THE
CARTER CENTER

Summary of Proceedings
Automated Voting and Election Observation

The Carter Center

March 17-18, 2005

Please note: This summary may not reflect the view of all participants

Introduction

Automated voting (sometimes referred to as electronic or e-voting) technologies are increasingly used in elections across the world, particularly because they are often seen as symbolic of a country's level of modernization. The possibilities for rapid aggregation and analysis of results, as well as potentially greater accuracy, have all added to the attractiveness of computer-based voting equipment. There is little doubt that the ability to quickly publish results can be of particular advantage in conflict and post-conflict scenarios, where a prolonged period of counting can heighten tensions and reduce confidence in the final results. The potential to remove some traditional elements of unintentional voter error or intentional fraud can also contribute to greater confidence, while at the same time raising new questions.

Automated voting systems, thus pose important challenges for election observers: How can observers assess the workings of electronic systems? What is the relevance of traditional election observers, who may have limited technological expertise? What can and should be observed? To what extent should observers be involved in monitoring automated voting equipment?

In order to explore these and other questions related to the challenges of observing electronic voting, The Carter Center convened a meeting of election authorities, academics, technical experts, and representatives from organizations involved in international election observation on March 17-18, 2005 in Atlanta. (An agenda and list of participants are attached).

This document provides a general summary of the issues discussed at The Carter Center meeting, and aims to capture most of the key points. It is not intended to be a verbatim transcript, nor does it attribute positions to any particular participants.

General Overview

In general, the meeting participants agreed that electronic voting represents only one, albeit a central, aspect of a broader electoral and political process. Inevitably, because of the nature of the technology, electronic equipment places limits on an observer's capacity to detect fraud. On one level, election technology has to be trusted. Still, traditional observers are far from obsolete. The physical presence of observers can deter some aspects of electronic fraud and provide legitimacy to an election outcome if it is deemed free of irregularities. While a high-level of technical expertise is needed to check equipment for sophisticated fraud (e.g. the presence of spyware[1], Easter eggs[2]), there are measures that observers can and should take to minimize the potential for fraud. For example, they can determine whether election officials are scrupulously following procedures designed to detect some types of cheating (e.g. has zero tape been printed out? Does the precinct number appear on ballot?). In addition, observers can identify whether security during the equipment's storage and transportation was adequate. They also can evaluate whether independent certification and testing of software and hardware have taken place. Finally, they can observe post-election counts, or audits, of paper receipts to verify electronic vote recording, if such a paper-trail exists.

The need to observe pre- and post-election testing and certification of election equipment and systems underscores the need for and role of election observers. However, if electronic equipment is to be credibility monitored, it is essential that technically qualified observers have adequate access to key aspects of the electronic equipment. Otherwise, the credibility of the overall observation mission could be compromised, undermining voter confidence and the legitimacy of the results.

Voting technology and security issues

There are four major voting technologies being used in elections across the world: paper-marking, mechanical lever system, optical scans, and direct recording electronic voting equipment (DREs). There are two basic means of transmission of results: networked machines that transmit electronically or through modems, and stand-alone voting machines in which the electronic record (e.g. on chip, disc, etc) is physically transported to the next level of tabulation. Each of these technologies has their own challenges and security problems.

- **Paper-marking**: Voters cast their vote by marking a box or punching out a hole next to a candidate/ party on the ballot. From an observation point of view, this system is ideal as there is physical evidence that reflects a voter's intent. There is no need to trust machines. However, ballot design flaws can lead to the incorrect marking of ballots, while the

[1] A program that can surreptitiously gather information about a user.
[2] Pieces of code introduced into a program that will produce a "hidden treasure" when a user types in a specific combination of commands.

counting, transmission, and tabulation of results can be subject to human error or intentional manipulation.

- **Mechanical lever system**: Voters lower a lever next to the name of a candidate. The programming of the mechanical levers is very simple, making it attractive as a voting technology. Yet that same simplicity also poses problems. Levers can be programmed in such a way that votes cast in favor of one candidate actually go to another. This technology emerged in the 1930s in the U.S. and is no longer produced on a widespread scale. The only record of the vote is within the machine.

- **Optical scan**: A ballot with multiple-choice options is marked and fed through a scanning machine that tallies the votes. The marking of the sheet was traditionally done by pencil, but punch cards and computerized ballot marking are increasingly popular. Voters are given the option to check and then acknowledge or discard their vote. Also, the machine would alert the voter to over- and accidental under-voting. This system probably represents the most secure technology, since a scanner has a small "trusting computing base" (TCB). In other words, it relies on relatively few lines of source code, which makes any malicious source code more difficult to hide.

- **Direct recording electronic voting equipment (DRE):** The ballot page is displayed on a computer screen and selection usually takes place via a touchscreen system. DRE provides for candidate selection and tallying in a single computer. Because it performs a number of functions it has a larger TCB than an optical scanner, increasing the opportunity for hackers to hide disruptive code. This becomes a concern as traditionally separate election stages (e.g. counting and tallying), are conflated into one process on DRE. Of particular concern are Easter eggs, which are secreted into the computer and then erase themselves, leaving little to no trace. Nevertheless, some electronic and physical safeguards can minimize these dangers, such as independent examination of the source code, and setting the machine to the date of the election during pre-testing.

- **Electronic transmission of results:** The security of transmission is a concern because data is vulnerable unless properly encrypted or otherwise insulated from potential hackers; bi-directional communication needs to be protected against. Physical transport or modem transmission (as opposed to transmission via digital media) can reduce vulnerability.

- **Physical transport of electronic record**: The concerns regarding delivery of traditional voting materials such as ballot boxes, ballots and tally sheets still apply. Most electronic voting machines have multiple data storage devices that can be compared against one another to serve as an additional check.

Privacy and transparency in automated voting using DREs

It is important, particularly in highly polarized environments, to be able to distinguish between human error, computer error, and fraud. But, the very nature of DRE technology can be an obstacle to that differentiation. The difficulty for observers lies in the fact that DRE voting machines do not provide a means of independently verifying results unless the voter discloses his/her choice (which would directly contravene the democratic right to secrecy of the ballot).

However, DRE voting systems can be designed to produce a "voter verifiable audit trail" (VVAT), such as a paper receipt, that can then be verified against the electronic results, without requiring that individual voters disclose their votes.   With a VVAT, the accuracy of a DRE voting machine can be verified by simply comparing the paper receipt results with the electronic results for that machine. Likewise, comparing the results from a representative sample of machines can provide a means of assessing the accuracy of the overall results.

These methods, however, raise some potential problems: (a) a voter could tamper with a paper receipt (fail to deposit it, or change it out); (b) if the voter never touches the paper receipt, the system would need to be designed to allow both voter sight verification of the ballot, while protecting privacy (perhaps by scrambling the order of the vote in some way); and (c) if there is a discrepancy between the results of the DRE machines versus the paper receipts, the electoral law would need to be clear on which has the legal validity.

Two technology solutions designed to address the dual needs of privacy and transparency were discussed at the meeting. One suggestion envisaged the use of a number of machines providing checks on each other to ensure that votes are recorded as accurately as possible. Another suggestion combines a computer-based system with an optical scanner. In the latter, a stand-alone machine would allow the voter to mark and print out a ballot that can be read, much like an airplane boarding pass, and then optically-scanned into a separate vote-counting machine. Should the vote-marking machine print out the wrong ballot, a voter would be able to discard the ballot, obtain a new ballot, and re-select a candidate. If correct, a voter can then feed the ballot into a scanner to record their choice. Such a system would have the technological advantages of a DRE, providing for fast vote tabulation and vote confirmation, while benefiting from the security advantages of a low TCB optical scan system.

Public and private interests

A transparent electoral process is essential for ensuring voter's trust in the system and in the democratic process in general. As a result, some experts advocate disclosing a DRE's source code (referred to as "open source"). Currently, private sector vendors regard their codes as private intellectual property and are unwilling to make them available for public scrutiny. However, in some cases, such as the state of Georgia in the U.S., a copy of the source code is provided to an independent verification center located at a university. In the U.S., the national testing laboratory examines the source code of all voting machines.

Even if source code is made available to widespread, independent verification, as the Smartmatic company has offered, the question remains as to who should conduct the verification and what role international observers and political parties should play, or with what level of expert capacity.

Testing methods

There was general agreement at The Carter Center meeting that testing and auditing are key to detecting fraud and hence also for the maintenance of voter trust. Participants discussed several methods that could be employed by officials and observers to test equipment (assuming access was provided), including:

Technical tests

- **Debugging prior to voting:** debugging means running software with the aim of detecting possible errors. Errors can be detected by running the software step-by-step or by stopping a program at specified breakpoints and examining variables. Specific measures may include:
  - During a pre-test, adjusting the machine's internal clock to the day of the election (in order to test for the presence of Easter egg).
  - Running logic and accuracy tests prior to the vote.

- **Parallel testing during voting** (as opposed to parallel vote tabulation (PVT) or quick count, which offers predictions based on a statistically relevant sample of results): This involves selecting a voting machine at random and placing it in a controlled room with a distribution of voters that matches the real distribution as closely as possible. Conditions should be as similar as possible to actual conditions as the machine may be programmed to recognize if these diverge. This type of testing can occur before and after the election. The key is to trick the machine's internal clock into thinking it is election day in order to trigger pre-coded efforts to commit electronic fraud. If the test is conducted on election day, however, the removal of machines during polling may have legal ramifications as the relevant election laws would need to have provisions to allow for testing to take place during elections.

Statistical tests (assuming there is a paper trail)

- **Sampling:** In DRE systems that produce a paper trail, a sample of electronic votes can be compared to paper receipts . This sampling method is more cost-effective and efficient than manually counting all the votes. In general, the fewer votes are counted, the more accurate the manual count (which is susceptible to human error). Therefore, a small sample size with high statistical significance is desirable.

- **"Hot and cold audits":** Not to be confused with recounts, the aim of an audit is not to determine the winner of an election but only to verify the accuracy of the voting system by means of a re-examination of a statistically relevant sample of results. Hot and cold audits follow the sample methodology described above. However, cold audits are carried out a few days after the election, whereas hot audits take place immediately at the close of the election in the location of the voting.

Automated voting and election observation

Four distinct phases of the electoral process are affected by automated voting: ballot marking, vote recording, vote transmission, and tabulation of the voting results. All four stages pose independent challenges to election observers.

As mentioned above, even though the ballot marking and vote recording stages are conflated on DREs, the marking stage differs from the recording phase in that a machine's recording may not necessarily reflect how the voter intended to mark the ballot. In principle, the more aggregated DREs are, i.e., the more election phases are handled by one machine, the more difficult observation becomes. The secrecy/transparency dilemma inherent in DREs means that achieving total security and drawing an unequivocally clear demarcation line between human error, computer error, and outright fraud is only possible through the unacceptable surrender of voter secrecy.

Nonetheless, election observers can focus on specific steps undertaken at several points in the electoral process in order to determine whether authorities have done their utmost to maximize security, and to minimize the potential for fraud before, during, and after election day. These include:

Pre-election:

- Voter education
    - Observers can verify whether voter education encouraged voters to verify their selection before finally casting their ballot.

- Transparency of software and hardware certification process
    - Evaluate whether the certification body is truly independent.
    - Obtain reports prepared by certification body.
    - Consult with technical experts.

- Quality of pre-election tests
    - Check whether procedures were followed.
    - Confirm if debugging and/or some form of parallel testing has taken place.
    - Consult with technical experts.

On election day:

- Before polling:
    - Confirm that zero tape has been printed before voting starts.
    - Confirm that voting machines display the correct precinct numbers.

- During polling:
    - In cases where results will be transmitted to central headquarters electronically, confirm that voting machines are not networked with an outside computer (e.g., in a tabulation center) while voting takes place. Networking opens the possibility of interference via modems and should only take place *after* the electronic results

have been printed out by the voting machine, so that aggregated results may be compared against it.

  - Check position of voting units: are units positioned so as to guarantee voter secrecy? Are they away from direct sunlight, so that the writing on the screen is clearly legible?
  - Observe that procedures are being followed:
    - to prevent electronic stuffing.
    - to allow voter verification (where possible).
    - to allow parallel testing (where allowed).

- During counting and tabulation:
  - Check number of voters against voter list and electronic tally.
  - Review precinct results in order to perform statistical verification of results.
  - Observe delivery of the voting materials (electronic media and paper records).
  - Where there is a paper trail, carry out sampling and "hot audits."

Post-election:

- Assess the quality of post-election tests:
  - Check whether procedures were followed.
  - Consult with technical experts.

Conclusions and next steps

Clearly, automated voting poses new challenges for election observers. In order to meet these challenges, observers need to adopt a two-pronged approach: First, they will have to rely on a core team of IT experts, ideally working as long-term observers to assess the technical aspects of electronic voting equipment. Second, observers still need to focus on the other procedural and political aspects of the conduct of an election. As the emphasis of election observation becomes more equitably distributed between the pre- and post-election period on the one hand, and on election day itself on the other, the diverse roles and value of long-term observers will increase.

Participants at The Carter Center conference also discussed the nature of the relationship between election observers and the host country. For elections that rely heavily on electronic voting equipment, election observers will need to have access to certification reports and the testing process of DREs. In such cases, observers may be at risk of being seen as meddling in a country's sovereign affairs. Thus, a carefully balanced approach that takes into consideration the political situation, yet meets the need for thoroughness will be required.

A set of basic guidelines were suggested for possible inclusion in election observation standards and a code of conduct for observers:

- Observers do not certify voting systems.
- Observers can evaluate whether independent certifications of software and hardware takes place (and the quality of the certifications).
- Observers should focus on procedures.

- Observers need technically skilled long-term observers to observe pre- and post-election tests.

Whereas the Carter Center conference offered the opportunity to consider many of the issues surrounding automated voting and election observation, many other questions remained unanswered and could form the basis for future meetings. The growing use of automated voting systems adds new dimensions to election observation, and raises important questions such as what are the minimum criteria for election observation of automated voting systems and what can be done to promote greater understanding among observers, election officials, vendors, academic experts and legislators?

THE
CARTER CENTER

"Automated Voting: Challenges and Lessons for Election Observation"

Atlanta
March 17 – 18, 2005

Participant List

Maria Helena Alves
Collaborator on Elections and Technology
ACE Project

Henry Brady
Professor of Political Science and Public Policy,
UC Berkeley

David Carroll
Interim Director, Democracy Program
The Carter Center

Paul DeGregorio
Vice Chairman,
Election Assistance Commission

David Dill
Professor of Computer Science,
Stanford University

Rachel Fowler
Senior Program Associate, Democracy Program
The Carter Center

John Hardman
Executive Director
The Carter Center

Torquato Jardim
Former Member of the Tribunal
Electoral Tribunal of Brazil

Keith Jennings
Senior Representative, Electoral Processes
National Democratic Institute of International Affairs

Merle King
Executive Director, Center for Election Systems,
Kennesaw State University

Jennifer McCoy
Director, Americas Program
The Carter Center

Gerald Mitchell
Head of Election Section,
OSCE/ODIHR

Katelina Montana
Specialist of the Department of Democratic and Political Affairs.
Organization of American States

David Pottie
Senior Program Associate, Democracy Program
The Carter Center

Vladimir Pran
Elections Officer, West Bank and Gaza
National Democratic Institute for International Affairs

Aviel Rubin
Professor of Computer Science,
Johns Hopkins University

Herman Ruddijs
Business Project Manager
Sdu Uitgevers

Eric Rudenshiold
Director for the Europe and Eurasia Division
IFES

Ted Selker
Associate Professor,
MIT Media and Arts Technology Lab.

Carlos Mario da Silva Velloso
President
Electoral Tribunal of Brazil

Nikolai Vulchanov
Deputy Head of Election Section
OSCE/ODIHR

Observers

Paulo Bhering Camarão
Computer Science Secretary
Electoral Tribunal of Brazil

Avery Davis-Roberts
Assistant Program Coordinator, Democracy Program
The Carter Center

Steve Hochman
Director of Research
The Carter Center

Shelley McConnell
Associate Director, Americas Program
The Carter Center

Phil Wise
Assistant Executive Director, Operations
The Carter Center Center

Rapporteurs

Daniel Kosinski
Intern, Democracy Program
The Carter Center

Jennifer Martin-Kohlmorgen
Intern, Democracy Program
The Carter Center