are counted by machine, the machines must be configured to count the ballots. Whether on mechanical voting machines or electronic systems, this involves setting the interlocks on the different voting positions to enforce the rules of each race on the ballot. For example, in the race for president, voters may vote for only one candidate, while in the race for county commission, they may be entitled to vote for five out of the ten candidates, and in the race for city council, they may be allowed to cast a ranked-preference ballot, indicating first, second and third choices.

Ballot layout and voting system configuration are both subject to error, and machines that worked in the previous election may no longer be functional by the time they are used in the next election. Testing provides our primary defense against such problems. There are several types of testing:

- Acceptance testing (discussed above).
- Pre-election testing prior to delivery to the polling places.
- Pre-election testing at the polling places.
- Parallel testing during the election.
- Post-election testing.

Pre-election testing: With paper ballots, pre-election testing may involve little more than careful proofreading of the ballots. With voting machinery, the test should also involve casting test ballots, tabulating them, combining the results from multiple precincts, and verifying that the aggregate result of the test matches the expected result. Such a test involves the entire process of vote tabulation from the voting machinery used by voters to the computers used by the central election authorities.

Pre-election testing may also involve exhaustive testing—that is, complete testing of all system behavior. This is appropriate, but difficult to complete for machinery in election headquarters, including both central computer software and central ballot-tabulating machines. Exhaustive testing is practically impossible for machinery used in polling places. A reasonable scheme involves intensive testing of a random sample of the machines prior to their delivery to the polling

places, with care taken to ensure that every ballot style is tested.[27]

Testing may be conducted by elections office staff, or the public may be involved. In the extreme, pre-election testing becomes indistinguishable from pre-election voter outreach, as in Kazakhstan's 2005 presidential elections, where the public were invited to visit polling places and cast test ballots in the period prior to the election.[28] This was an effective public education measure, and it provided polling-place election officials with useful practice, but such a testing model must be considered an adjunct to, and not a substitute for, carefully designed tests.

As the official election begins, and immediately prior to opening the polls, the polling place election workers have one last chance to perform simple pre-election tests. These must be brief and simple, but they provide important protection to the election process. Failure to do such testing has led to embarrassing problems, as was the case in 2000 in Palm Beach County, Florida, when perfunctory tests were performed without anyone examining the results until a year later. As a result, voters in that election were allowed to vote on a significant number of defective Votomatic voting machines.[29]

During the election itself, the primary challenge posed by technology involves failure. Voting machinery is no different from other machinery, and thus sometimes fails. Provisions for dealing with failure can range from posting technicians at every polling place, as was done in Miami in 2004 and in Kazakhstan in 2005, to equipping every polling place with emergency paper ballots to be used in the event the machinery fails.[30]

Parallel testing: Some jurisdictions do parallel testing, that is, they select random voting machinery from among the machinery deployed to the polling places for testing during the election day. This obviously requires that there be sufficient equipment that taking random equipment for testing will not prevent proper conduct of the election. If properly conducted, parallel testing offers the possibility of detecting widespread rigging of election machinery, for example, by insertion of malicious software or improper ballot configuration files.

To achieve maximum effect, machines should be selected for parallel testing at the last possible moment and the test should be conducted in such a way that the machine cannot reasonably infer from the pattern of test votes that it is a test. Thus, test votes should be cast at realistic times of day, the number of test votes should be typical of the number expected at the polls, and the number of votes for each candidate should be typical. For polling places routinely equipped with multiple voting machines, the most extreme parallel testing model requires that the voting system testers arrive at random polling places just before the polls are opened. The testers then randomly select machines for testing after the machines are turned on and enabled for voting, but before any voters have cast ballots.

Post-election testing: Some jurisdictions require post-election testing. This is typically done with central tabulating equipment in order to verify that, after the official tabulation has been completed, the machinery is still functioning correctly. Post-election testing of direct-recording and precinct-based tabulators is extremely rare, except in cases of contested elections or suspected fraud. For example, extensive post-election tests (mistakenly called parallel tests) were performed after the contested 2006 election in Florida's 13th congressional district.[31]

---

[27]Miami-Dade County Elections Department, *Logic and Accuracy Test, August 32, 2004 Primary Election* (August 13, 2004). Available at http://www.cs.uiowa.edu/~jones/voting/miamihandout.pdf.

[28]"Election officials put final touches on ahead of vote," *Kazakhstan News Bulletin* (November 29, 2005). Available at http://www.kazakhembus.com/112905.html.

[29]Joel Engelhardt and Scott McCabe, "Poll workers ignored flaws in pre-vote machine tests," *Palm Beach Post* (December 9, 2001).

[30]"Temporary use of printed ballots in voting machine precincts," Iowa Administrative Code 721-22.431(52). See also "Counting emergency paper ballots," 721-26.61(49). Available at http://nxtsearch.legis.state.ia.us/NXT/gateway.dll?f=templates&fn=default.htm.

[31]Florida Bureau of Voting Systems Certification, *Parallel Test Summary Report for Sarasota County, FL, November 7, 2006 General Election Using Election Systems and Software, Inc. Unity Version 4.5, Version 2* (December 18, 2006). Available at http://election.dos.state.fl.us/pdf/parallelTestSumReprt12-18-06.pdf.

After the polls close, the concern with failure continues. Errors in the transmission of voting results from polling place to the election headquarters are quite common. Signed voter registers and paper ballots must be physically secured and transmitted, and electronic results must be recorded to physical media for physical transport. Redundancy is an important defense against loss. In Miami-Dade County, Florida, for example, electronic voting results are printed at the polling place immediately after the polls close. The paper copy is sealed in an envelope and sent to the regional election headquarters along with an electronic copy in a removable memory module, and the results are transmitted by modem to the central election headquarters.[32] Similar redundancy was present in the 2005 Kazakh election system.[33]

The canvass of the election usually proceeds through a hierarchy of levels. First, the polling place election officials certify a report of the canvass of the votes at that polling place. Then, once these reports are received by the regional election authorities, they are combined to make the certified regional canvass. Regional canvass reports are then combined to produce a state canvass.

Jurisdictions differ in the extent to which elections are subject to auditing. Auditing is an important post-election activity.[34] It may take a number of forms:

- Checking redundant information.
- Election recounts.
- Auditing the tabulation process.
- Re-doing the canvass.

All auditing activities may be further subdivided into *hot audits*, that is, those conducted before the certification of the canvass, and *cold audits*, or those conducted later. Hot audits are necessarily limited, since the time available is limited, while it is more difficult to correct erroneous election results with the result of a cold audit. Some jurisdictions have mixed models, involving a preliminary certification of the canvass, after which certain audits may be performed prior to the final certification.

Checking redundant information: All elections produce redundant information. For example, the number of signatures in the poll book and the number of ballots ought to be the same (in a vote-for-one election), the sum of the number of votes for particular candidates plus the number of invalid ballots ought to equal the number of ballots. In addition, with electronic voting machines, as mentioned above, it is common to produce multiple redundant reports of the results from each polling place. The extent to which this redundant information is considered in checking the canvass varies considerably. In Miami, the paper copy of the results and one of the electronic records from every polling place are routinely compared prior to certification of the regional canvass, and then, after the certification of the canvass, the county's audit and management department conducts a cold audit of randomly selected precincts, comparing other electronic and paper records. In contrast, in 2005, only the electronic copies were considered in the Kazakh election.

Election recounts: Recounts are, effectively, audits requested by candidates when they suspect that the official count is inaccurate. Some jurisdictions have automatic recounts for every election where the results are closer than some threshold. Recounts generally involve a complete repeat of the canvassing process, but they vary in the amount of information considered from the ballots themselves. Hand recounts involve actual inspection of all ballots by people, while machine recounts involve re-tabulation of the ballots by machine. The most limited form of recount, the re-canvass, involves no examination of actual ballots.

Auditing the tabulation process: California has long required that, after each election, ballots from polling places representing 1 percent of the vote be recounted by hand in order to check the correct function of the ballot tabulating machinery. This model has since been adopted by many other jurisdictions, with considerable variation in the number of polling places subject to audit,

[32]Miami-Dade County Elections Department, *Logic and Accuracy Test, August 32, 2004 Primary Election*.
[33]OSCE/ODIHR, *Final report on the presidential election in Kazakhstan*. See section VI.
[34]Douglas Jones, "Auditing Elections," *Communications of the ACM,* 47:10 (October 2004), 46-50.

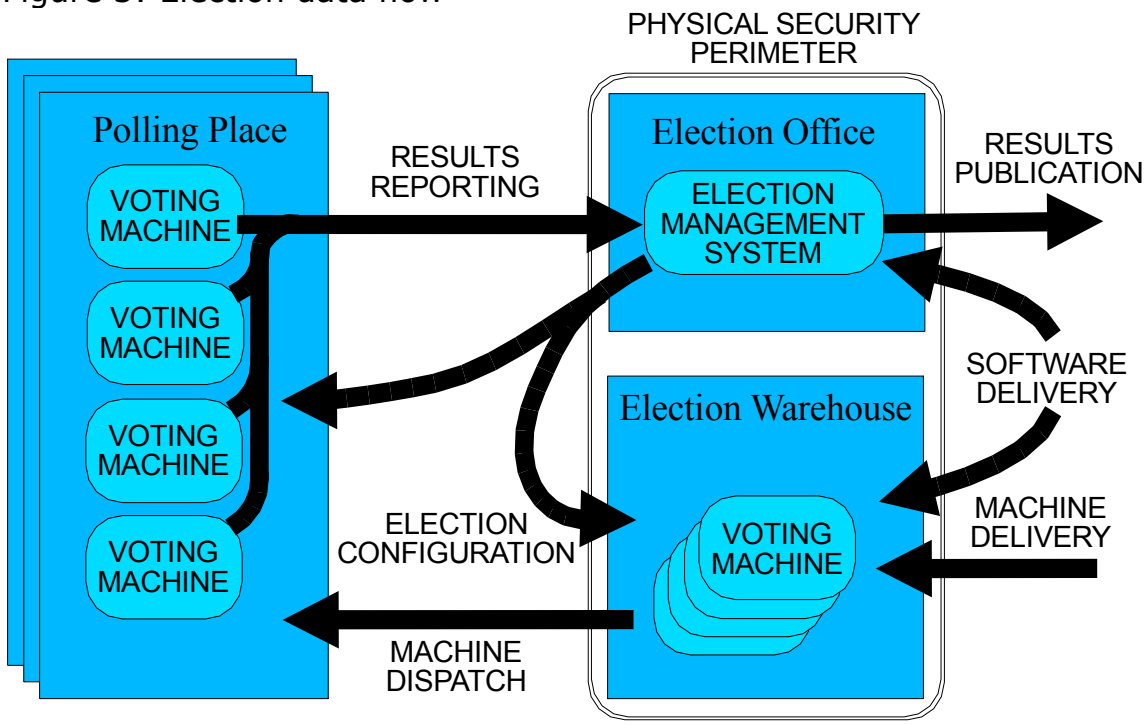
how those polling places are identified and when those polling places are known. The best practice is to determine the identity of the polling places as late as possible, so that there is no way for polling place election officials to know whether their work will be audited until they have completed it. The polling places to be audited should be selected at random, although there are proposals that the candidates should be able to name some of the polling places if they think there were irregularities.

The announcement of the results does not mark the end of the election cycle for the election official! Cold audits may occupy several weeks of effort after the results are finalized, and when this is done, one additional step remains: storing archival copies of the results so that the machinery may be reused in the next election. This archived election data is evidence that may be relevant not only to questions about the legitimacy of the election but also to prosecution of violations of the electoral law at any level. As such, it is prudent to store this information until the expiration of the statute of limitations for prosecution of such crimes and to store it under the same security rules that apply to criminal evidence.

C. The Data Flow View

A security analysis of an election generally begins by isolating all of the data paths through the election system. Once these data paths are identified, the potential attacks on each path can be enumerated. Only after this is done can the defenses be meaningfully evaluated. Figure 3 illustrates these data paths for a jurisdiction using voting machines, but it should be noted that most of these data paths exist regardless of the technology being used.

Figure 3: Election data flow



Machine delivery: As the voting system life cycle begins, machines are delivered to the election warehouse. At this point (as mentioned above), the jurisdiction should conduct acceptance tests to verify that the machines, as received, are functional and are indeed the machines that were ordered. During the lifetime of the hardware, the voting system vendor typically delivers software updates. Each such update should be treated as if it was a new voting system, and again, it is essential to check that the software received was indeed the software certified for use in this jurisdiction.

Machine dispatch: With each election cycle, the machines are moved from the secure warehouse of the election authority to polling places. Typically, the equipment is delivered hours or days before the election, and even if armed guards are present, the authenticity of the machines should again be checked before the polls are opened.

Election configuration: Voting machines, whether electronic or mechanical, must be configured for the election. This configuration has traditionally been done in the warehouse, before dispatching the machines to the polling places, but with modern compact electronic media, it is possible to deliver unconfigured machinery to the polling place and deliver the appropriate configuration files separately.

Wherever voting machinery is joined to election configuration files, it is essential to test that the configurations are authentic and that the machinery, as configured, is fully functional. This can naturally be combined with pre-election testing in the warehouse, or it can be part of testing at the polling place as part of opening the polls. In the latter case, however, the limited expertise available at the polling place poses problems, as does the question of what to do if the configuration is incorrect.

Results reporting: After the voting is complete at a polling place, the results from the various machines used there must be gathered and transmitted to the election management system. As already discussed, this may involve redundant data paths, paper and electronic. These exist, in part, to ensure that the data received from the polling place is indeed the data that was transmitted. Paper records, both physical ballots and paper summary data, provide a simple assurance that is independent of complex technology, while electronic transmission protects against forgery or alteration of the paper records.

For all electronic transmissions, there are technical defenses that can help authenticate the data. This applies to transmissions from the manufacturer to the election authorities, from the election management system to the polling place equipment, and from the polling place to back to the election management system. Broadly speaking, these are generally described as digital signatures or as secure hash codes. These are cryptographic tools for ensuring that a document is authentic and has not been altered.

It is important to emphasize that we are interested in authentication here, not encryption. It is a mistake to require that all election data be encrypted, as is required by the Council of Europe E-voting standards.[35] Encryption, as such, does not prevent or detect alteration, and encryption of information that is publicly known serves no useful purpose.[36] Election results should generally become public records as soon as the polls close, and most of the contents of the election configuration files is public. The only exceptions to this are digital authentication keys for election results transmittal that are included as part of the election configuration. These must, of course, be secured until after the election results have been received and published.

Results publication: The final link in the data flow is from the election management system to the public. Election results must be released. In the days of manual canvassing, it was common for the counting to be conducted in public, with results shown on a blackboard. Anyone could observe the process and copy down the results, and it was trivial for all observers to note that the only ones writing on the blackboard were election officials.

This story changes considerably when computerized election management systems replace the blackboard. With such a system, results from the precincts are entered into a computer, sometimes directly from memory cartridges or by modem, and then the computer declares the result. How can the public be given sufficient access to the election management system that they can observe the election results without granting the public sufficient access to disrupt or alter

[35]Council of Europe, *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*, (September 2004). See item 34. Available at https://wcd.coe.int/ViewDoc.jsp?id=778189&Lang=en.

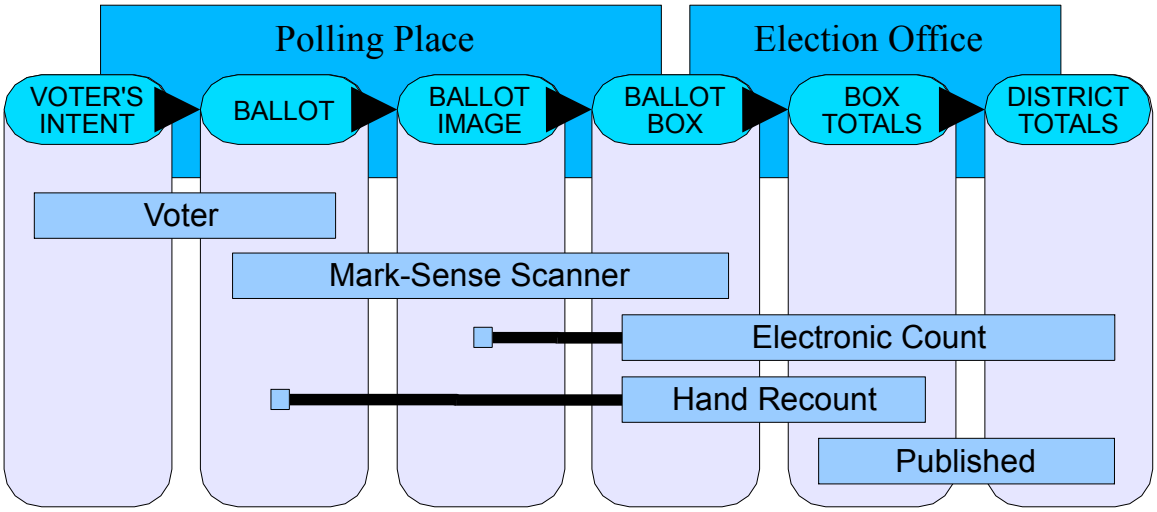
[36]Douglas W. Jones, "Misassessment of Security in Computer Based Election Systems," *Cryptobytes,* 7:2 (Fall 2004), 9-13. Available at http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_Fall2004.pdf.

those results? Many jurisdictions have directly connected their election management systems to the Internet,[37] a very bad idea. Miami-Dade County recognized the dangers of this and invented a defensive scheme that was simultaneously ingenious, extraordinarily complex and impossible to assess.[38] More appropriate solutions involve easily verified one-way data transmission devices. In the literature, these are known as data diodes.[39]

D. The Chain of Custody View

A final perspective that is useful to consider involves the chain of custody of votes and vote totals as they pass from the voter to the final published election results. The term "chain of custody" comes from the rules of evidence in the United States. Evidence presented with a well documented chain of custody can be trusted, while if there is a weak chain of custody, this raises questions about the authenticity of the evidence. Short chains of custody are easier to trust than long chains. Storing evidence in a secret location known to only one custodian is dangerous if that custodian is not perfectly honest. Storing evidence in the hands of multiple custodians who are subject to public oversight is far safer. Similarly, putting multiple copies of the evidence in the hands of independent custodians offers considerable assurance.

Figure 4: The chain of custody for optical mark-sense voting



The chain of custody illustrated in Figure 4 applies to precinct-count optical mark-sense voting—that is, the voting system where voters mark paper ballots that are then tabulated by a mark-sense scanner in the voter's presence. The scanner drops ballots in a secure physical ballot box as it scans them. The scanner records an electronic ballot image of each ballot as it is scanned, and these are stored in an electronic ballot box. At the close of the polls, both the physical and electronic ballot box are transported to the election office. The votes in the electronic ballot box are then counted to produce the totals for that box, and these are then incorporated into the district-wide vote totals.

At each link in this chain, it is fair to ask who has custody of the data and what proof do we have

[37]Science Applications International Corporation, *Risk Assessment Report – Diebold AccuVote-TS Voting System and Processes* (September 2, 2003). See section 2.2.2. Available at http://www.verifiedvoting.org/downloads/votingsystemreportfinal.pdf.
[38]Douglas W. Jones, *Observations and Recommendations on Pre-election testing in Miami-Dade County* (September 9. 2004). See section 7. Available at http://www.cs.uiowa.edu/~jones/voting/miamitest.pdf.
[39]Douglas W. Jones and Tom C. Bowersox, "Secure Data Export and Auditing Using Data Diodes," *Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '06)*, Vancouver, August 1, 2006. Available at http://www.usenix.org/events/evt06/tech/.

that the data correctly reflects the collective intent of the various voters. As the voters mark their ballots, they directly expresses their intent, and election observers can easily observe that the voters themselves place their ballots into the scanner. If the scanner were able to report its interpretation of the ballot to the voter, this would allow the voter to verify not only that the ballot had been scanned, but that it had been scanned correctly. No current scanners do this.

The scanner and ballot box are in the custody of the polling place workers and under observation by the voters and election observers until the polls close. From this point, two distinct chains of custody emerge, one for the electronic data that leads to the district totals, and a second for the ballot boxes and paper ballots.

The electronic records are physically in the custody of the mark-sense scanner software until they are transmitted by modem or extracted to electronic storage media. The notion of software having custody of anything is problematic because the notion of custody usually applies only to people. Nonetheless, the software is able to act independently of its physical custodians, behaving as specified by the programmer or programmers who constructed it and the ballot configuration files that it interprets in order to scan the ballots. This suggests that we must guard secondary chains of custody from the programmers to the machine and from those who prepared the configuration files.

These secondary chains of custody are long and difficult to guard, so many jurisdictions are moving toward a different model based on auditing. In each jurisdiction, after every election, a randomly selected sample of the original paper ballots is subject to a hand count. California pioneered this model in the punch-card voting era.[40] The purpose of this hand count is to verify that the electronic count of those same ballots is accurate. For this hand count to be of any value, we must guard the chain of custody of the paper ballots between the time they are tabulated by the ballot scanner and the time they are subject to hand counting.

In general, the sooner we publish election results, the more difficult it is to fraudulently alter them. If the only published result is the final result, then we must closely guard the chain of custody all the way to the point of publication. If, on the other hand, we publish results earlier, creating multiple copies in the hands of independent witnesses, it becomes far more difficult for later custodians to make alterations without detection. This is one reason why many jurisdictions require that the election results from each polling place be printed in duplicate, with one copy posted for public inspection prior to the transmission of the official copies from the polling place. The procedures for this outlined in Kazakh election law are a good example. This law requires that one copy of the results be posted at the polling place for the public, that additional copies be given to election observers who request them, and that both paper and electronic copies be delivered to the election offices.[41] This early publication allows independent verification of the consolidation of the polling-place results into the final election totals.

IV. Conclusion

Each of the views outlined above serves a different role. The voting equipment life cycle view says more about the voting equipment acquisition process. The election cycle view allows examination of election administration. The data flow view allows evaluation of voting system security, and the chain of custody view helps observers understand the significance of the various pieces of evidence they see. All of these views can play a role in crafting election laws and administrative procedures, and they can play a role in the evaluation of specific voting technologies.

Many of these views reinforce each other. The importance of auditing, for example, emerges clearly in the election cycle, data flow, and chain of custody views. Acceptance testing emerges in

[40]Roy G. Saltman, *Effective Use of Computing Technology in Vote-Tallying* (National Bureau of Standards, March 1975). See page 45. Available at http://csrc.nist.gov/publications/nistpubs/NBS_SP_500-30.pdf.
[41]"On Elections in the Republic of Kazakhstan," *Constitutional Law of the Republic of Kazakhstan* (September 1995). See Chapter 8, Article 43, Section 8. Available at http://www.eurasianet.org/departments/election/kazakhstan/kazelectlaw.html.

both the equipment life cycle and data flow views, while pre-election testing emerges in the election cycle and data flow views. Further examination of these different views can help reveal the nature of the expertise required by the different participants in the process. This is an essential first step that must be undertaken before hiring and training those participants.

The questions raised by the different views of election technology outlined here may appear daunting. Indeed, these issues are daunting. The United States has been using mechanical voting machines for over a century, yet controversies about election technology remain in the headlines today. The Netherlands moved to almost universal use of direct-recording electronic voting machines 20 years ago, yet in their most recent parliamentary elections, controversies about those machines became front-page news. It is clear that these technologies are difficult to administer and that election officials frequently find that they have accepted a burden that is more complex than they are prepared to handle.