Donald P. Moynihan
Texas A&M University

Building Secure Elections: E-Voting, Security, and Systems Theory

The increased use of information technology promises to revolutionize both the provision of government services and the vibrancy of democracy. In the aftermath of the Florida voting controversy during the 2000 presidential election, governments have placed their faith in technology, adopting e-voting machines that offer enhanced voter convenience and eliminate the need for subjective recounts. However, the same underlying assumptions that apply to e-government theory do not apply to e-voting because of the severity of consequences if failure occurs and the loss of transparency traditionally associated with the voting process. A more useful theoretical guide is systems theory, which deals with complex, high-risk systems. This literature has been largely overlooked by adopters of e-voting technology, even though the practical criticisms of e-voting made by computer security specialists reflect an essentially systems theory perspective.

In recent years governments have embraced the idea of using information technology (IT) to improve services, a trend known as *e-government*. In the aftermath of the Florida voting controversy during the 2000 presidential election, governments again placed their faith in technology, adopting e-voting machines that offer enhanced voter convenience and eliminate the need for subjective recounts. The basic assumptions and values of e-government have been applied to the electoral process. This article argues this is a mistake, and that the relative benefits and risks associated with the application of IT are markedly different for e-government and e-voting. E-government is associated with making services and information more accessible; there are limited risks with this approach, and failure in service may create an inconvenience for the individual citizen, but it does not pose fundamental risks for the government. However, the failure of e-voting technology has profound consequences for the reliability of and public confidence in our electoral system. The consequences of a failed election are much greater, and the adoption of e-voting has increased the risk that such failures will occur.

Given the high consequences of election problems, a more suitable theoretical guideline can be found in the aspects of systems theory that deal with high-risk technologies. Systems theory provides a mental framework for describing, modeling, analyzing, and designing social systems; developing and institutionalizing changes to social systems; and managing systems and system change (Banathy 1996, 157). Senge (1990) ties a systems approach to organizational learning, to understanding complex, recurring interrelationships through feedback loops and directing purposeful change. This literature examines the complexity of social processes, where system outcomes are shaped by unpredictable micro-level effects (Stacey 2003). Aspects of systems theory that deal with complex and high-risk technologies are Perrow's (1999) natural accident theory and the high-reliability theory associated with several Berkeley scholars (Frederickson and LaPorte 2002; LaPorte and Consolini 1991; LaPorte 1994, 1996; Roberts 1990). This article finds that computer security specialists have offered specific criticisms and possible policy solutions that closely fit with the basic framework offered by natural accident theory and high-reliability theory.

The first section examines the growth of e-government and describes the e-voting technology that governments are increasingly adopting. The next section of the article examines the potential for failure in complex systems, an at-

Donald P. Moynihan *is an assistant professor at the George Bush School of Government and Public Service at Texas A&M University. He received his doctorate from the Maxwell School of Citizenship and Public Affairs at Syracuse University. His research analyzes the process of selecting and implementing public management reforms. His work has appeared in a number of edited volumes and journals, including* Public Administration Review *and* J-PART. ***E-mail: dmoynihan@bushschool.tamu.edu.***

tribute identified by natural accident theory. The following section examines in detail the attributes of e-voting that make system failure likely, represented by the criticisms of computer security specialists. The next two sections address two obvious questions that arise from this analysis: why did elected officials adopt e-voting technology, and what are the policy implications? Finally, the article offers a series of policy prescriptions, again based on natural accident theory and high-reliability theory, and the analogous principles argued by computer security specialists.

Distinguishing E-Government from E-Voting

President George W. Bush's President's Management Agenda (OMB 2001, 23) declares, "The federal government can secure greater services at lower cost through electronic government, and can meet high public demand for e-government services. This administration's goal is to champion citizen-centered electronic government that will result in a major improvement in the federal government's value to the citizen." The Clinton-era National Performance Review also pointed to IT as a means to "reengineer governmental services" (Gore 1993) and to "serv[e] the public on its terms" (National Partnership for Reinventing Government 1997). E-government has proven to be a durable and popular public management reform option over the last decade, attractive to elected officials of both parties who see its political benefits (Coursey and Killingsworth 2000).

The central premise of e-government is a faith in technology as a way to satisfy customer service expectations, increase the efficiency and effectiveness of government operations, make information more available, increase online transactions, raise participation in government, and meet expectations for trustworthiness (National Research Council 2002). Public management scholarship on e-government focuses on the beneficial effects of new technologies and examines the reasons why and how technology adoption occurs (Abramson and Means 2001; Fountain 2001; Hinnant 2001; Moon 2002; Ho 2002). Such research has not directly questioned the basic premise that e-government is a positive and inevitable route to improvement and progress.

Some e-government proponents argue that declining rates of trust in government can be reversed through the use of technology, either indirectly because of greater citizen satisfaction with more convenient services, or directly through enhancing civic participation in the public sphere. The latter approach has been referred to as "digital democracy," "e-civics," and "e-democracy" (Fountain 2003; Thomas and Streib 2003a). This approach argues that IT can enhance democracy by making public information more accessible and by enabling a range of civic discourse that otherwise would not occur, from facilitating citizen-initiated contacts through the Web (Thomas and Streib 2003b), to enabling a representative and meaningful discourse that replaces the moribund town-hall meeting (Moynihan 2003; Shi and Scavo 2000). As West (2004) notes, however, the potential of e-government in this area has remained largely unfulfilled.

With the rise of e-government and criticisms of existing voting procedures, can IT be used to improve the electoral process? The increased adoption of direct recording electronic (DRE) machines and the pilot testing of Internet voting for presidential primaries and overseas military staff suggests that election officials believe so.

In addition to ensuring the rule of law, there is no public administration task more central to guarding democracy than providing for elections that accurately reflect voters' intentions and ensure public confidence. As the sanctity of elections declines, so too does the legitimacy of the governing regime. In terms of the administration of elections, the controversy surrounding the results of the Florida 2000 presidential election recount had a number of implications. First, it brought to the forefront a previously obscure but powerful group of administrators: election board officials at the state and local level. Second, Florida highlighted the role that existing voting technology plays in shaping the number of votes counted and, in particular, problems associated with punch-card machines. A third effect was the creation of mandates for electoral reform. In October 2002, the federal government passed the Help America Vote Act, which provided federal funding to replace punch-card technology and created the Election Assistance Commission to serve as a national clearinghouse of information on the provision of federal elections.

The aftermath of the Florida election controversy and the passage of the Help America Vote Act put election officials at a crucial juncture in deciding how to replace older voting technology. Many states subsequently passed their own legislation to encourage the adoption of alternative voting technologies. Given the rate at which change is occurring, there are no definitive data on the number of DREs in place, but it is clear they are increasing. A survey of the National Association of County Recorders Election Officials and Clerks (2003) found that 54 percent of those expressing a preference indicated DREs as their choice for a new system, followed by optical-scan ballots with 40 percent. While just 12 percent of voters used DREs in 2000, this figure is expected to increase to 29 percent in 2004 (Seelye 2004).

DREs are the ATM version of the ballot box. When voters arrive at the polling station, they are given a memory card to insert into the machine. Voters select the candidate of their choice using a touch-sensitive screen or parallel

button. The votes are internally tabulated by the machine and reported to a central counting station. In the aftermath of the Florida election, DREs seemed to be an ideal choice. They promised to record each vote perfectly and instantly, doing away with the slow and potentially subjective recounts featuring pregnant, dimpled, or hanging chads. DREs have other advantages: They are user friendly, report votes more quickly, prevent voters from voting for more than one candidate in the same race, and remind voters if they did not vote in a particular race. DREs also promise to help the visually impaired through the use of larger screens and earphones.

The policy changes that followed the Florida controversy signaled the willingness of governments to provide the resources necessary to adopt the most advanced technological solution available, eliminating human error and manipulation, as well as antiquated technologies that plagued the election system. However, as the rest of the article argues, the adoption of DREs creates real risks of failure among election systems.

The Problems of Complex Systems: Natural Accident Theory and the Computer Security Perspective

This article critiques the adoption of DREs based on systems theory and a closely analogous set of claims put forward by computer security specialists. This perspective has not been widely considered in the e-government literature, and it has not been of central concern to election officials thus far.

Charles Perrow (1999) has made a major contribution to systems theory with his examination of high-risk, complex systems. Natural accident theory argues that the central problem of complex systems is that they make accidents inevitable. Errors in multiple parts of complex systems can lead to dramatic and unexpected system failure. The potential for failure increases when the complexity occurs in tightly coupled systems that have the potential for unpredictable feedback loops. System failure, therefore, occurs not as a result of predicted vulnerabilities, but because errors occur and interact in unexpected ways.

Previous election technology could be characterized as relatively simple, with linear and predictable interactions between parts. To varying degrees, the different technologies were imperfect in their ability to count votes, but there was little risk of catastrophic failure. DREs are more complex systems, primarily the result of a highly complex subsystem: the software used to count the vote. "Even a simple computer program has hundreds of thousands of lines of computer code doing all sorts of different things. A complex computer program has thousands of components, each of which has to work by itself and in interaction with all the other components" (Schneier 2000, 6). Complexity in software is associated with analogous demands on hardware. As a result, e-voting hardware is more complex than traditional voting machines, also creating potential risks.

We shall return to a detailed discussion of systems theory literature in the section on policy prescriptions; for now, we will examine how Perrow's natural accident theory is reflected in the concerns of computer security specialists. On the surface, it seems surprising that suspicion of new technologies is coming from the information technology community rather than election boards. But computer security specialists argue that election boards are making a basic error in their understanding of new technology: They overestimate the reliability of technology, assume it will solve existing problems, and ignore the potential for unanticipated consequences and new vulnerabilities. The new technology creates an illusion of security, resulting in machines that are not protected by some measure of redundancy or able to recover from failure.

The work of Bruce Schneier reflects the evolution of thinking among computer security specialists. Schneier's 1993 book, *Applied Cryptography,* became a bible of sorts among security specialists, preaching the ability of advanced cryptography to secure the information of private and public companies and individual citizens. His later works, *Secrets and Lies: Digital Security in a Networked World* (2000) and *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (2003), recanted his earlier claims. The reason for his about-face was a realization that secure systems depend on much more than cryptography. Other factors such as hardware, software, and physical access undermined the ability to create truly secure systems.

To a remarkable degree, Schneier and Perrow overlap in assuming that as complexity increases, system failure becomes not just more likely, but normal and inevitable. Like Perrow, Schneier sees the increased complexity that usually accompanies new technology as a source of new vulnerabilities and risks, even if the technology seeks to fix earlier security problems. In addition to applying systems concepts of complexity, interactivity, and emergent or unanticipated outcomes to computer security, Schneier adds an interpretation of systems theory that is peculiar to computer issues: Systems have bugs—a particular and undesirable property that does not cause systems to malfunction or stop, but to continue behaving in a way that was not intended by its designers. In the case of voting, DREs may appear to count votes, but may do so incorrectly.

Schneier notes the tendency of digital systems to pursue security through prevention, to the exclusion of detection and reaction to failure. Such an approach works only if the methods of prevention are perfect. However, digital

systems have a poor track record in this respect: "Computer insecurity is inevitable" (Schneier 2003, 367). Prevention that relies on verification is always problematic because testing itself is imperfect and is likely to miss bugs that inevitably occur in complex software. Verifying or evaluating security weaknesses becomes more difficult with more complex systems. "Testing for every known weakness is impossible.… Testing for all possible weaknesses means testing for weaknesses that you haven't thought of yet. It means testing for weaknesses that no one has thought of yet; weaknesses that haven't even been invented yet" (Schneier 2000, 337). A case in point is the high number of bugs in Microsoft systems even after hundreds of man-years of testing. The difficulty of identifying weaknesses is more pronounced if vendors face low oversight, thereby reducing the incentive to fix problems.[1]

Assessing System Risks for Election Technologies

This section examines in detail the risks of competing election technologies, informed by the systems theory and computer security perspectives. While convenience and speed are important considerations, the core criterion for an election system is that it accurately translates the intent of the voter. The traditional approach to assessing the effectiveness of voter technology has been the residual vote—that is, votes lost because voters chose more than one candidate, created an unreadable ballot, or left a ballot blank. In the aftermath of Florida, election boards worried about technology that did not properly reflect voter intentions and focused primarily on votes lost by punch-card technology. However, with the advent of more complex election technologies, the residual vote is only one aspect of election-system risk. Two additional and overlooked risks are the potential for tampering and failure and the inability to recover. Including these additional criteria reduces the apparent advantages of DREs and exposes their potential to induce system failure.

The Residual Vote

Based simply on residual votes, DREs are not the most reliable technology. A report by a group of Caltech and MIT social scientists, engineers, and computer security specialists provided evidence on the residual vote associated with different voting technologies based on data from approximately two-thirds of U.S. counties from all elections during 1988–2000 (Caltech-MIT 2001a). The report shows that between 1988 and 2000, the most reliable voting approaches were the oldest technologies: manual ballot counting and levers (table 1).

The data showed punch cards to be the least reliable, a finding that would surprise few familiar with the problems in Florida in 2000. DRE machines were similarly unreliable, although they improved over the observation period, dropping from a 3.5 percent residual rate in 1988 to 1.6 percent in 2000, partly because of greater voter familiarity with DREs and similar technologies, but also because of improvements in user interface. During the same period other technologies also improved, with optical scanning, paper balloting, and the DataVote punch-card machine still being more reliable than DREs in 2000. For governments interested in the most reliable technology for reducing residual votes, DREs are not the solution. A follow-up report explicitly recommended the use of optical scanners for new election systems (Caltech-MIT 2001b). The report noted the reliability of optical scanners and their lower costs.[2]

Table 1 Aspects of System Risks for Election Technology

Type of election technology	Average county residual vote		Technology errors and tampering	Recovery
	Average 1988–2000	2000		
Paper: Voter marks preference next to printed list of options; ballot is dropped into sealed box and manually counted.	1.9	1.3	Ballot-box stuffing possible on a limited scale	Paper ballots for recount
Levers: Voter pulls lever next to candidates name; machine records and tallies record.	1.9	1.7	Tamper with machinery; antiquated machinery may cause error	No paper trail
Optical scanning: Voter marks computer readable paper ballot; computerized tabulation machine tallies votes.	2.1	1.2	Tamper/error with tabulating program	Paper ballots for recount
Punch cards: Voter uses computer readable card to mark vote by punching hole into numbered boxes, indicated by a ballot booklet, or directly onto a ballot card; computerized tabulation machine reads votes by identifying holes in the ballot.				
VotoMatic	3.0	3.0	Tamper with machinery; antiquated machinery may cause error	Paper ballots for recount
DataVote	2.9	1.6		
DRE: Voters select candidate listed on a computer screen by directly touching the screen or button; votes tabulated on computer.	2.9	1.6	Tamper/error with software program	No paper trail

Programming Error and Tampering

A second criterion for evaluating election-system risk is programming error or tampering. Bev Harris (2004), a journalist who became interested in e-voting, found dozens of documented miscounts by election machines—both DREs and optical scanners—which in some cases reversed election results. In most cases, the mistakes were discovered because of obviously incorrect errors, leading to further investigation (for instance, a candidate receiving no votes, more votes being counted than registered voters, or high numbers of unaccounted votes). Less dramatic swings, such as switching every fiftieth vote from one candidate to another, are less likely to be detected and investigated.

Harris also details the ways in which malicious programmers could rig machines. Schneier (2000) argues that all computer security systems must assume the presence of a hacker who will introduce subtle faults that will cause failure at the worst possible time. By definition, the vulnerabilities that hackers exploit cannot be foreseen by programmers, and therefore are unprotected. Such vulnerabilities are more likely to be exploited if an interested actor can profit from a failure, or if a hacker is simply seeking publicity (Schneier 2000, 23-41). In both cases, elections are perfect targets.

The programming software used for DREs is proprietary to the vendor, and therefore it is not publicly accessible. Companies argue this is commercially necessary and reduces the potential for manipulation of the voting machines, an argument known as "security through obscurity" among computer security professionals. One problem with this argument is that it overlooks the potential for internal programming errors in software from vendor programmers, either deliberate or accidental.

The vendor-certification process seeks to catch such errors. Certification of DREs is based on standards created by the Federal Election Commission and implemented through a process established by the National Association of State Election Directors. Vendor products are tested by approved laboratories for states that adopt the standards or by an independent examiner selected by the state. But the certification standards have problems. The General Accounting Office has criticized the standards as not being comprehensive or up-to-date (GAO 2001). New standards were passed in 2002, but they failed to test commercial, off-the-shelf software used in DREs and remain "notably weak in the areas of secure system design and usability," according to computer security specialists (Mercuri and Neumann 2003, 37). A report by a task force commissioned by California's secretary of state highlighted the need for federal standards to be "substantially improved" (Shelley 2003, 7). Computer security consultants for Maryland's board of elections noted, "Unfortunately, there does not exist at this time a clear set of requirements that any voting system must meet … [Existing] guidelines fail to articulate requirements that reflect the unique demands of current all-electronic systems" (Wertheimer 2004, 5). The testing process lacks transparency, as the testing labs (who are paid by the vendors rather than the government) do not provide information about the nature of the tests or the credentials of the testers (Harris 2004). What is known about the testing process offers little evidence that testing examines source code line by line; rather, current testing focuses on hardware stress tests for heat and vibration and examines software on the basis of positive functionality—that is, seeing that the DRE does what it is intended to rather than focusing on points of weakness in the software (Wyposal 2003). Obvious errors are caught, but software bugs that do not occur in a predictable fashion are overlooked, says David Dill (2003) of Stanford's Department of Computer Science. Such unexpected, unseen, and potentially interactive errors are, according to natural accident theory, most likely to create major problems.

Even with this process of certification, the machines in place on election day may not be the same version of the machine that was tested. If a vendor finds internal problems after the machine is certified, it may decide to add a patch to eliminate the problem before election day. For instance, 17 counties in California found that their DRE vendor, Diebold, had run software on machines that were not certified by the state and, in some cases, were untested. After glitches occurred in primaries during March 2004, the secretary of state banned the use of 14,000 Diebold DREs in the November elections (Schwartz 2004). In Georgia, Harris (2004) details Diebold's effort to fix malfunctioning DREs before facing additional state testing. Both instances violated state election law. Such actions question the validity of the federal testing process, which did not catch the problems, and the lax oversight of the DREs operating on election day.

Of course, tampering can occur in any election system. Vote rigging has a long and dishonorable history in American politics (a fascinating example is provided by Caro 1990). However, the Caltech-MIT report notes that the potential for manipulation is greater with DREs: "We are also concerned about the secretive and proprietary treatment of tabulation software of all electronic voting. The fraud that occurs one ballot at a time or one lever pull at a time accumulates slowly like grains of sand on a scale. We are more concerned about someone putting his or her thumb on the scale" (2001b, 10). While tampering and error can occur with older technologies, it would require a great deal of coordination to perpetuate voting fraud on a vast scale without being detected. Computer security specialist Roy Saltman noted as early as 1988 that such manipulation might be impossible to uncover, prove, and correct.

The proprietary nature of DRE software code has meant that criticisms could be made only indirectly, based on suspicions and infrequent acknowledgments of problems. However, the alleged source code of one of the primary DRE vendors, Diebold, became available in January 2003, apparently left unsecured on the company's Web site. This provided an opportunity for computer security specialists at Johns Hopkins and Rice universities to undertake a line-by-line analysis of the source code, which revealed several vulnerabilities with the software (Kohno et al. 2003). The authors concluded, "The model where individual vendors write proprietary code to run our elections appears to be unreliable, and if we do not change the process of designing our voting systems, we will have no confidence that our election results will reflect the will of the electorate" (Kohno et al. 2003, 22).

Diebold responded that the software examined was outdated. The state of Maryland had been considering adopting Diebold as a vendor at the time and employed an external consultant, Science Application International Corp., which found vulnerabilities in the Diebold DREs but concluded they were fixable. A second independent consultant, RABA Technologies, found that many of the software vulnerabilities identified in the Johns Hopkins report still existed and that the Diebold machines were vulnerable to hacking, but again concluded that fixes could be undertaken (Wertheimer 2004). Less important than the specific failures was the closed-source system that had produced the vulnerabilities. Such failures could be addressed with fixes, but they did not come to light without external oversight. Without continued oversight, vendors are likely to produce other errors again in the future.

Ability to Recover

Schneier declares that "good security systems are designed in anticipation of possible failure" (2003, 58). This means that systems should be designed not only with an emphasis on prevention, but also with an assumption that prevention will fail and countermeasures will be needed. Well-designed systems, therefore, should fail smartly, incorporating an ability to recover quickly, retracing and remedying the failure if possible. Schneier describes systems that fail badly as brittle and systems that fail well as resilient: "Good security systems are resilient. They can withstand failures, a single failure doesn't cause a cascade of other failures. They can withstand attackers, including attackers who cheat. They can withstand new advances in technology. They can fail and then recover from failure" (2003, 120).

Because DREs are designed and marketed on the assumptions that preventative measures are foolproof and failure will not occur, DREs are brittle. If DRE security is breached and programming or some other type of failure occurs, such a failure interacts with the inability to independently verify the vote tally. With other approaches to voting (apart from levers), close or contested elections can verify voters' intentions through an ex post examination of the paper ballots. With DREs such an option is not standard. DREs have an internal paper record that can be examined after the election, but this is the same basis for the original tabulation of votes, and therefore it is not an independent verification. In short, if a machine is sufficiently damaged, or if it produces questionable results, it is impossible to examine what the voters' original intentions were. Even the imperfect recounts of punch-card ballots employed in Florida provided some representation of voter intentions. The brittle nature of DREs is such that if DRE failures are significant enough to throw an election into question, the only alternative to accepting the results would be to rerun the election.

Adopting DREs

Given the risks associated with DREs, why are so many states turning to this technology? Three theories offer explanations, illustrated by examples from the state of Georgia. The first explanation is a general faith in technology among administrators. As discussed previously, a basic assumption of e-government is that information technology is a benign force that helps to improve the public sector, and newer and more sophisticated technology is an improvement on older systems. This faith in technology is consistent with a wider public-sector reform ethos: March and Olsen (1983) explain how public administration reforms represent an expression of values and a belief in rationality. In the same way, the adoption of technology communicates to the public that government is modern and innovative, valuing technology and its benefits. Moon and Welch (2003) report such attitudes among administrators. Their comparison of attitudes of administrators and members of the public finds that bureaucrats tend to express a desire for rapid implementation of e-government driven by a high degree of general confidence in IT, particularly its ability to provide more convenient and efficient public services. Members of the public are less confident about the promise of e-government, express much greater concern about security and privacy, and favor slower implementation.

In general, administrative faith in new technology is welcome because it usually provides for enhanced productivity and convenience. But the assumption that new technology will always lead to improvement has not proven true in the area of election reliability; the most basic of technologies—hand-counted ballots—have proven more reliable in terms of residual vote than all other technologies, barring the optical scan. Punch cards

introduced in the 1960s were not more reliable than the lever machines that predated the twentieth century. DREs are not more reliable than optical-scan technology. For generations, election boards have gradually eliminated older technologies in favor of newer ones that do not count votes as reliably.

The current move toward DRE machines appears to represent one more reform based on a misplaced trust in technology. In Georgia, the secretary of state who had championed DREs pointed to voter satisfaction with and confidence in the new machines as a measure of success, consistent with the e-government emphasis on customer service (Cox 2002). The secretary of state's Web site includes a motto of "advancing the e-government revolution," and her biography boasts of e-government achievements.[3] Her ability to rapidly implement DREs won Secretary Cox national praise, including a 2002 Public Official of the Year award from *Governing* magazine.

A second explanation is based on the administrators' perceptions of risk. In evaluating risk and security options, Schneier (2003) calls for decision makers to explicitly recognize the trade-offs between the size and likelihood of the threat on one hand, and the costs of actions to reduce the threat on another. But there are at least two factors that limit the ability of decision makers to make such trade-offs. The first is that assessing the costs and benefits underlying trade-offs is a subjective exercise, and individuals often do not evaluate risks well. For example, individuals tend to overestimate the risks of occurrences that receive a large amount of media attention and underestimate the risk of occurrences that do not. The second factor is that assessment of risk also occurs in political context, where players have different agendas and leverage different degrees of power to determine the outcome. It is the subjective perception of powerful decision makers, therefore, and the interests that lobby them, that are the key determinants of how risk trade-offs are assessed in practice (Sagan 1993).

The outcome of the 2000 Florida elections sensitized election officials to residual votes, problematic recounts, and antiquated technology. The unreliability of punch-card technology was a known entity and had been flagged prior to Florida (Saltman 1988). However, Florida served to illustrate the dramatic consequences of unreliable technology in a close election. A high residual vote was no longer a tolerable option. Florida also provided a window of opportunity within which there was political support for change. In Georgia, the 2000 residual vote was above that reported in Florida, but it did not garner immediate attention because the results were not close. In the aftermath, Secretary Cox and other proponents of e-voting repeated a variation of the theme that "we could be the next Florida."

As election officials became aware of and concerned with the risks of punch-card technology, they appear to have given this factor primary consideration over other criteria for assessing voting reliability. Learning from system failure is rare, problematic, and often erroneous (Perrow 1999, 371). Like generals preparing to fight the previous war, election officials sought technology that would prevent them from becoming the next Florida. Programming error and ability to recover were not given significant consideration. To a limited degree, this has changed. Revelations about Diebold and the arguments of members of the information security community have created an active and public debate about problems with DREs, and some governments have rejected moving toward this technology.

A third explanation derives from principal–agent theory. In this explanation, the election officials (the principals) are at an information disadvantage relative to the agents (the vendors of DRE), and they are unable to make fully informed decisions. Because of the closed-system approach to software and the inability to provide an adequate independent audit, election officials have weak sources of information to assess a highly complex product. As a result, election officials struggle to specify the product they want or to verify the technology in operation is the same as the product they were sold. They can specify the outcome they want (low error in voting), but they cannot fully verify whether this outcome has occurred or whether failures in the system have occurred instead. The vendors are often represented by lobbyists who are closely connected with state government or by former election officials, adding aspects of power and interests to the risk-assessment process. In Georgia, Diebold was represented by a former secretary of state (Pettys 2002). Election officials trust in testing to ensure the product is reliable, but the standards of those tests have been questioned, and the technology in operation may not be the same as the one tested. They contract with vendors with greater experience but fail to ask the right questions about tampering or the ability to audit (Harris 2004). The Caltech-MIT Voting Technology Project describes the scenario, "Because of the long shelf life of the product—twenty years or more—relationships between a county and its vendor are long-term. Contracts are negotiated each time a new equipment purchase is made, often between savvy veterans from the company sales force and county officials who rarely, if ever, negotiate any major contracts and are unlikely to have negotiated a previous contract for election equipment" (2001b, 53). Such asymmetry may be reduced by competitive firms who find it in their interest to do so, but the DRE industry is dominated by three major firms whose share of the marketplace has increased from 74 percent in 2000 to 89 percent in 2002 (Fischer 2003, 22).

It is difficult to determine which of these theories is relevant for the adoption of DREs. Clearly, additional empirical research is needed on the factors that shape election officials' perceptions of DREs and competing technologies. It is worth noting, however, that the theories are not in direct conflict with one another. A combination of faith in technology, a blinkered assessment of risk, and information asymmetry may explain the adoption of DREs.

Policy Implications

The most critical and obvious policy implication of DREs is that they may undermine the electoral process, the basis for representative democracy. While all election technologies have risks of error or manipulation, the danger of DREs is that the manipulation could be catastrophic and would be extremely difficult to detect or prove.

A second policy implication is that the rapid adoption of these technologies creates a risk that governments will become locked into suboptimal technology. New electoral technologies are expensive relative to their level of use. Once adopted, governments are slow to replace a technology, which explains why lever machines and punch-card technology still served the majority of voters until 2000 (Caltech-MIT 2001a, 5). Given the investment in resources and previous commitment to DREs, governments may remain committed to DREs and deny the possibility of error. For instance, the secretary of state in Georgia criticized the Johns Hopkins report that highlighted weaknesses in the Diebold system the state had purchased, arguing the tests had not been done in realistic conditions (Witte 2003). The follow-up report by an independent consultant, which identified 328 vulnerabilities in the Diebold system (26 of them serious), was characterized by the secretary as a "you're-healthy-but-you-need-to-exercise-more" kind of report (Galloway 2003). When Diebold machines malfunctioned in Broward and Dade counties in Florida, Georgia did not see these failures as technological, but as human. A report issued by the secretary of state did not acknowledge any vulnerabilities with the DREs, saying, "Georgia learns from this experience and increases the amount of training made available to poll workers" (Cox 2003, 13).

Clarke (1999) has identified the tendencies of corporations and cooperating governments to downplay system risk and to use organizational rhetoric to exaggerate the ability to recover. Such official statements—"fantasy documents"—operate primarily as symbolic documents that are intended to reassure the public. The degree of uncertainty associated with failure is glossed over, and risks are portrayed as manageable, based on comparisons with previous recovery experiences that are not analogous to the risk at hand. Georgia's guide to election reform (Cox 2003) presents increased user satisfaction and reduced residual vote as proof of the efficacy of DREs, but it ignores other vulnerabilities associated with the technology. It identifies previous technologies as problematic given their high rate of residual voting, but it does not mention the problems that Georgia experienced with DREs. Instead, the document emphasizes the thoroughness of the verification process and the state's proactive efforts to educate voters and to train poll-workers in the new technology.

A third policy implication is public confidence in the electoral process. An explicit goal of the Help America Vote Act and the state adoption of DREs was to restore public trust in this process; however, as evidence of the risks associated with these systems comes to light, the public will become more skeptical, especially in the absence of a recount mechanism. As Schneier (2003) notes, decision makers may adopt technology that aims to increase voters' feeling of security but provides little additional basis for doing so. Governments tend to be highly concerned about reassuring the public, and therefore they may adopt technology that provides a palliative. The general public does not currently perceive the risks posed by DREs, which enjoy increased user satisfaction and confidence over previous election technologies. Having used levers and punch cards, and having witnessed the weaknesses of these systems in Florida, DREs appear to represent a positive alternative. However, the nature of DRE failures will, in time, lead to negative press reporting and growing suspicion. In Georgia, the 2002 election was hailed as a success by the secretary of state, notwithstanding reports from Republican poll watchers that some machines had registered votes for Democratic candidates when the voter had selected a Republican, and the temporary disappearance of a number of memory cards (Stanford 2002a; Tagami and Stanford 2002). Other observers saw a conspiracy in the election, linking the surprise defeats of incumbents in the senate and gubernatorial race to the introduction of the new technology (Gumbel 2003). While the majority of the public may not give credence to such theories, outcomes that appear anomalous (such as the Texas county where three winning Republican candidates received exactly 18,181 votes each, or the Florida precinct that reported –16,022 votes for Al Gore in 2000) are likely to undermine public confidence in elections.

Policy Options: Moving from Normal Accidents to High Reliability

Systems theory and computer security specialists not only provide parallel criticisms of DREs, but also offer analogous solutions. Given that natural accident theory considers accidents to be inevitable, it would seem more useful to look to high-reliability theory. This theory is based on the premise that, although accidents will occur, there will be variation in the distribution of accidents among

organizations with similar properties (LaPorte and Consolini 1991, 22). High-reliability organizations that are more successful at reducing risk have some common characteristics that can be learned.

There has been some controversy as to whether high-reliability theory and natural accident theory represent competing (Sagan 1993) or complementary theories. LaPorte (1994) argues that a distinction between the "pessimistic" view of natural accident theory and the "optimistic" approach of high-reliability theory is overdrawn. High-reliability theorists see their work as a complementary outgrowth of Perrow's observations and call for "a more integrated or cumulative approach" (LaPorte 1994, 211). While pointing to differences, Perrow (1999, 372) also acknowledges overlap. Both theories assume the difficulty of constructing error-free systems in organizations featuring "garbage can" processes. Critically, Perrow acknowledges the basic point of high-reliability theory: that variation in the ability to reduce (though not eliminate) error can be explained by system characteristics.[4]

Can these streams of systems theory help to move the current approach to DREs toward a high-reliability model? Frederickson and LaPorte (2002) review high-reliability theory, outlining many of the necessary components for high-reliability organizations (LaPorte and Consolini 1991; LaPorte 1996). There is a wide gap between these criteria and the current way that DREs are adopted, overseen, and managed. High-reliability systems require "extraordinary levels of technical competences, sustained high technical performance…and processes that reward error discovery and reporting and a continual search for system improvement" (Frederickson and LaPorte 2002, 36), and "the availability of venues for credible operational information on a timely basis" (38).[5] The potential for software problems, the existence of information asymmetry between vendors and election boards, the proprietary nature of software, and an inadequate certification process reduce the potential for these criteria to be satisfied.

Instead of matching the criteria of high-reliability organizations, the current approach to DREs looks more like a complex system destined for Perrow's normal accidents. Not only do DREs feature complex interactivity and tight coupling, they also feature many of the error-inducing characteristics that make complex systems prone to failure. The specialization of different actors in the process reduces the awareness of interdependencies and creates limited understanding of important processes. With DREs, election workers face a technology they have received limited training in and may not be able to recognize or correct a major malfunction. Perrow also points out dangers where the operating scale of the system grows rapidly with little time to build a bank of experience, a pattern that matches the developments of DREs. Internal company e-mails and programmer notes from Diebold reveal the pressure and concerns that employees expressed given the deadlines they faced (Kohno et al. 2003), and the infrequency of elections provides limited opportunity to build experience in dealing with problems. High-reliability theory emphasizes the importance of training as a means to prepare for unexpected occurrences and complex technologies and to create a culture of reliability (Roberts 1990). But lack of close and continuous control over staff—either the staff that run the elections or the contractors that provide the technology—limits opportunities for training or for preventing malicious or inept behavior (Perrow 1999).

In addition, Perrow argues that failures are more likely to occur when there is low organizational density of the system environment with interested parties. Again, this matches the current DRE approach to elections. Traditional core principles of the electoral process include external transparency to interested groups who can verify and check the actions of one another, public control of voting equipment, and the ability to audit systems (Caltech-MIT 2001b). These standards resemble many of the key tenets of accountability in public organizations or public policy making—transparency, checks and balances, external and independent audits—and are based on the assumption that government institutions may be targets of manipulation, but that the wide involvement of its citizenry and interested parties reduces the potential for corruption or error. The current approach to DREs has undermined these basic tenets of safety: The ability to observe the process is much more limited because the tabulation and transfer of votes is now done electronically, and the process by which this occurs can be neither observed nor understood by concerned actors. It is not that there are no longer disinterested parties in the organizational environment, but that the DRE technology has reduced their ability to monitor the system.

Can the situation be reversed? Can DREs be made reliable, impervious to error? The two most far-ranging policy prescriptions made by computer security professionals again reflect a systems theory perspective. A proposal to create voter-verified paper copies of DRE votes is a form of redundancy. A proposal to open the internal workings of DREs to external review draws on the systems theory prescription for external oversight of systems. With these and other changes, DREs are in a better position to adopt the characteristics of high-reliability organizations (Frederickson and LaPorte 2002).[6]

Voter-Verified Paper Trails

Schneier (2003) argues that when prevention fails (which is always), detection and recovery countermeasures should be in place. Such countermeasures need not rely on complex technology. Audits are a traditional and effective ex

post form of detection employed in financial transactions which could also be applied to e-voting. Audits help to identify system failure, evaluate why the failure occurred, and deter wrongdoers by exposing them to the risk of detection. Frequent random audits are a particularly useful form of deterrence because adversaries can never be sure how to successfully disguise an attack to prevent an audit.

To audit an election requires a basis on which to assess the intention of the voter. Traditionally, paper ballots have performed this function for all types of voting bar-lever machines. Optical-scan technology is based on paper inputs, and therefore has a record in case of disputed elections, although not all states permit the use of these paper ballots for audit purposes. If an election were in doubt, it could be rechecked against a paper record, but DREs are not designed to provide such a record.

Critics of DREs have called for adding printers that provide a voter-verified paper receipt, while vendors and some election officials have countered that such printers are unnecessary and expensive. Adding such a function would create redundancy in the system. The concept of redundancy accepts the potential for any part of a system to fail and limits the impact of tightly coupled systems, where failure in one part of the system drags down another (Landau 1969). To reduce the potential for failure of components to bring down the entire system, a redundant component should be included to back up in case of failure. High-reliability theory scholars have embraced the idea of redundancy as a means of reducing error in high-risk systems (Roberts 1990).

A voter-verified paper trail would enable a recount if a machine was unable to tabulate a vote or if its vote totals were suspect. Voters could assess whether their vote was reported accurately by the computer and could alert poll workers if the machine was not recording correctly. The paper votes, once verified, would then be deposited in a ballot box to be reviewed if necessary (Mercuri 2002).

The problem with redundancies is that they increase costs while only infrequently, if ever, providing a demonstrable benefit. This has led to a conflict between proponents of redundancy and the traditional efficiency perspective in public administration (Frederickson and LaPorte 2002). Consistent with this approach, the addition of voter-verified paper trails has been resisted thus far by election officials, who balk at the additional costs involved, in terms of printing and maintenance of machines, and recounting ballots.[7] In Georgia, Secretary of State Cox resisted calls for paper ballots, citing costs and increased risks: "There is a hundred times more opportunity for mischief with a paper ballot" (Stanford 2002b). The state of California also struggled with the costs and additional complexity of printing paper ballots (Shelley 2003) before deciding to require all DREs to provide a paper trail in 2003.[8]

System Transparency

Openness and oversight can also prevent system failure. Perrow (1999) argues for increasing the oversight of interested parties in the systems environment, while Frederickson and LaPorte (2002) point to the need to examine operational information and to create incentives to find and eliminate error. As LaPorte (1996, 65) notes, "Aggressive, knowledgeable 'watchers' increase the likelihood that reliability enhancing operations/investments will be seen as legitimate by corporate and regulatory actors." This transparency is crucial not only to reduce error, but also to ensure public trust in a system: "The higher the potential hazard associated with HRO [high-reliability organization] operations, the more critical is the organization's proper conduct. Put it another way, trust is sustained (or in the more demanding case, recovered) when the more one knows about the agency or firm, the more confident one is that hazardous processes are, and will continue to be, done very well" (LaPorte 1996, 68). Trust demands, among other things, the pursuit of technical operations where consequences can be clearly understood by much of the public, rigorous internal review, and continuous involvement of stakeholders (LaPorte 1996, 68).

The proprietary nature of DRE software is in conflict with these recommendations. It is also in conflict with the views of computer security specialists, who view the security-through-obscurity approach as discredited, especially with complex computer programs that are inherently more likely to contain bugs. The only way to identify such bugs is through more widespread evaluation and use. An open-source approach to election software offers an alternative to the current security-through-obscurity approach. Software would be available to all citizens to be examined and critiqued, increasing the incentive for vendors to produce products that avoid errors, since such errors would be exposed, thereby resulting in adverse publicity and attacks to the product.

The Johns Hopkins researchers demonstrated the benefits of this approach when their criticisms led to improvements in the Diebold DREs in Maryland and Georgia. They argue that "an open process would result in more careful development, as more scientists, software engineers, political activists, and others who value their democracy would be paying attention to the quality of the software that is used for their elections" (Kohno et al. 2003, 22). Cautioned by the experience of the United States, Australia took an open-source approach to election software. Private companies designed the code, but to the specifications of public election officials. The code was posted on the Internet to allow for external review and criticism. After the information had been posted, revisions were made as a result of feedback from those who had studied it, as well as by independent auditors.

While elections have traditionally relied on principles of transparency and the inclusion of parties with competing interests to avoid error or fraud, the use of DREs reduces the ability of interested parties to verify what is occurring. High-reliability theory writers suggest this is because high-risk organizations are wary of close vigilance and real input from their external environment, operate defensively, and seek to manage oversight using political rather than scientific arguments (Mannarelli, Roberts, and Bea 1996). The oligopolistic nature of the market has increased the ability of the dominant firms to resist the external oversight that open-source software offers. Schneier (2003) argues this is a classic mistake in security. New technology not only creates new vulnerabilities, but also sidelines the creativity, ingenuity, and adaptability that people exhibit—but that machines do not. Open-source software would provide at least one avenue by which the officials who run the system would be subject to informed public oversight, maintaining a role for people in security systems, exploiting their ability to adapt to changing situations, and recognizing anomalies. Such a move should not necessarily spell the demise of the vendors, who could still maintain a viable product by maintaining proprietary control over software responsible for user interface and by adopting a service-oriented business model, offering training to election officials on the internal workings of the vote-tabulating parts of the machine.

Conclusion: The Difficulties of System Change

Employing an open-source approach to DREs is consistent with the recommendations of systems theory, traditional approaches to keeping elections honest through a high level of transparency, and the rejection among computer security specialists of the security-through-obscurity approach. It is important to note, however, that high-reliability theory does not suggest the characteristics of high-reliability organizations can be easily adopted. The conditions recommended are not common to all organizations, are difficult to apply, and demand substantial internal change, particularly in terms of organizational culture (LaPorte 1994).

Proposals for voter-verified trails and open-source systems require a willingness to move toward a different model of contracting with vendors, one in which the software involved in tabulating votes would no longer be proprietary. This would reassert the public ownership of the process, requiring a willingness among election officials to clearly specify the product they are ordering and to take responsibility for inspecting it, rather than relying on vendor discretion and support. As Roberts (2004) has noted, increased outsourcing may mean that the commercial preferences and motivations of private vendors will shape the technology behind the provision of public services. Such changes are likely to meet with resistance from the current oligopoly of vendors. The Caltech-MIT Voting Technology Project (2001b) lamented the growing loss of public control over voting machines, asserting that the public-good nature of elections, combined with their importance to democracy, demands direct government control.

Such control demands an enhanced internal capacity, which could be established by hiring technical specialists to support state boards of elections (Saltman 1988). Thus far, local election boards and state election officials have a poor track record of identifying vulnerabilities with the new DREs, partly because of a lack of IT capacity to assess technology risks. Such risks have been flagged and solutions offered by a loose community of concerned citizens, computer security specialists, and academics who have provided the IT capacity lacking in existing structures of public oversight. Organizing on the Internet, this group provides evidence of the possibilities of intelligent civic e-participation. However, the very need for and existence of this form of protest indicates a gap in governmental capacity.

The limits of state and local capacity also raise the question of whether more central oversight of the system is needed in the form of direct federal involvement in setting and testing standards. The Help America Vote Act created a Technical Guidelines Development Committee to establish national standards for voting. However, the initial guidelines simply adopt existing standards, the process remains voluntary, and the current processes for testing through selected laboratories remain in place.[9] Even a moderately centralized process has risks. High-reliability theory warns of the need for local discretion in dealing with developing situations. National standards may not anticipate possible vulnerabilities, an adherence to standards may be substituted for an emphasis on real security, and the voluntary nature of participation may lead states to exit the process if it raises the costs of testing, replacing, and producing e-voting machines (Fischer 2003, 25). In addition, the slow process of creating standards makes it likely that it will take some years for new federal standards to be developed and implemented, reducing the flexibility needed to accommodate new conditions and innovations. For instance, standards recommended in a 1984 report by the General Accounting Office and the National Institute of Standards and Technology were not adopted by the Federal Election Commission until 1990 (Caltech-MIT 2001b, 73). If a more centralized approach is to be taken, these concerns must be addressed.

The changes proposed in this article would increase reliability, but they may not be enough to avoid error. As Perrow (1999) notes, redundancies themselves can fail and may even increase the risk of error. A problem with the

proposed voter-verified paper trail is the assumption that the hard copy represents what is actually recorded in the DREs internal tabulation (Saltman 1988). It may be possible to write a program that prints out the correct data but actually records different outcomes. Even if this were the case, it would still be better to have a correct hard copy to check against the results of the DRE. More prosaically, printers could jam or break down, causing delays and increasing confusion among voters. While open-source software would provide greater oversight and security, it still may be subject to manipulation. Open-source operating software such as Linux has not suffered the same security issues as Microsoft, but it has had problems. Furthermore, it would be difficult to completely verify that the open-source software published is indeed the software actually featured on DREs on election day. The bottom line of such a pessimistic viewpoint is that there is no such thing as a completely secure electronic system, and therefore e-voting will never be error free. However, given current trends in the adoption of DREs, it may be better to seek a system that moves DRE toward high reliability rather than rejecting technology that will be adopted anyway.

Notes

1. For commercial software, this problem has been addressed by a full-disclosure approach, in which security specialists simply publicize product weaknesses, forcing companies to react quickly to reduce adverse publicity and minimize attacks.
2. Optical scanners have lower acquisition costs but higher operating costs, so the estimate of lower costs assumes a 15-year life span. Over 20 years, the costs of DREs and optical scanners are similar.
3. Available at http://www.sos.state.ga.us/misc/cathybio.htm.
4. The error-reducing characteristics that Perrow (1999) identifies are experience with operating scale; experience with critical phase; availability of information on errors; organizational control over members; and organizational density (a rich environment ensures persistent investigation).
5. The complete list of characteristics of high-reliability organizations proposed by Frederickson and LaPorte (2002) is divided into internal and external properties. Internal properties are adequate financial and human resources; a strong sense of mission valence; a culture of reliability and organizational and managerial properties that include extraordinary levels of technical competence; sustained high technical performance; regular and continuous training; structural redundancy; flexible decision-making processes involving operating teams; collegial, decentralized authority patterns in the face of high-tempo operational demands; and processes that reward error discovery and reporting and a continual search for system improvement. The external properties of reliability organizations are based on the nature of top-down governance, policy making, and oversight (that is, governmental structure); the visibility or salience of the high-reliability system to the governing body or bodies; the presence of stakeholder groups; mechanisms for managing boundaries between the high-reliability systems and governance, often in the context of protecting the system and its technology from external influences and buffering the effects of contextual turbulence; and the availability of avenues for credible operational information on a timely basis.
6. A number of more minor suggestions have been made to further reduce the potential for error. These include moving toward a more simple and secure tabulating mechanism, one separated from the more complex user interface; removing the "test" status on DREs, thereby eliminating the chance there will be differences in the DRE actually tested and employed on election day; and frequent random audits of machines beyond disputed elections (Caltech-MIT 2001).
7. Recounting paper votes could be done more quickly by including a barcode on the printed paper that would enable another tabulating machine (produced by another manufacturer) to automatically count the paper votes (Mercuri 2002). Such a move would allow large-scale cross-checks of DREs and paper ballots.
8. There are also efforts to pass a bill in Congress that would require all machines in federal elections to include voter-verified paper trails. However, H.R. 2239 has struggled to find bipartisan support and failed to emerge from the House Committee on House Administration.
9. The committee will be chaired by the director of National Institute of Standards and Technology and will include representatives of the Institute of Electrical and Electronics Engineers, who will be responsible for developing new standards (Fischer 2003, 23).

References

Abramson, Mark A., and Grady E. Means. 2001. *E-Government 2001*. IBM Center for the Business of Government Series. Lanham, MD: Rowman and Littlefield.

Caltech-MIT Voting Technology Project. 2001a. Residual Votes Attributable to Technology: An Assessment of the Reliability of Existing Voting Equipment. Version 2, March 30. http://www.vote.caltech.edu/Reports/index.html.

———. 2001b. Voting: What Is, What Could Be. http://www.vote.caltech.edu/Reports/index.html.

Caro, Robert A. 1990. *The Years of Lyndon Johnson: The Means of Ascent*. New York: Alfred A. Knopf.

Clarke, Lee. 1999. *Mission Improbable: Using Fantasy Documents to Tame Disaster*. Chicago: University of Chicago Press.

Cox, Cathy. 2003. Touch the Future of Voting: Georgia's Guide to Election Reform. Georgia Secretary of State. http://www.sos.state.ga.us/elections/georgia_guide_election_reform.pdf.

Coursey, David, and Jennifer Killingsworth. 2000. Managing Government Web Services in Florida: Issues and Lessons. In *Handbook of Public Information Systems*, edited by G. David Garson, 331–44. New York: Marcel Dekker.

Dill, David. 2003. Openness and Security. Paper presented at the "Building Trust and Confidence in Voting Systems" conference, National Institute of Standards and Technology, December 10. http://www.vote.nist.gov/agenda.html.

Fischer, Eric. 2003. Election Reform and Electronic Voting Issues (DREs): Analysis of Security Issues. Congressional Research Service Report No. RL32139. Washington, DC: Library of Congress.

Fountain, Jane. 2001. *Building the Virtual State: Information Technology and Institutional Change*. Washington, DC: Brookings Institution.

———. 2003. Electronic Government and Electronic Civics. In *Encyclopedia of Community*, edited by Barry Wellman, 436–41. Great Barrington, MA: Berkshire.

Frederickson, H. George, and Todd LaPorte. 2002. Airport Security, High Reliability, and the Problem of Rationality. *Public Administration Review* 62(Special Issue): 33–43.

Galloway, Jim. 2003. OK for Voting Machines Relieves Officials. *Atlanta Journal-Constitution*, September 28, 4C.

Gore, Albert. 1993. Reengineering through Information Technology: Accompanying Report of the National Performance Review. http://govinfo.library.unt.edu/npr/library/reports/it.html.

Gumbel, Andrew. 2003. All the President's Votes? A Quiet Revolution is Taking Place in U.S. Politics. *The Independent*, October 14, 2.

Harris, Bev, with David Allen. 2004. *Black-Box Voting: Ballot Tampering in the 21st Century*. Renton, WA: Talion Publishing. http://www.blackboxvoting.com/.

Hinnant, Chris. 2001. Adoption of E-Services in State Agencies. Paper presented at the annual meeting of the American Political Science Association, August 30–September 2, San Francisco, CA.

Ho, Alfred Tat-Kei. 2002. Reinventing Local Governments and the E-Government Initiative. *Public Administration Review* 62(4): 434–45.

Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan Wallach. 2003. Analysis of Electronic Voting System. Institute of Electrical and Electronics Engineers. http://avirubin.com/vote.pdf.

Landau, Martin. 1969. Redundancy, Rationality, and the Problems of Duplication and Overlap. *Public Administration Review* 29(4): 346–58.

LaPorte, Todd R. 1994. A Strawman Speaks Up: Comments on The Limit of Safety. *Journal of Contingencies and Crisis Management* 2(4): 207–11.

———. 1996. High Reliability Organizations: Unlikely, Demanding, and at Risk. *Journal of Contingencies and Crisis Management* 4(2): 60–71.

LaPorte, Todd R., and Paula M. Consolini. 1991. Working in Practice but Not in Theory: Theoretical Challenges of High Reliability Organizations. *Journal of Public Administration Research and Theory* 1(1): 19–47.

Mannarelli, Thomas, Katherine H. Roberts, and Robert G. Bea. 1996. Learning How Organizations Mitigate Risk. *Journal of Contingencies and Crisis Management* 4(2): 83–92.

March, James G., and Johan P. Olsen. 1983. Organizing Political Life: What Administrative Reform Tells Us about Government. *American Political Science Review* 77(2): 281–96.

Mercuri, Rebecca. 2002. A Better Ballot Box: New Electronic Voting Systems Pose Risks as Well as Solutions. *IEEE Spectrum*, October, 46–50. http://www.notablesoftware.com/Papers/1002evot.pdf.

Mercuri, Rebecca T., and Peter G. Neumann. 2003. Verification for Electronic Balloting Systems. In *Secure Electronic Voting*, edited by Dimitris A. Gritzalis, 31–42. Boston: Kluwer Academic Press.

Moon, M. Jae. 2002. The Evolution of E-Government among Municipalities: Reality or Rhetoric? *Public Administration Review* 62(4): 424–33.

Moon, M. Jae, and Eric W. Welch. 2003. Same Bed, Different Dreams? A Comparative Analysis of Citizen and Bureaucrat Perspectives on E-Government. Paper presented at the annual conference of the American Political Science Association, August 28–31, Philadelphia, PA.

Moynihan, Donald P. 2003. Normative and Instrumental Perspectives on Public Participation: Citizen Summits in Washington, DC. *American Review of Public Administration* 33(2): 164–88.

National Association of County Recorders Election Officials and Clerks. 2003. Results of the Fax-Back Survey as Submitted by Election Officials. http://www.nacrc.org/interest_groups/ElectionsAdmin/pdf/FaxBackSurvey.pdf.

National Partnership for Reinventing Government. 1997. *Access America: Reengineering Through Information Technology*. Washington, DC: U.S. Government Printing Office.

National Research Council. 2002. *Information Technology Research, Innovation, and E-Government*. Washington, DC: National Academy Press.

Perrow, Charles. 1999. *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press.

Pettys, Dick. 2002. State Makes $54 Million Deal to Modernize Voting Equipment. *Associated Press State and Local Wire*, May 3.

Roberts, Alasdair. 2004. *Transborder Service Systems: Pathways for Innovation or Threats to Accountability?* Washington, DC: IBM Endowment for the Business of Government.

Roberts, Karlene H. 1990. Some Characteristics of High Reliability Organizations. *Organization Science* 1(2): 160–77.

Sagan, Scott D. 1993. *The Limits of Safety: Organizations, Accidents and Nuclear Weapons*. Princeton, NJ: Princeton University Press.

Saltman, Ray G. 1988. Accuracy, Integrity, and Security in Computerized Vote-Tallying. NBS Report SP500, National Institute of Standards and Technology. www.nist.gov/itl/lab/specpubs/500-158.htm.

Schneier, Bruce. 1993. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley.

———. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley.

———. 2003. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Copernicus Books.

Schwartz, Kevin. 2004. High-Tech Voting System is Banned in California. *New York Times*, May 1, A9.

Seelye, Katharine Q. 2004. Demand Grows to Require Paper Trails for Electronic Votes. *New York Times*, May 23, A20.

Shelley, Kevin. 2003. Secretary of State's Ad Hoc Touch Screen Task Force Report. California Secretary of State, July 1. http://www.ss.ca.gov/elections/taskforce_report.htm.

Shi, Yuhand, and Carmine Scavo. 2000. Citizen Participation and Direct Democracy through Computer Networking. In *Handbook of Public Information Systems*, edited by G. David Garson, 113–25. New York: Marcel Dekker.

Stacey, Ralph D. 2003. *Complexity and Group Processes: A Radically Social Understanding of Individuals*. New York: Brunner-Routledge.

Stanford, Duane. 2002a. Touch Screen Devices a Hit. *Atlanta Journal-Constitution*, November 6, 1A.

———. 2002b. Georgia Puts Trust in Electronic Voting; Critics Fret about Absence of Paper Trail. *Atlanta Journal-Constitution*, October 31, 1A.

Tagami, Ty, and Duane Stanford. 2002. 2,180 Fulton Cards Located after Tally; 67 Memory Cards Misplaced, but Shouldn't Change Results. *Atlanta Journal-Constitution*, November 8, 1C.

Thomas, John Clayton, and Gregory Streib. 2003a. *E-Democracy, E-Commerce, and E-Research: Examining the Electronic Ties between Citizens and Governments*. Paper presented at the annual conference of the American Society for Public Administration, March 15–18, Washington, DC.

——— . 2003b. The New Face of Government: Citizen-Initiated Contacts in the Era of E-Government. *Journal of Public Administration Research and Theory* 13(1): 83–101.

U.S. General Accounting Office (GAO). 2001. *Elections: Status and Use of Federal Voting Equipment Standards*. GAO-02-52. Washington, DC: U.S. Government Printing Office.

U.S. Office of Management and Budget (OMB). 2001. *The President's Management Agenda*. Washington, DC: U.S. Government Printing Office.

Wertheimer, Michael. 2004. Trusted-Agent Report: Diebold AccuVote TS Voting System. http://www.raba.com/press/TA_Report_AccuVote.pdf.

West, Darrell M. 2004. E-Government and the Transformation of Service Delivery and Citizen Attitudes. *Public Administration Review* 64(1): 15–27.

Witte, Brian. 2003. Study Finds Computer Voting System Vulnerable to Tampering. *Associated Press State and Local Wire*, July 24.

Wysopal, Chris. 2003. Learning Security QA from the Vulnerability Researchers. *login: the USENIX magazine* 28(6): 13–15.