NATIONAL DEMOCRATIC INSTITUTE
FOR INTERNATIONAL AFFAIRS

MONITORING ELECTRONIC TECHNOLOGIES IN ELECTORAL PROCESSES

An NDI Guide for Political Parties and Civic Organizations

Vladimir Pran and Patrick Merloe

MONITORING ELECTRONIC TECHNOLOGIES IN ELECTORAL PROCESSES

AN NDI GUIDE FOR POLITICAL PARTIES AND CIVIC ORGANIZATIONS

Vladimir Pran and Patrick Merloe

NATIONAL DEMOCRATIC INSTITUTE FOR INTERNATIONAL AFFAIRS (NDI)

Library of Congress Cataloging-in-Publication Data

Pran, Vladimir, 1972-
Monitoring electronic technologies in electoral processes: an NDI guide for political parties and civic organizations / Vladimir Pran and Patrick Merloe.
p. cm.
ISBN 978-1-880134-36-8 (pbk.)
1. Election monitoring--Handbooks, manuals, etc. 2. Electronic voting--Handbooks, manuals, etc. 3. Voter registration--Handbooks, manuals, etc. 4. Freedom of information--Handbooks, manuals, etc. I. Merloe, Patrick. II. National Democratic Institute for International Affairs. III. Title.
JF1032.P73 2007
324.6'5--dc22 2007041501

ABOUT NDI

The National Democratic Institute for International Affairs (NDI) is a nonprofit organization working to strengthen and expand democracy worldwide. Calling on a global network of volunteer experts, NDI provides practical assistance to civic and political leaders advancing democratic values, practices and institutions. NDI works with democrats in every region of the world to build political and civic organizations, safeguard elections, and promote citizen participation, openness and accountability in government.

Democracy depends on legislatures that represent citizens and oversee the executive, independent judiciaries that safeguard the rule of law, political parties that are open and accountable, and elections in which voters freely choose their representatives in government. Acting as a catalyst for democratic development, NDI bolsters the institutions and processes that allow democracy to flourish.

Build Political and Civic Organizations: NDI helps build the stable, broad-based and well-organized institutions that form the foundation of a strong civic culture. Democracy depends on these mediating institutions-the voice of an informed citizenry, which link citizens to their government and to one another by providing avenues for participation in public policy.

Safeguard Elections: NDI promotes open and democratic elections. Political parties and governments have asked NDI to study electoral codes and to recommend improvements. The Institute also provides technical assistance for political parties and civic groups to conduct voter education campaigns and to organize election monitoring programs. NDI plays a leading role in international election observation and was an initiator and co-drafter of the Declaration of Principles for International Election Observation. The Institute has organized international delegations to monitor elections in dozens of countries, helping to ensure that polling results reflect the will of the people.

Promote Openness and Accountability: NDI responds to requests from leaders of government, parliament, political parties and civic groups seeking advice on matters from legislative procedures to constituent service to the balance of civil-military relations in a democracy. NDI works to build legislatures and local governments that are professional, accountable, open and responsive to their citizens.

International cooperation is key to promoting democracy effectively and efficiently. It also conveys a deeper message to new and emerging democracies that while autocracies are inherently isolated and fearful of the outside world, democracies can count on international allies and an active support system. Headquartered in Washington D.C., with field offices in every region of the world, NDI complements the skills of its staff by enlisting volunteer experts from around the world, many of whom are veterans of democratic struggles in their own countries and share valuable perspectives on democratic development.

NATIONAL DEMOCRATIC INSTITUTE FOR INTERNATIONAL AFFAIRS
2030 M Street, N.W., Fifth Floor
Washington, D.C. 20036
Tel +1 202 728 5500
Fax +1 202 728 5520
Website http://www.ndi.org

ACKNOWLEDGEMENTS

This Guide was prepared by the National Democratic Institute (NDI) to assist political parties, civic organizations, journalists, election officials and others concerned with ensuring the integrity of elections and building confidence in electoral processes. The Guide reflects NDI's 20 years of experience in international election observation and in supporting the efforts of political parties and domestic nonpartisan election monitoring groups in more than 90 countries to promote electoral integrity and popular political participation.

The Institute supports the efforts of government and election officials who open electoral processes and build public confidence based on transparency, and NDI supports the efforts of political and civic activists, as well as journalists, to gain access to and to report on all elements of election processes, including those that employ electronic technologies. These efforts protect each citizen's right to democratic elections. The Institute appreciates the important work of international organizations to observe and to provide electoral assistance so that elections around the world may meet international standards. Many such organizations have taken increasing interest in helping ensure transparency for electronic technologies, which are being used more widely in elections. It has been NDI's privilege to work with many individuals in each of these sectors. We have learned from them and are inspired by their untiring efforts.

Vladimir Pran, former NDI Senior Program Manager in elections and political processes, and Patrick Merloe, NDI Senior Associate and Director of Electoral Programs, were the authors of this Guide. Vladimir concentrated on issues related to the selection of various electronic technologies, their applications and challenges presented for verification. Pat focused on the basis for seeking access (transparency) and various monitoring approaches. During his seven years with NDI, Vladimir worked with NDI partner organizations to verify vote tabulations, audit voter registries and conduct other efforts to promote electoral integrity in more than 15 countries. He was formerly a leading member of the Croatian civic organization GONG and in July 2007 became the Chief of Party for IFES's programs in the Palestinian Authority. Pat has observed election processes in numerous countries around the world during his almost

15 years with NDI, and has produced over a dozen publications on democratic elections, human rights and comparative law.

NDI benefited greatly from comments and suggestions concerning drafts of the Guide that were provided, in their personal capacities, by noted experts in the field of electronic technologies: Jarrett Blanc, Open Society Institute, USA; Robert Krimmer, Competence Center for Electronic Voting and Participation, Austria; Henri Snyers, Coordinator for Electronic Voting, Government of Belgium; and Melanie Volkamer, University of Passau, Germany. NDI also benefited greatly from comments and suggestions on the Guide that were provided, in their personal capacities, by election monitoring experts: David Carroll, of The Carter Center; Sean Dunne of the United Nations Office for Project Services, formerly with the UN Electoral Assistance Division; Armando Martinez-Valdes of the UN Electoral Assistance Division; and Gerald Mitchell of the Organization for Security and Cooperation in Europe Office for Democratic Institutions and Human Rights. Former NDI Deputy Director for Asia Lawrence Lachmansingh, NDI Senior Advisor for Electoral Programs Richard L. Klein and NDI Programs Manager for Information and Communication Technologies (ICT) Ian Schuler also provided valuable comments on the Guide.

Under the guidance of Pat Merloe, Joseph Scrofano, NDI Legal Projects Assistant in elections and political processes, prepared the appendices for the Guide. His contribution through legal research and analysis of relevant jurisprudence was a substantial contribution to the Guide.

Pat Merloe and Linda Patterson, NDI Program Officer in elections and political processes, were the editors of the Guide. Linda has worked on all elements of NDI election programs, with emphasis on international election observation and assisting domestic nonpartisan election monitoring efforts. NDI Program Officer Julia Brothers supported the authors and managed publication efforts for the Guide. Program Assistant Laura Grace and Intern Sam Bromell also assisted in the publication.

We hope that the Guide will be useful in addressing new challenges and opportunities posed by the use of electronic technologies in elections. These include access to decisions on whether to employ

electronic technologies, considerations as to which types of technologies to use, evaluations of what specific technologies will be purchased, and verifications of the integrity of the technologies before, during and after the respective processes are completed. NDI, of course, takes full responsibility for any weaknesses that appear in the Guide.

The writing, editing, production and publication of this Guide were made possible by a grant from the National Endowment for Democracy (NED). We hope that those who use this Guide will contact NDI with any comments, suggestions and requests.

Kenneth Wollack
President, NDI

TABLE OF CONTENTS

CHAPTER ONE:

The Legal and Policy Basis for Monitoring Electronic Technologies

INTRODUCTION TO MONITORING ELECTRONIC TECHNOLOGIES

Citizens have a right to genuine elections, manifested in the right to vote and to be elected, and citizens have a right to seek and impart information that informs the public concerning whether elections are genuine, somehow tainted or fraudulent. These precepts are as fundamental as a government's obligation to organize genuine elections. They are critical to any discussion concerning the proper application of electronic technologies in the electoral context.

Electronic technologies are increasingly important to election processes around the world. Without doubt they will be used ever more broadly in future elections and the integrity of elections will increasingly depend on their proper functioning. There are definite benefits accompanying the appropriate application of electronic technologies in the electoral context. The benefits include more rapid performance and the potential elimination of possibilities for certain types of errors and fraud. At the same time, every technology, including electronic technology, brings with it challenges and risks that must be addressed.

Electronic technologies pose particular challenges and risks, because they often limit "transparency" in elections, which makes it more difficult for the public to know whether elections are genuine, somehow tainted or fraudulent. Electronic technologies therefore must be monitored by election authorities, by the electoral

contestants (political parties and candidates) and by citizens through nonpartisan election monitoring organizations. The news media should also play important roles in reporting on electoral integrity.

Monitoring the functioning of electronic technologies and broader factors that determine electoral integrity is important in every country. Party and candidate efforts to monitor all elements of election processes enhance electoral integrity and allow the electoral contestants to more easily understand whether the official results actually reflect the will of the electorate. Monitoring by nonpartisan citizen organizations also plays a critical role in establishing the appropriate level of public confidence in elections.

The impact of electronic technologies is transforming electoral processes and with it, election observation. Transparency is evermore critical and observers from all sectors will need to concentrate their attention on gaining access to decision-making early in the election process, as well as examining the technologies themselves.

Monitoring the applications of electronic technologies in the varied elements of an election process is central to establishing public confidence - both among those seeking elected office and among the electorate. Monitoring elections - including the role of electronic technologies - is not simply expedient, nor is it a matter that can be arbitrarily permitted or denied by those wielding governmental powers. Monitoring elections is a matter of exercising fundamental rights that form part of the core of sovereignty, which ultimately belongs to and derives from the people of a country. Among those core political rights, recognized in international instruments[1] and most modern national constitutions, are:

- The authority of government derives from the will of the people expressed through genuine, periodic elections;

[1] Please see, for example, the *Universal Declaration of Human Rights*, which is applicable to all United Nations Member States, Articles 2, 6, 7, 8, 19, 20 and 21*; International Covenant on Civil and Political Rights*, which creates immediate and direct obligations for all 160 countries that have entered into this treaty, Articles 2, 3, 16, 19, 22, 25 and 26. See Appendices 3 and 4 of this Guide for the relevant texts of numerous international human rights instruments and brief analyses of relevant decisions of international human rights tribunals.

- Citizens have the right and must be provided the opportunity, without unreasonable restrictions, to participate in government and public affairs, directly or through freely chosen representatives;

- Citizens have a right to vote and to be elected;

- Elections must provide universal and equal suffrage, through a secret ballot, guaranteeing the expression of the free will of the electors;

- There is a right to associate to pursue the exercise of these rights and other legitimate activities;

- There is a right to seek, impart and receive information in pursuit of the freedom of expression, which is applicable to information relating to whether elections are genuine; and

- Everyone, including prospective voters and electoral competitors, is to be equal before the law, is entitled without discrimination - based on political opinion or other suspect factors - to equal protection of the law and has a right to effective remedies if their political and civil rights are abridged.

All of these rights come into play when the role of electronic technologies in elections is evaluated.

Governments have an overriding obligation to their citizens to provide genuine democratic elections, which carries special responsibilities in designing electoral organization. This applies to the legal framework for elections, the structure of election administration, the mechanisms for conducting elections, the fairness of electoral competition, as well as reporting accurately and honestly about citizens' choices expressed at "the ballot box."

Political parties, candidates, and supporters and opponents of propositions offered in referendums have an obligation to conduct their activities within the rules of electoral competition — and to safeguard electoral integrity. This includes acting in self-interest to

protect votes gained through campaigning. It also means recognizing an obligation to honor the electorate and its will, rather than seeking to impose a party's, individual's or small groups' will over that of the citizens who voted.

Citizens themselves have a right and a responsibility to ensure electoral integrity. This pertains to each citizen's right to choose representatives who will serve and represent them in government. Joining in the efforts or otherwise supporting civic organizations and news media that monitor and report on election processes is a fundamental element of exercising each citizen's right to participate in government and public affairs.

Electronic technologies pose a critical challenge to election monitoring because their operation is not observable by the "naked eye," and, thus, it is particularly difficult to establish whether the technologies are functioning properly or whether there are malfunctions and even fraudulent outcomes that subvert electoral integrity. This concern must be addressed by: policy makers, who draft, debate and enact laws and regulations; election and other governmental officials, who administer processes that are central to elections; political parties and candidates, who seek to exercise their right to be elected to represent the people; and the citizens, who seek to exercise their sovereign right to choose representatives - who will then have legitimate authority to exercise the powers of elected office.

Monitoring the application of electronic technologies therefore is a key element of guaranteeing genuine democratic elections. Such monitoring can reinforce confidence in electoral authorities and increase participation in election processes. It can also identify problematic areas and lead to corrective action by election administrators, or it can provide a basis to challenge processes and to seek redress before the courts or other forums.

This Guide is designed primarily for political contestants and citizen organizations, though it is also meant to be useful to electoral authorities, legislators and others concerned with honoring the will of the people concerning who should have the authority and legitimacy to exercise the powers of government. The following sections of this Chapter examine the legal bases for seeking

transparency - access to vital information about the functioning of electronic technologies employed in election processes. This provides the foundation for seeking information needed to monitor the application of electronic technologies.

THE LEGAL AND POLICY BASIS FOR MONITORING ELECTRONIC TECHNOLOGIES

Sovereignty and the Right to Genuine Democratic Elections:

In any democratic system of government, it is recognized that sovereignty belongs to and derives from the people of the country. Citizens have the right to participate in government and public affairs to shape governance and demand its responsiveness to their expressed interests. The legitimacy and authority of government therefore derives from the people's will concerning who shall occupy and exercise the powers of electoral office. The right to vote and the right to be elected extend from and are inexorably linked to these fundamental democratic principles.

Most modern constitutions enshrine these precepts in some form, and they are expressed in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and all other human rights instruments that address political rights.

> "Everyone has the right to take part in the government of his [or her] country, directly or through freely chosen representatives...The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures." (Article 21, *Universal Declaration of Human Rights*)

> "Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2,[2] and without unreasonable restrictions: (a) To take part in the conduct of public affairs, directly or through freely chosen representatives; (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal

[2] "[R]ace, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status..." Article 2, *International Covenant on Civil and Political Rights*.

> suffrage and shall be by secret ballot, guaranteeing the free expression of the will of the electors..." (Article 25, *International Covenant on Civil and Political Rights*)

The popular interests in genuine democratic elections therefore are in essence sovereign rights, and guaranteeing and protecting those interests should take a dominant position when they are weighed against other interests presented in election processes, such as privacy interests and proprietary interests in commodities employed by election administrators. Such other interests may be accommodated appropriately, but the popular interests in realizing genuine democratic elections are fundamental and should take a primary position in any interest weighing calculus.

The right to participate in government and public affairs provides a direct basis for the long-accepted state practice of allowing political parties and candidates to have their agents (sometimes referred to by terms such as poll watchers, scrutineers or proxies) present in polling stations and at other critical points in various elements of election processes. The right also belongs to citizen associations dedicated to electoral integrity, often referred to as nonpartisan domestic election monitors or observers. While party and candidate agents seek to protect the right to be elected, domestic election monitors seek to protect the rights to vote and to be elected — together they (and news media acting in accordance with standards for professional integrity) promote and defend the popular right to genuine elections that governmental authorities are obliged to respect.

These points form critical parts of the foundation of monitoring the integrity of electronic technologies used in election processes.

The Right to Associate into Political Parties and Nonpartisan Election Monitoring Organizations to Promote and Defend Electoral Integrity:

The rights to genuine democratic elections discussed above, as well as related rights enumerated below, are both individual rights of citizens and associational rights. To pursue these rights, people must have the freedom to associate and form organizations.[3]

[3] See, for example, Article 20, *Universal Declaration of Human Rights* and Article 22, *International Covenant on Civil and Political Rights* concerning the right to freedom of association.

This may take the form of political parties or individual candidate groups seeking to exercise the right to be elected. Organizations also are formed to seek to pass or defeat propositions put before the electorate in referendums. Such political organizations allow people to aggregate their interests through participation in government and public affairs. In addition, citizens associate to promote and defend their right to vote and overall electoral integrity (the right to genuine elections). This usually takes the form of election monitoring (or observing) organizations or coalitions. In essence, citizen groups that promote and defend electoral integrity are "human rights defenders" and merit the attention that such defenders receive from the international community.[4]

Freedom of Expression and the Right to Seek, Receive and Impart Information Concerning Electoral Integrity — Including Electronic Technologies:

Political contestants (parties and candidates seeking elected office) cannot know whether their right to be elected is honored or abridged unless they know that the sensitive elements of electoral processes are conducted properly. Citizens cannot know whether their right to participate indirectly in government and public affairs through selection of representatives is honored or violated unless they know this as well. Citizens, of course, cannot examine such things individually.

The public depends on governmental authorities, including election officials, to ensure that election processes are honest and accurate. Some citizens rely on the political contestants to safeguard electoral integrity. Many citizens also seek information from what they perceive as independent, impartial, reliable sources. Citizens therefore often rely on nonpartisan civil society organizations that monitor elections, as well as on credible news media, which also have the right to seek information about the functioning of election processes and to report to the public.

[4] This is important in the United Nations regime for protection of human rights defenders and is relevant to instruments like the Organization for Security and Cooperation in Europe's 1990 Copenhagen Document provisions concerning human rights (paragraphs 10 and 11).

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." (Article 19*, Universal Declaration of Human Rights*)
>
> "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his [or her] choice." (Article 19*, International Covenant on Civil and Political Rights*)

The right of citizens to seek, receive and impart information concerning whether election processes are in fact honest and accurate (i.e., genuine), combined with the right to participate in public affairs (such as monitoring and evaluating the character of election processes - whether as electoral contestants, nonpartisan election monitors or news media), form the basis for the requirement of "transparency" in election processes.

Electoral transparency is widely accepted in state practice as a principle for democratic elections. It is not difficult to understand why "transparency" — the ability of electoral contestants, monitoring organizations and the media to see into and understand all elements of the electoral process — is a principle for democratic elections. The right of citizens to have access to government held information that is central to knowing whether elections are genuine is self-evident, recognizing that: sovereignty belongs to the people; their will provides the basis of authority of government; and their will freely expressed through genuine elections determines who shall legitimately occupy elected office and wield governmental powers as representatives.[5]

The rights of electoral contestants, monitoring groups and the media to seek, receive and impart information concerning electoral integrity applies directly to the use of electronic technologies in election processes. As the later chapters in the Guide discuss, the right to information concerns the criteria and process upon which decisions

[5] Please see the appendices to this Guide for the relevant texts of various international human rights instruments concerning the right to seek, receive and impart information and a review of decisions of international tribunals on the subject.

are made to employ electronic technologies in each element of election processes (e.g., creation of voter registries, electronic voting, results tabulation and transmission), the selection of suppliers of electronic technologies, the testing of the technologies and evaluating the performance of the technologies.

At each step, the interests of the public in access to information concerning electronic electoral technologies - exercised through political contestants, nonpartisan monitoring groups and news media - must be recognized as a fundamental right, in parallel to the individual rights of citizens. The opportunity to exercise that right must be provided without unreasonable restrictions. In practice, this means that, although other legitimate interests may be considered and appropriately accommodated, the right must be honored, guaranteeing access to information that allows the public to know whether the use of electronic technologies may ensure or undermine electoral integrity.

Equality before the Law and Equal Protection of the Law, Universal and Equal Suffrage, and Effective Remedies when Evaluating Electronic Electoral Technologies:

As noted above, "everyone/every citizen" has a right to take part in government and public affairs, among other ways, through genuine elections, and universal and equal suffrage is to be applied to the rights to vote and to be elected. Everyone, without discrimination and without unreasonable restrictions, also must be permitted to exercise the right to seek, receive and impart information and other political rights necessary to realize genuine democratic elections. These principles relate to a non-discrimination norm that derives from the fundamental precepts that everyone is entitled to equality before the law.

> "All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." (Article 26*, International Covenant on Civil and Political Rights*)[6]

[6] See also, for example, Articles 2 and 7, *Universal Declaration of Human Rights*.

Going beyond these precepts, international human rights instruments state that if fundamental rights are abridged, everyone has a right to an effective remedy.

> "Each State Party to the present Covenant undertakes: (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; (b) To ensure that any person claiming such a remedy shall have his [or her] right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy; (c) To ensure that the competent authorities shall enforce such remedies when granted." (Article 2, Paragraph 3*, International Covenant on Civil and Political Rights*)[7]

To be *effective*, any remedy must be able to address the harm created by the violation of rights and cure that harm. In the electoral context, remedies typically must be rapidly available - or the harm will quickly become irreparable. Prevention of harm is critical which merits an even stronger priority for providing access to all elements of an electoral process at early stages, such as criteria and processes for deciding on whether to employ electronic technologies, on where to acquire them, testing and other phases.

Effective remedies cannot be available where it is not possible in a timely manner to determine whether a technology actually performed properly. For example, if electronic voting is conducted and no auditable basis exists for a recount of votes, the only remedy available may be to hold a new election. Otherwise, the person who would take office, while time-consuming forensic investigations are conducted, would lack a legitimate mandate and could be the wrong person. In addition, re-elections are time and resource intensive, and holding a vote at a different point in time may produce a different electoral outcome. Thus, the remedy may not be truly "effective" for protecting the right to be elected or the right to vote. Examples can

[7] See also, for example, Article 8, *Universal Declaration of Human Rights.*

also be illustrated concerning application of electronic technologies in the creation of voter registries and other election processes, which are described in the following chapters of this Guide.

At every point where electronic technologies are to be employed in election processes the following question must be asked by policy makers, election administrators, political contestants, nonpartisan election monitors, the media and the public:

> Will it be possible to provide sufficient transparency into the application of this technology to allow problems to be identified and allow effective remedies to be provided?

If the answer is no, or if the answer is uncertain, there may be an unacceptable risk that the principles of equality before the law and equal protection of the law will be denied. In those cases, protection of the fundamental right to genuine elections should take priority, and the technology should not be employed.

CHAPTER TWO:

Introduction to Electronic Technologies in Elections

INTRODUCTION

Every electronic device used in elections operates and interacts with a variety of inputs in a set of circumstances that provides a context or "*environment*." In order to understand the interaction between election officials, voters, political contestants and electoral technology, observers must examine and analyze the environment in which the equipment is being used.

As noted above, any technology is one part of a broader electoral environment, where human interactions largely determine environmental quality. Knowledge of the electoral choices, the presence or absence of intimidation, the competence and integrity of electoral officials at all levels are among the environmental factors that have direct and substantive impact on the performance of electronic technologies in elections. Monitoring electronic technologies therefore cannot be isolated from the broader electoral and political context. However, just as proper application and performance of electronic technologies can take place in an otherwise fraudulent election, an otherwise proper election can be derailed by fraudulently manipulated or faulty electronic technologies.

A technological environment can be classified as either *controlled* or *uncontrolled*. For an electoral environment to be considered controlled, it is generally accepted that it must meet all of the following criteria:

- Representatives of political contestants, nonpartisan domestic election monitoring organizations and other appropriately authorized persons are physically present, and are able to access and observe the environment.

- Election officials are present, in charge of the process and have legal responsibilities and powers to ensure the accuracy and integrity of the electoral process.

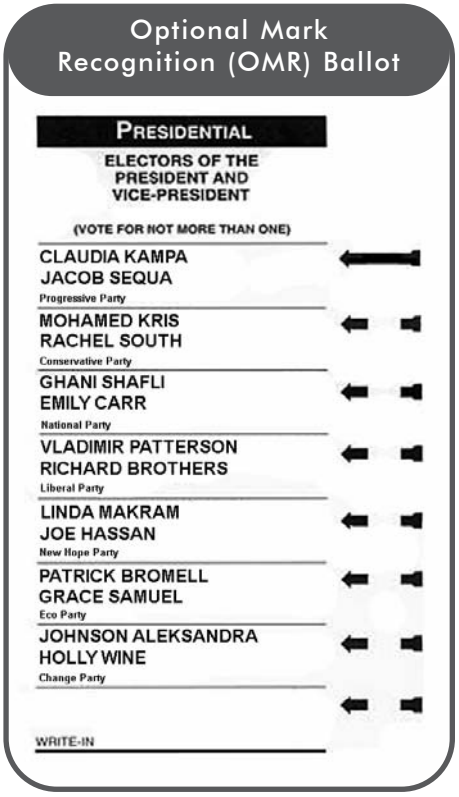
- Access (whether physical or virtual) to the environment, including the technological devices, is secured and controlled, and is regulated by a process that is independently auditable and verifiable.

An example of a *controlled* environment is a polling station where secured electronic voting devices are used, and the polling station staff are liable for the proper functioning of the devices. Party and/or candidate agents, as well as nonpartisan election observers, are present, understand and monitor whether the electoral procedures are properly followed. The electronic devices must not be in a network, and they must be restricted so that they do not interact with other computers (and are thus "isolated"). Interaction restrictions must be safeguarded with the use of hardware and software with security features, and the administration of devices must fall under established security protocols.

Environments can be classified as *uncontrolled* if any of the following exist: representatives of political contestants, nonpartisan domestic election monitoring organizations and other appropriately authorized persons are not physically present, and are not able to access and observe the environment; election officials are not present, not in charge of the process or do not have legal responsibilities and powers to ensure the accuracy and integrity of the electoral process; and access (whether physical or virtual) to the environment, including the technological devices, is not secured and controlled, and is not regulated by a process that is independently auditable and verifiable. Examples of uncontrolled environments are on-line voter registration or voting through the Internet. In both cases, the environment is uncontrolled because election officials are not present to authenticate the identity of the voter and supervise use of devices, and the data transmission is occurring over an open network.

OPTICAL MARK AND OPTICAL CHARACTER RECOGNITION

The basic principle behind Optical Mark Recognition (OMR) and Optical Character Recognition (OCR) technology is for the equipment to turn marked data or hand written data into electronic records. OMR and OCR devices are commonly used for processing voter registration forms and counting votes.



OMR devices are machines that capture data by scanning and recognizing a set of predetermined marks on a sheet of paper. In the electoral context, voters are asked to indicate their choice by placing a specific mark on the ballot paper. The ballot papers are then fed through the OMR device, and the machine is able to quickly recognize the marks and tabulate the results. For example, voters are asked to connect the arrow in front of the candidate of their choice by filling in a space.

OCR devices function similarly to OMR machines, but they record data by scanning and recognizing written letters rather than predetermined marks. This technology is sometimes employed in voter registration processes. It can also be used to read "write in" names on ballot papers.

OMR devices are generally considered to yield more accurate results than OCR devices because they are designed to identify specific marks in a set of predetermined places, whereas OCR devices must recognize hand writing, which differs from individual to individual. This requires the device to interpret the written responses of voters and can lead to higher error rates. On the other hand, the OCR system is designed to read more complex information and thus can be used by election administration officials for a multiplicity of purposes, including recording names and other information on voter registration forms.

When OCR devices are used in voter registration, the record should then be verified for error correction by comparing the information

with the written record. This is often accomplished during the claims and objections period, when citizens can review entries on a preliminary voter registry and request that errors be corrected. If OCR technology is used to read write-in names on ballot papers, the verification should be done immediately by election officials in the presence of political party/candidate agents and nonpartisan election observers to meet the requirements for a controlled environment and ensure electoral integrity.

Scanned ballots from OMR devices should be reviewed by election officials in the presence of party/candidate agents and nonpartisan observers to ensure votes recorded on rejected ballots or votes not recorded though marked are properly included into the overall count, and the counting results recorded on the devices should be verified by a reliable method to ensure that they correspond to the ballots cast. For example, a statistical sample of devices could be selected and verified against the ballot, while all rejected or non-counted ballot choices could be reviewed on the spot. Such methods are discussed below in Chapter 4.

PUNCH CARD SYSTEM

A punch card system requires that voters punch a hole in the ballot paper to indicate their choice. The ballot is then fed into a counting device, similar to an OMR device, that reads which hole has been marked and translates that information into an electronic record. This data is stored in the memory of the device.

An issue that emerges with this technology is whether the ballot is properly designed so that the voter actually punched the hole that corresponds to the candidate or party of his or her choice. Another critical issue that emerges with this technology is whether the platform on which the punch card ballot is placed allows the voter to punch the hole completely through the card, thus ensuring that the voter's choice is accurately read by the counting device.

The punch card ballots should be inspected in the view of political party/candidate agents and impartial observers to determine whether a ballot choice was improperly omitted by the device because the card was not sufficiently punched. This may be decisive in close elections. In addition, the software used for counting should be

subjected to verification by reliable means and compared to the choices indicated on the punch cards, just as paper ballots should be compared to scanned results recorded on OMR devices. A post-election statistical sample of machines and punch cards should be reviewed to determine error rates, thus examining the effectiveness of the technology, even if there are no electoral challenges.

DIRECT RECORDING ELECTRONIC (DRE) SYSTEM

Direct Recording Electronic (DRE) systems are a type of technology that requires the voter to use a keyboard, touch-screen machine, mouse, pen or other electronic device to indicate their choice. Using such systems, a voter produces an electronic record of their vote rather than marking a paper ballot. The DRE device can be built to produce a paper record of each vote, including a paper record that can be reviewed by the voter before registering her or his vote. The paper record is then stored in the machine for verification purposes. An emerging consensus is developing to employ this approach when using DRE technology because it allows for recounts and other vote verification techniques that meet transparency requirements and enhance public confidence. As with OMR and punch card technologies, DRE machines should be subjected to post-voting verifications.[8]

Direct Recording Electronic (DRE) system
Source: Agencia Brasil/José Cruz

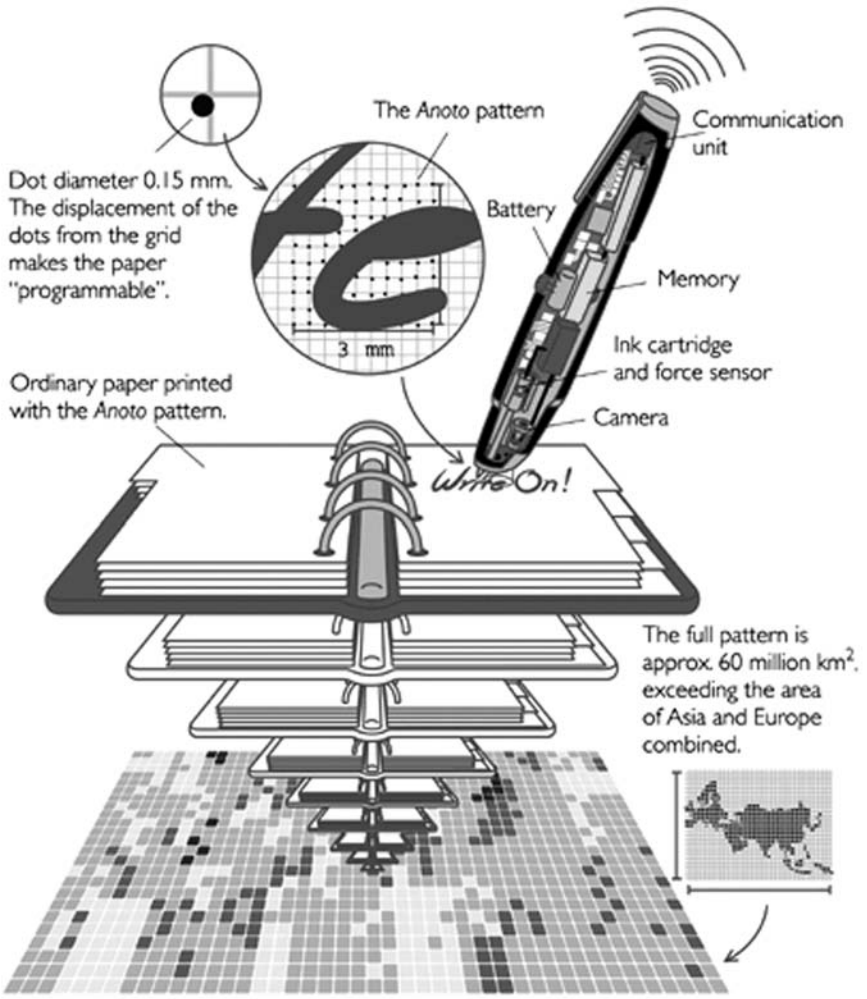
DIGITAL PEN

The digital pen is a DRE device that creates an electronic record while simultaneously marking specialized paper. The device recognizes and records the movement of the pen's point and at the same time leaves an ink trail on the paper. The paper contains microscopic dot patterns that allow the digital pen to recognize the position of the mark on the digital paper. Data stored in the pen can then be uploaded to a computer and software transforms the data into text.

[8] Please see Chapter 4 for further discussion of these subjects.

Digital Pen

Source: Anoto Functionality © Anoto Group AB



PAPER RECORD

A paper record (sometimes called Paper Trail, Audit Trail or Voter Verifiable Paper Audit Trail — VVPAT) is a printed record of a voter's action of touching the keyboard or screen - whether this record concerns the person's vote or his or her voter registration record. It is important to note that unlike OMR and OCR devices, a paper record is produced after the voter has entered her or his information into the DRE device. With DRE technology, the creation of the electronic record precedes the paper record.

There are different interpretations about the relationship between the electronic record of a vote and the paper record, when using DRE

technology. The legal status of the paper record is of fundamental importance to determining the overall integrity of the electoral process.

Equipping a DRE voting device with a paper audit trail capability is widely viewed as a basic requirement for ensuring transparency in the voting process. This, however, is not an infallible safeguard for electoral integrity, and precautions are required to ensure that the paper record is not manipulated. Nonetheless, if there is no reliable verification method, election results could be inaccurate - based on innocent error or fraud - and there would be no effective means to settle contested issues.[9]

If the DRE voting device does not produce a paper record, this is usually called "Black Box Voting."[10] It is generally agreed that such voting techniques do not provide a sufficient means for voters and political contestants to know whether the technology accurately represented the will of those who voted. In addition, should there be a reason to contest the outcome of an election where Black Box Voting is used, there is no reliable means to determine whether the voter's will was respected. This means that organizing new elections would likely be the only effective remedy, which is highly burdensome, expensive and unlikely to recreate the result that voters chose on the designated election day.

ENTRY AND TRANSFER OF DATA

At any stage in the electoral process where data is collected and stored electronically at the polling station level, data will need to be transmitted to higher levels either by electronic or physical means. Electronic methods to transmit data recorded during an election or voter registration process include telephone lines, radio waves or computer networks. Physical transmission involves the transportation of actual data in storage modules (e.g., memory cards, optical media or magnetic media) to the tabulation centers.

---

[9] Please see Chapter 4 for further discussion of these issues, including monitoring techniques.

[10] In Belgium, voters are given a data memory card at polling stations where e-voting is conducted. The voter places the card in a machine inside the polling booth. The machine registers the voter's choices on the data card - not on the machine. Voters then take their data cards to an electronic ballot box, which reads and records the votes on its memory device and a CD. The electronic ballot box keeps the voters' data cards, which could be used in a recount. No voter verifiable paper audit trail (VVPAT) is used in this system, although this is not "Black Box Voting." A number of issues are presented by the system, including among others the accuracy of data recorded onto the card, the accuracy of how the card's data are read and registered by the electronic ballot box device and the method of vote tabulation. Please see the Country Note in Chapter 4 of this Guide for further description of Belgium's system.

The type of transfer is important because it will determine whether the environment is controlled or uncontrolled, which has an affect on the overall integrity of the electoral exercise. For example, transferring data over public networks, such as the Internet, is performed in an uncontrolled environment, because the devices are networked with numerous computers and servers. Even semi-closed networks, such as governmental networks, are essentially uncontrolled.

If sealed memory cards (or other electronic media or whole devices) are transported by election officials in a secure manner in the presence of party agents and nonpartisan observers, the data would be transferred in a controlled environment. If the environment is uncontrolled at any stage in the transfer, records will be exposed to the potential of entering different input, and therefore to different threats of corruption.

As with the Voter Verified Paper Trail, it is a good practice to back up an electronic record with the paper record. If the counting of votes is performed at the polling station, it would be advisable that the paper record is compiled and transferred along with the electronic one.

Monitoring of data entry and transfer is critically important. As with ballot boxes, memory cards, optical media or magnetic media used to record sensitive information, such as votes or voter registration information, should have unique identifiers and other safeguards to ensure that they are not switched during the electoral process and should have special security mechanisms to ensure against the corruption of data. Before sensitive data is entered, such as recording votes, the cards or other electronic recording media should be inspected to ensure that they are "empty" (politically neutral) before voting begins. These electronic recording devices should be inspected in the presence of party/candidate agents and impartial observers to establish that they do not contain pre-recorded votes or instructions that would corrupt the election. Tests for corruptions should be conducted by reliable methods before and/or on Election Day in the presence of party/candidate agents and impartial observers.

Using uncontrolled methods like the Internet or semi-closed governmental networks to transfer sensitive electoral data multiplies

possibilities for interception and corruption of data. Such means of data transfer require robust encryption systems. If memory cards are removed from electronic devices, the cards can be switched with pre-programmed cards or can be modified before the data is transferred - just as ballot boxes can be switched or stuffed in transport. Special safeguards need to be employed to secure and seal memory cards (just as ballot boxes are sealed and their identity numbers are recorded). This should be done under the view of party/candidate agents and impartial observers. The transport of sealed memory cards with unique identifiers should be accompanied by such monitors. It is generally accepted that the transfer of voting data should occur only after the polls have closed and not during the voting process. Internet voting is an exception to this practice (see below).

THE INTERNET IN ELECTION PROCESSES

Voter Registration:

The Internet as a global public network is increasingly important in the electoral process. Election officials are using the Internet to register voters,[11] display voter lists or individual voter registration records[12] and communicate polling station assignments to voters.[13] Entering voters' relevant information on the spot at registration centers into Direct Data Capture (DDC) devices that allow transport of the data to create a centralized voter registry can facilitate the registration process, and that data transfer is sometimes done via the Internet.[14]

Using the Internet to display voter lists or individual voter registration records can provide an effective means for political competitors and citizens to check the voter lists and verify their accuracy. This can provide the basis for requests for corrections to errors in individual data, to add data concerning individuals who were improperly omitted from the registry and to challenge the appearance on the voter registry of people who died, or the existence of multiple entries for one person or the appearance of persons who are ineligible. As

[11] E.g., State of Arizona (US), Province of British Columbia (CA), Hong Kong SAR.
[12] E.g., Croatia, Palestinian Territories.
[13] E.g., South Africa.
[14] Security issues discussed above concerning transporting such data over open networks or transporting sealed memory cards (or other recording media) apply to voter registration data as well. It is therefore important that the process be transparent to party/candidate agents and impartial observers as the data is recorded and that they are able to verify the security of data transfer. Please see Chapter 3 for further discussion of these issues.

will be discussed later in this Guide, electronic copies of the voter registry can also be provided in a number of forms to political contestants and to impartial election monitoring organizations, so that they can conduct verifications of the registry and assist citizens to check the voter lists and request corrections. These activities contribute to heightened public confidence in the voter registry.

Internet Voting:

Internet based voting presents significant security concerns, where "hacking" and other means of corrupting data appear thus far to overcome the benefits of using this technology in elections for public offices. In addition, serious problems concerning secrecy of the ballot arise in Internet based voting. Therefore, in the view of most experts at this time, Internet based voting is not an acceptable electoral technology.[15]

In very limited examples, the Internet has been used for voting, though Estonia is the only example to date where the Internet has been used for general voting in elections for public office.[16] As mentioned above, Internet based electoral technologies operate in uncontrolled environments. For example, "Remote Internet Voting" is where a voter can vote from any computer that has access to the Internet. In these circumstances, there is no oversight by election officials, which means that voting takes place in an uncontrolled environment. This has serious implications for maintaining the secrecy of the ballot.

"Poll-site Internet Voting" is a system where a voter votes via the Internet, but only in a polling station designated to the voter, with computers provided by and under legal control of election officials. "Kiosk Voting" is basically the same as Poll-site Internet Voting, except voters can choose to vote at any polling place in the election district. These are attempts to create partially controlled environments, but many of the risks to electoral integrity remain unaddressed.[17]

---

[15] For an excellent overview of threats and weaknesses of Internet voting, see David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, *A Security Analysis of the Secure Electronic Registration and Voting Experiment*, Carnegie Mellon Institute for Commerce (January 5, 2004), available at http://euro.ecom.cmu.edu/program/courses/tcr17-803/MinorityPaper.pdf.

[16] It has been allowed for those citizens who possess national ID card with an integrated chip. Internet voting is available in Switzerland, UK and Canada, but it is limited to certain voters or local elections. Please see http://db.e-voting.cc for further information.

[17] Please see Chapter 4 for further discussion of Internet voting and related monitoring issues.

Displaying Voting Results:

Election officials sometimes use the Internet to post election results. Partial unofficial results, as well as complete official results, are increasingly posted on the websites of election authorities. When this is done, it is particularly important to post the disaggregated results (i.e., polling station-by-polling station results for each electoral contestant), as well as the aggregated results. This allows analysis by the political contestants, impartial election monitors and the news media to understand where the results reported came from and to understand what areas have not yet been recorded. This can help prevent premature expectations of victory and premature disappointments and corresponding reactions that can destabilize an electoral environment. In addition, posting disaggregated results allows political contestants and impartial observers to compare polling station records with the copies of results they collected through their agents (poll watchers and observers). This builds confidence in the accuracy of the vote tabulation and results reporting by election officials.

SPECIFIC STANDARDS FOR ELECTRONIC VOTING

Given that internationally recognized standards for electronic voting do not yet exist, countries utilizing such technology are developing their own principles and guidelines. Important elements for discussing standards for equipment, technology and procedures on a national level include the following:

- LEGAL FRAMEWORK requirements that are prescribed by the election laws and other national laws and electoral administration bylaws and regulations;

- TECHNICAL REQUIREMENTS and specifications developed by electoral administration;

- PRINCIPLES FOR DEMOCRATIC ELECTIONS set forth in international instruments and developed by international organizations;

- PRODUCTION STANDARDS of manufacturers;

- INFORMATION TECHNOLOGY STANDARDS developed by expert and standards setting organizations.

To date, the most significant multinational attempt to develop international standards for electronic voting is the "Recommendation of the Council of Europe Rec (2004) 11."[18] This document and the corresponding associated Explanatory Memorandum provide non-binding recommendations to the member states on how to implement electronic voting. Rec (2004) 11 deals with a very broad set of issues and includes legal, operational and technical standards.

It is noteworthy that the Council of Europe (CoE) Recommendation endorses the use of EML 4.0, Elections Markup Language[19] developed through an open process by the Organization for the Advancement of Structured Information Standards (OASIS[20]). EML is a standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services to public or private organizations. The services performed for such elections include but are not limited to voter list maintenance, redistricting, requests for absentee/expatriate ballots, election calendaring, logistics management, election notification, ballot delivery and tabulation, election results reporting and demographics.

In the United States, there is a shared responsibility between the three levels of government in overseeing the conduct of elections. Each state sets its own guidelines for the conduct of local, state and federal elections. In turn, states have generally delegated the authority to conduct elections to smaller subdivisions, such as counties, cities or towns. As a result, there are thousands of jurisdictions that administer federal elections throughout the country. However, states must comply with requirements set forth in certain federal legislation in order to receive funding for electoral matters and concerning certain elements of federal elections. The Help

[18] Recommendation Rec (2004) 11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and Explanatory memorandum on Legal, Operational and Technical Standards for E-Voting. Please see Appendix 3 of this Guide for an excerpt of REC (2004) 11.

[19] See Cover Pages, *Election Markup Language*, (last modified August 14, 2007), available at http://xml.coverpages.org/eml, for an overview of the design goals and standards of EML 4.0, the Election Markup Language developed by OASIS and approved by the Election and Voter Services Technical Committee.

[20] OASIS (Organization for the Advancement of Structured Information Standards) is a nonprofit, international consortium whose goal is to promote the adoption of independent standards for information formats (www.oasis-open.org). For more information, please see Appendix 2 of this Guide.

America Vote Act (HAVA), for example, mandates federal standards[21] for the functionality, accessibility and security of voting systems across the country, as well as for allocating funds to states to help upgrade outdated equipment.[22] HAVA is not exclusively an electronic voting standard; it addresses other types of voting. HAVA established the US Election Assistance Commission (EAC), which-in cooperation with the National Institute of Standards and Technology (NIST)—is developing voluntary guidelines for voting systems. The voluntary voting system guidelines (VVSG) will provide a set of specifications and requirements that voting systems, voting devices and software must meet to receive a certification from the EAC. Under HAVA, adoption of the VVSG by the U.S. states would be voluntary. Nonetheless, states may adopt the VVSG and make them mandatory within their jurisdictions. EAC accredited laboratories will test electronic technologies against the VVSG and provide a recommendation to the EAC, while the EAC's Executive Director will make the decision concerning whether to issue a certification. When activated, this will be the first time that federal authorities will test and certify voting systems. Previously, voting systems were tested and certified by companies qualified by the National Association of State Elections Directors (NASED).[23]

INFORMATION TECHNOLOGY STANDARDS

There are many recognized private, public, national and international institutions that are developing standards for information technology (IT). The largest and most developed is International Organization for Standards (ISO), but there are many more recognized by the IT industry.[24] These standards, however, are not specific for electronic elections systems or specific products. They deal, for example, with process, security requirements, management certification and audit processes.

---

[21] Although HAVA is legally limited to federal elections, in practice it influences virtually all elections in the US. It addresses requirements for the electronic voting such as: testing, certification, decertification, and recertification of voting system hardware and software. Also, voting system standards and requirements are addressed (in Sec 301). See generally, Help America Vote Act (HAVA), 42 U.S.C. § 15301 (2002).

[22] There are numerous relevant bills currently in the U.S. federal legislative process (e.g., Voter Confidence and Increased Accessibility Act of 2005, Voting Integrity and Verification Act of 2005 (VIVA 2005), Count Every Vote Act of 2005, Voting Opportunity and Technology Enhancement Rights Act of 2005 (VOTER Act of 2005), Know Your Vote Counts Act of 2005, Verifying the Outcome of Tomorrow's Elections) and many before the State legislatures.

[23] "EAC Seeks Public Comment on TGDC's Recommended Voluntary Voting System Guidelines," U.S. Election Assistance Commission Press Release (31 October 2007) (www.eac.gov).

[24] For example, Institute of Electrical and Electronics Engineers (IEEE), NIST, European Committee for Standards (CEN), and OASIS. See Appendix 2 of this Guide for more information.

IT specialists who are engaged in evaluation of the electronic voting and other IT systems in electoral process should be acquainted with these standards, as they provide internationally recognized framework. Election monitoring specialists associated with political contestants and impartial observation organizations should be familiar with these standards to better evaluate some components of the electronic elections system, though they do not provide information concerning how specific elections equipment or software should be built or should perform.

CHAPTER THREE:

Monitoring Electronic Techonologies Used in Voter Registration

INTRODUCTION

Voter registration is vital to democratic elections. In many countries prospective voters cannot cast ballots unless their names appear on the voter list at a specified polling station or are otherwise verified as being included in the registry of voters. A proper voter registration process is thus a prerequisite to citizens being able to exercise the right to vote and the right to be elected. Voter registries are developed in different ways, and increasingly they employ electronic technologies. This creates a need to review the ways that the public and the political contestants can gain confidence in voter registration efforts through transparency and monitoring of electronic technologies used in the process.

Observation groups and political contestants that are evaluating a voter registration process will soon realize that voter registration is administratively complex and technically sensitive.[25] For example, where election officials generally respect voter eligibility requirements and follow the law and regulations for registration of voters, a significant number of voters nonetheless could find themselves excluded from the voter registry — and thus disfranchised — because of poor execution of the registration process. There are numerous examples where the production of the voters list was problematic because of the poor use of information technology. There are also examples, such as in the 1994 Dominican

[25] This Guide concentrates on IT in the voter registration process. For a discussion of monitoring the broader administrative and other aspects of voter registration, please see generally, Richard L. Klein, Patrick Merloe, Building Confidence In the Voter Registration Process: An NDI Monitoring Guide for Political Parties and Civic Groups (NDI 2001), available at www.ndi.org.

Republic elections, where the final voter lists were printed and distributed to polling stations based on a fraudulent manipulation of the database. As with monitoring technologies used in other aspects of the electoral process, evaluation of the use of technologies in voter registration provides valuable information on the quality and integrity of the election.

It is important to note that evaluating the use of technology in the registration process can be cost and time effective. While monitoring the use of electronic technology in voter registration may require detailed knowledge of specific technologies, developing an understanding of basic principles is important for deciding on monitoring approaches. Even if observation groups and/or political contestants do not have a capacity to evaluate in detail a specific technology or range of technologies being considered for application in the voter registration process, they should have a firm basis for approaching the issues and for determining what kind of assistance they may need.

UNDERSTANDING VOTERS LIST DATABASES

If the voters lists are electronic and not paper records, they are contained in an electronic database. The lists can be kept in some decentralized form, for example by election district or municipality, or they can be centralized into one national voter registry. In order to understand how election authorities are managing registration of voters and how they operate voter records, it is necessary to grasp the basics of how databases work and some terminology related to databases and formats of the voter data.

"Voter's Record" is all of the information related to the individual voter.

"Primary Voters List Database Data" is information that is required to be in the voter lists by electoral legislation (for example, first name, last name, date of birth, etc.).

"Secondary Voters List Database Data" is information that is not required by the legal framework, but is useful in overall administration of the electoral process (for example, assigned polling station, flags, record tracking data, etc.).

"Format of the Voter Record" will define the kind of operations that are possible with the data. Following are simple examples to illustrate this.

In case A, the voter record is divided into three columns. If the electoral authorities want to separate voters according to a specific criterion such as provence, for example, it would not be simple to do so.

Case A

Name	*Address*	*Region*
Maria Chen	Main Avenue #13 Springfield, Sojob Provence	Eastern

In case B, it would be possible to separate voters based on several criteria.

Case B

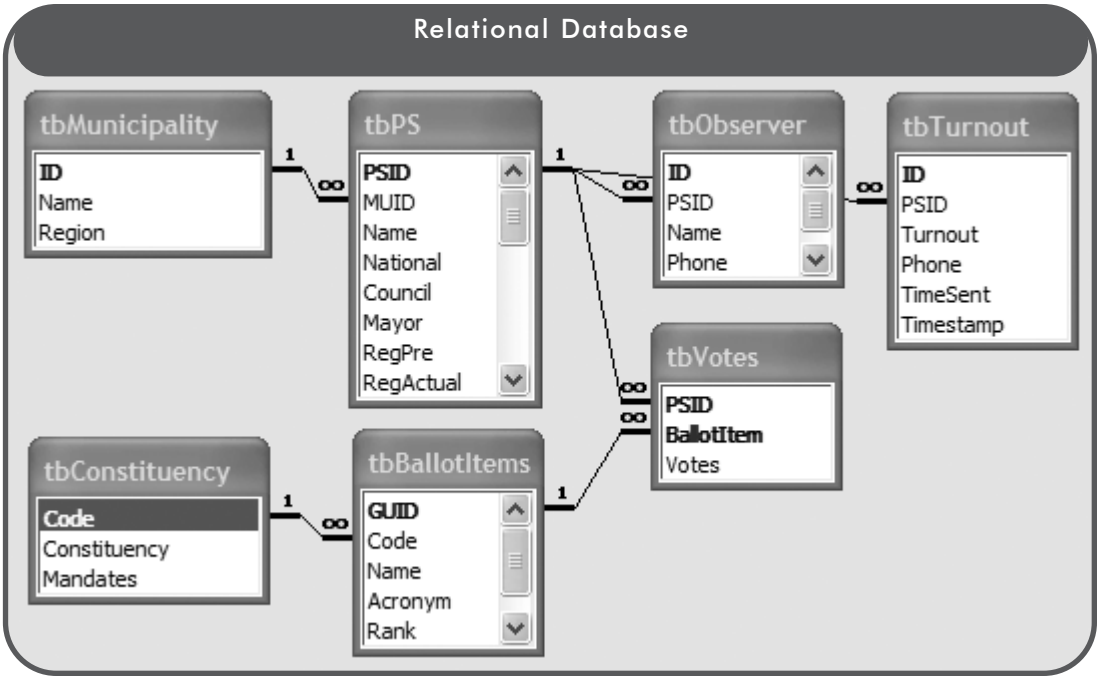
First Name	*Last Name*	*Street*	*House*	*Town*	*Provence*	*Region*
Maria	Chen	Main Avenue	13	Springfield	Sojob	Eastern

"Flat Databases" look like a spreadsheet. They have a simple design; each row represents one voter; columns contain information on each voter's first name, last name, date of birth, and extended address with complete geographical information. The data can be easily observed, but management and processing of the data is not practical. The redundant nature of some of the data increases the size of the data file, making it difficult to update and run queries.

Flat Database

District	Last Name	First Name	Date of Birth	Address
01.01	Tsai	Coonoor	10/10/1977	590 Jacarundu Street #2
01.01	Absher	Luis	2/8/1944	1910 Ficus Avenue
01.01	Cadogan	Jumana	5/7/1964	2223 Easy Street #5
01.01	Martinez	Tatiana	12/29/1965	2085 Esperanza Boulevard #4
01.01	Dansoko	Fawzi	3/7/1960	2445 Dulal Road

"Relational Databases" are designed in a more complicated way, in order to increase efficiency of the computing and data manipulation process. They have many tables that are related and "share" information. For example, it is very likely that the information about which polling station a voter is assigned will appear in a column that receives the information on polling station assignments from a different table.



"Database Product" is an output of the database containing a compilation of information available in a variety of formats intended for the end user. For example, a database product could be a printout of a final voters list or a webpage where a voter can correct his or her records or data for electronic poll books. To evaluate the product of the database, it is necessary to understand the architecture of the database, because the product does not indicate how the data were processed and whether there were technical flaws in compiling the list. For example, the exclusion of underage voters could have failed because the label in the database that marks underage voters was not part of the query that extracts the records of eligible voters.

"Database Exports" are electronic versions of some or all of the records in a database intended to be used by another database and thus not "intelligible" for people. The export can be described as an intermediary product.

"Database Design Requirements" are set by the election authorities and inform the specifications that are used by programmers to build the database. Requirements should be derived from the needs of the electoral process. It is impossible to build an adequate database without first understanding what kind of data are collected and used. Once the input of the data into the database initiates, changes in the database architectures are limited and risky. Adding or removing capabilities from the database is best done at the requirements phase of the process. A poorly conceived and poorly built database leads to repetition of input of records, an inability to properly manipulate records and corrupts the transparency of the database.

"Database Accountability" refers to the requirement outlined in the database design that, in addition to voter records, requires the database to keep records of changes, deletions and insertions for review purposes.

USE OF EXISTING RECORDS— TRANSFER OF RECORDS

When existing databases (such as civil registries) are used as a basis for creation of the voter list,[26] election monitors and political contestants usually do not have complete access to the "original" databases. Their access is limited to the voter list database. However, in order to understand the transfer process of the voter records from the original database to the voter list database, political contestants and election monitors should understand the following features of the original database:

- process of the data collection;
- management and update of the records;
- compatibility of the database with requirements of the voter list; and
- capability of the database to export the data and the features of the export.

[26] In some countries the civil registry is in fact a register of voters and does not involve creation of the separate voters list that is managed and updated by election officials—for example, Denmark and Sweden follow this model.

It is often impractical to use existing original databases as the voter list database. They are not built to serve as voter list databases, and they contain information that is not related to the voter list. Therefore, the transfer of records will not be a simple process of copying the original database. Data have to be prepared for the "receiving" (voter list) database; and they need to be exported in the format that the voter list database can receive.

In countries with a long history of voting and use of existing civil registries for the creation of the voter list, civil registry database design and integrated data management tools are sometimes utilized for efficient export of the civil registry records to the voter list database.

Even if the civil registry is well maintained and contains all of the data required for the voter list (including primary and secondary voter list data), the transfer of records to the voter list database can be troublesome and even create a fatal flaw in the process.

In countries where the use of existing records for compiling the voter list is a first time occurrence, it is common for there to be numerous problems with the process. These problems multiply in cases of corrupted records, inadequate maintenance of the data, interrupted management of the dataset and in translation/transliteration of records in different scripts and languages.

Data Migration Process:

Where the civil registry is used as the basis of the voter registry, moving information from the civil registry into the voter registry will involve a data migration process. Data migration between these two systems, built in different ways to serve different purposes, can present a number of challenges. Differences in data contained within these two systems present the first challenge. Monitors should ask whether the information in the civil registry is sufficient to cover the primary and secondary data required for elections. Data migration can also be compromised by technical differences between these systems, such as differences in database design, software used and field formats. Migration must be careful to avoid losing relationships, primary/foreign keys and character sets.

Formatting of Fields and Records:

Every database has a defined format for each field. This information is integrated into the database. Fields that contain geographical locations will have different parameters than fields that contain dates or "flags." If the format of the field is not properly transferred into the data export, the receiving database will have difficulty recognizing these fields and may interpret them incorrectly.

The format of the records (e.g., how the individual records are divided in columns) will dictate what operations are possible with the records. For example, if address fields are not properly structured, it will be impossible to automatically assign the voter to a specific district or polling station. The process would have to rely on manual checking of the records or involve some type of software that would recognize addresses and assign the proper location code. In the case of automated recognition of addresses, error rates may be significant and correction efforts must be planned.

COUNTRY NOTE:
Ukraine 2007 - Incompatibilities of Databases Required 11 Million Manual Re-Entries on Voter Lists

Ukraine held early parliamentary elections in 2007 as a result of a protracted political crisis. Amendments to the election law required the voter registry for the 2006 elections be sent by the Central Election Commission (CEC) to 679 Working Groups around the country for them to merge the 2006 voter lists with databases from 10 state agencies and otherwise update the voter lists. Incompatibilities between database software resulted in the manual re-entry of information for approximately 11 million prospective voters. The Working Groups delivered draft voter lists to the District Election Commissions, as required by law, without passing them back to the CEC for it to create a national voter registry and/or to conduct verifications as was done in the 2006 elections. There was a short period for the public to scrutinize the voter lists and file for corrections, and the corrections process was not well publicized. While the quality of the voter lists varied around the country, double and multiple entries occurred in significant numbers on the 2007 lists, while other problems led to exclusions of qualified voters from the lists, thus creating opportunities for illegal voting as well as disenfranchisement. These factors led to lower public confidence in the voter lists and a general assessment that the 2007 voter lists were not as accurate as those of the previous year.

Sources: "Preliminary Statement of the NDI International Observer Delegation to Ukraine's September 30, 2007 Parliamentary Elections", NDI (1 October 2007); "Statement of Preliminary Findings and Conclusions on the 30 September 2007 Parliamentary Elections in Ukraine", OSCE, et al. (1 October 2007); "Pre-Election National Monitoring Report", OPORA (Support)(27 September 2007).

Unique Identifiers:

Unique identifiers are also called "primary keys." These are entries in the databases that serve to unmistakably identify a specific set of information, for example, a voter. Rather than linking different pieces of information to the voter's name, a primary key is assigned to the voter so that the database effectively identifies individual voters. These keys must have a standardized, distinct and well defined format so that the database can properly maintain relationships between different pieces of information.

Software Compatibility:

Software of the original and receiving databases have to be compatible so that the export of the data from the original software can be imported into the receiving database without loss of individual pieces of information or relationships between the data. One of the most common problems is different language schemes and definitions of character sets between exporting and receiving databases. Databases might operate with different systems that define letters and numbers. Even within the same language script there could be differences in use of coding standards. The situation becomes more complex if the script of the exporting database has to be transliterated into a different language script for the receiving database.

COLLECTION OF DATA

Creation of a voter list that is a "voter registry" independent from other registries (such as, the civil registry) involves collection of voter data by election authorities. However, rarely is an independent registry truly independent. There are almost always aspects that depend on the work of other institutions (e.g., the Ministry of Interior that issues ID cards or other proof of citizenship or the Transportation Department that issues driver's licenses, which are used by voters to prove their eligibility). Also, it is not unusual in these circumstances for the creation of the independent voter registry to be a one-time occurrence, and updates to be processed by some automated mechanism that requires sharing of data with institutions that are issuing birth, marriage or death certificates or some other means of recording the status of citizens.

It is important that monitors understand all manners of populating the voter database and recognize there will inevitably be some degree of error in creating the voter list. Database design and management processes should include "built in" tools to tackle this issue, but monitors should also look into what steps are taken to minimize, uncover and correct error.

This section will discuss issues related to the monitoring technologies used in the creation of the voter list, irrespective of whether the creation will be a one-time occurrence or continuous or periodic exercise, or whether it will be a voter-initiated or state-initiated process. What they all have in common is that the voters' data are not immediately recorded as electronic records in a central voter registration database and that fairly complex and sensitive operations must be used to collect and process these data.

Whether the collection of the data is done by direct or indirect recording, it is important to determine what type of information is being captured and whether this reflects the requirements of the legal framework. If election authorities are collecting data beyond what is required by the legal framework, this must be properly justified or discontinued. If election authorities are collecting data that will be shared with other governmental institutions, this should be disclosed.

Direct Recording:

Direct recording involves creating an electronic voter record at the moment and location when the voter (or his or her proxy) submits the data to the election officials in accordance with the law and regulations. In direct recording, voters do not fill out a form that will later be entered into the voter database by scanning or data entry in some remote location. Rather, their data is captured directly at the registration point using electronic equipment.

Development of the System. Observation of the direct recording technology must start at the point when election officials are developing specifications for hardware and software requirements. These requirements must match the model of the registration exercise — for example, mobile versus stationary registration points or a large number of points versus centralized locations. Equipment

requirements will differ if the equipment has to be transported or if it is stationary, if it relies on infrastructure (such as, electricity or networks) or if it is designed to work without infrastructure (for example, to run on batteries).

Software. Electronic records that the registration equipment creates must be compatible with the voter registry database so that records can be easily and accurately transferred to the central database. Principles discussed above, under "transfer of existing records" apply here too.

Testing. Direct recording equipment should be properly tested before it is deployed. Tests should be performed following the "end-to-end" principle, meaning that the complete process is simulated with actual components of the system and exact copies of the software in an environment that is similar, if not exactly the same as, the type where the equipment will be utilized. A complete testing and monitoring process requires recording data of people involved in the test at the actual registration points and transferring this data to the central database. In addition, "load tests" should be performed to gain a better understanding of how the equipment deals with the expected number of transactions and whether projections of the number of processed voters are realistic. Tests should also be conducted concerning how the database responds to malfunctions and problems.

Tests are performed not only to verify functionality of the equipment and the process, but also to examine usability of the system, both from the voters' and election officials' point of view. Beyond the functioning of equipment, authorities should solicit the opinions of all those involved in testing - simulated voters, officials handling equipment, supervisors and others. Monitors from political contestants and election observation groups should be allowed to provide input regarding any concerns they may have before tests are designed, review and ask questions about the testing procedures before they are conducted, witness all testing and be provided timely access to the opinions of all actors involved in the testing.

It is not expected that monitors from election observation groups or political contestants will perform these tests; however, they need to be able to evaluate how the testing was performed. Testing of the

systems is part of the electoral process. It requires that election officials have a clear test plan and that testing and outcomes are recorded and shared with monitors in a timely and understandable manner.

If tests are performed on a smaller scale, for example on a small sample of equipment, the tests are considered design tests or model tests. Performance tests are those that test the complete set of equipment. If the election officials do not perform a full scale performance test, it is necessary to establish criteria by which a sample of the equipment will be tested. The sample should be on a proper statistical probabilistic sample, where every piece of equipment that will be deployed to registration points has the same chance to be selected. Tests should not include just "the first 100 pieces of equipment delivered" or other arbitrary criteria because such tests have proven to be unreliable indicators of how the full set of equipment will perform.

Monitors from the political contestants and observer groups should be allowed to review sampling methodology. Monitors from observation groups and political contestants must thoroughly understand the system in order to evaluate whether performance tests can be reduced to test a sample of the equipment. Sometimes it is absolutely necessary to conduct full scale tests, especially if the equipment requires calibration and fine tuning (such as bio identification systems like fingerprint scans) or if it is impossible to troubleshoot problems once the equipment is deployed.

Accountability. As with every other aspect of the electoral process, direct recording of voter data should follow the principle of accountability. This means that every sensitive action should be recorded and stored to provide opportunities for possible examination. Since electronic records are not accessible to the public, individual voters cannot verify whether the equipment recorded their data properly. Therefore, direct recording registration systems must provide each voter with proof of her or his submission of their data. This proof can be a printout of the voter's record or some other type of receipt or certificate. Voters thereby are given an ability to prove their involvement in the registration process, which is usually needed in order to seek remedies should they discover errors or omission of their data.

In addition to the receipt that confirms submission of the data, the voter should receive a unique number for the transaction that will serve as an identifier. The receipt and identifier can aid voters in exercising their right to check the preliminary voter list and demand corrections if data is erroneously recorded or if the voter is somehow omitted from the list. The receipt and identifier also can aid election observation groups and political contestants to conduct independent verification exercises with the consent of registered voters, who agree to participate in such efforts.

Security, Back Up and Data Transfer Procedures. Security procedures should address two principal issues: (1) security of the data regarding unauthorized access and manipulation of data; and (2) security regarding potential loss and corruption of data. Election authorities should have defined security procedures that are made available for review by monitors from observation groups and political contestants. Monitors would not obtain security codes granting them access but would be able to comment on whether the procedures themselves seem adequate.

To ensure adequate security, data must be protected with technical and organizational solutions, and election officials should employ both methods to secure the data. Technical solutions are built in to the equipment and limit access to authorized election officials. Equipment must be tamper resistant or at least tamper evident. Technical security solutions should also have clearly identified access levels - not all of the officials should have access to all of the data and processes. Organizational solutions are a set of rules that election officials must respect to protect access to the system.

In order to protect data captured at the registration points, election officials must design a reliable back up process. Back ups have to be regular, scheduled and documented. Also, backed up data should be stored independently from the direct recording equipment, so that in case of malfunction of the equipment and loss of the original data, back ups are preserved. Storage and management of the back ups should also be included in design security procedures.

Monitors from political contestants and observer groups should also be allowed to evaluate procedures for the data transfer. Data transfer can be physical (e.g., by moving memory cards from the direct data

capture equipment to the central database) or through a computer network. Data transfers are sensitive points in the process since they pose a challenge to protection of the data by introducing elements of uncontrolled environments. Monitors should be allowed to accompany physical transfers or evaluate such transfers based on sampling techniques and should be allowed to evaluate transfer of data by networks through reliable techniques, such as comparing data sent from a particular machine or registration center (or sample of machines or centers) to corresponding data recorded centrally.

Development, Delivery, Maintenance, Troubleshooting and Service of Technologies. Ensuring the proper functioning of the direct recording equipment and related technologies—like every other aspect of election administration—is the legal responsibility of the election authorities. In effect, the election authorities have a duty to properly discharge the obligation of government to provide genuine democratic elections to the citizens, including to the voters and to those standing for election. It is common that election authorities outsource development and production of the technologies to independent companies, and they often rely on the private companies (that many times are foreign entities) to deliver, maintain, service or otherwise troubleshoot problems with the technologies. This normally creates a legal contractual relationship between the election authorities and equipment producers (vendors) and/or servicers. However, that legal relationship is subordinate to the election authorities' legal obligation to citizens, which is set by the country's constitution, electoral law and often reinforced by international human rights obligations.

The role of the equipment producers and/or servicers and the capacity of the election officials to service equipment is an important consideration in ensuring electoral integrity. The importance of building capacities of election authorities and avoiding over-reliance on vendors is essential to meeting a government's obligations to organize genuine democratic elections. Delivery of equipment should be complemented by the transfer of know-how to electoral authorities to effectively service the technologies, or electoral authorities must ensure that producers and/or servicers are in-country and in position to provide effective service that allows the technologies to perform according to the registration plans. Otherwise, the entire voter registration process can be jeopardized.

Contracts therefore should be open to scrutiny by observation groups and political contestants.

COUNTRY NOTE:
Nigerian Elections 2007 - Use of Electronic Technologies in Voter Registration

While the Nigerian electoral act prohibits electronic voting, the Independent National Election Commission (INEC) decided to employ direct data capture (DDC) devices to create an entirely new voter registry for the series of elections held in 2007. DDC technology would have enabled officials to electronically enter and store information about each voter who appeared at registration locations and then transfer the information to a computer database. Election authorities would then have been able to conduct various checks to ensure the integrity of voter lists, for example, to identify duplicate records and thus prevent double voting. However, the INEC's very tight and optimistic timetable proved not to be realistic. INEC expected to procure from three companies a total of 33,000 DDC machines by early November in order to complete registration of an estimated 70 million eligible voters by the December 14 legal deadline. At the beginning of registration only about 1,000 DDC machines were operational, and due to a number of factors, including delayed payments to the vendors, the 33,000 machines were not in place until mid-January. Only about 5,000 of the machines were voter registration devices, while the majority of machines used were laptop computers with digital cameras. In addition, registration staff apparently did not receive sufficient training on the use of the DDC devices. The batteries provided had a short life span and recharging facilities were limited in number, often rendering the DDC devices unusable. The printers frequently jammed, and there were shortages of ink. A manual registration process had to be used as back-up. The result was significant delays beyond legal deadlines, a problematic correction period, which led to likely disenfranchisement, and opportunities for illegal voting due to inaccurate voters lists. While aggregate registration figures were made public, there were questions about the large volume of registrations in the final phase of the exercise. Public confidence was further compromised because significant access to the voters list was not provided to political parties or domestic and international observers prior to election day. Eighteen political parties joined in a court challenge concerning noncompliance with legal provisions on voter registration.

Sources: "NDI Final Report on Nigeria's 2007 Elections,"; "Nigeria Final Report: Gubernatorial and State House Elections 14 April 2007 and Presidential and National Assembly Elections 21 April 2007," European Union Election Observation Mission.

Obligations of the producers and/or servicers after delivery of the products should be clearly defined by contracts that carry an appropriate level of guarantee that the producer will indeed effectively service the equipment. The contracts should address obligations to effectively remedy breakdowns of equipment due to design flaws, as well as due to operation in high temperatures, high humidity, exposure to sand particles, failures of batteries needed to operate equipment as specified; and the ability to rapidly provide replacement parts and otherwise ensure equipment performance. The schedule for delivery of equipment needed to meet the election

authorities' voter registration plan should be verified against the producer's available inventory and production schedule (including obligations to deliver equipment and technologies to other countries). All of these issues have had serious negative effects on voter registration processes and must be taken into account.

It must be expected that something will go wrong during registration of voters. Tests should help to identify and minimize weak points and reduce malfunctions, but officials must expect and plan for problems. A bigger problem than failure of some components is not having an effective response plan. Response plans must be clear and documented. They must define response steps, response times and roles. If the response involves the equipment producer or another contracted company, this should be clearly defined in valid contracts. Such response plans should be made available to observer groups and political contestants, with opportunity for their comment. This is an important point for genuine transparency and confidence building.

Training. Election officials who perform voter registration should be trained in verification of the voter's eligibility, in how to properly record the data and in how to otherwise operate the equipment. They must understand the functioning of equipment (technologies) on at least a basic technical level in order to identify problems, to be prepared to correct them on the spot, if possible, and to request appropriate assistance and service.

The training should be in line with standard training requirements - trainings should be thorough, mandatory, standardized and include simulations of normal procedures and responses to malfunctions. Monitors from observer groups and political contestants should as a best practice be allowed to review training plans and materials before they are employed and to provide comments. Monitors should in any case be allowed to attend and observe training sessions to build confidence in how officials will be prepared to use technologies during the voter registration process.

Indirect Recording:

Indirect recording of voter registration data employs collection of data through non-electronic means, which is later processed and

electronically recorded into the voter list database. Data are first collected on paper forms and then entered into computer systems either by manual data entry or scanning.[27] Scanning technologies as well as manual data entry present a number of challenges to electoral integrity. Monitors from observer groups and political contestants should be allowed to witness end-to-end testing or performance testing of scanning technologies, as with direct date capture technologies. Issues related to development, production, delivery, servicing, maintenance, troubleshooting and training discussed above also apply to indirect recording technologies.

Forms and Data Sources. There are two principal categories of data sources for indirect recording of voter data. The most usual source is forms created for the purpose of data collection. However, there are cases where election authorities use existing paper records, such as index cards or previous non-electronic voter lists. The primary difference is whether the election authorities are creating a new data collection from scratch or relying on existing paper records. If starting from scratch, the election authorities can (and should) design their data collection process and forms with the database and their information needs in mind. If they rely on existing paper records, the election authorities will have to be more creative in how they digitize the existing information and introduce it into the database. These processes are vulnerable to error in different ways.

Forms for capturing voter information must be designed to be compatible with the format of database records. Improper design of the fields on the forms, for example, leads to problems (or at least complications) when merging the data recorded on the forms into fields in the database. Form fields must be properly coded to speed up and facilitate data entry. It is also advisable to code the forms with a unique number in order to create a paper audit trail.

In terms of layout, forms have to take into consideration the applicable data entry method — a form that is prepared for scanning is different than one that will be used for manual data entry. The scanned forms have to be machine readable, while the manual data entry forms have to be human reader friendly. In either case, the forms must be understood by the person filling them out — whether

[27] In exceptional cases, data can be gathered with some other type of electronic record that would still need additional processing. An example would be typing the data into a word processing program that is not compatible with the voter list database and then "re-recording" the information into the database. In such processes there are risks that data could be corrupted, while the original record could be easily lost.

that is an election official or a prospective voter. A form that is easily readable by a scanner or data entry person that nonetheless is likely to lead to improper or incomplete information presents a major problem for the integrity of the registration process.

Forms therefore also should be available for review and comment by monitors from observer groups and political contestants. Having confidence in form design will provide a basis for building confidence in the training of the election officials who will complete the forms and/or in voter education — both of which are additional elements of the registration process that should be open to monitors.

Data sources (such as prior voters lists or index cards) that are not designed for data entry will likely present problems for scanning. If such sources are to be scanned, proper testing should be performed to determine a practicable entry method. If they are to be entered manually, it is advisable that the information on the paper be marked with field codes in a pre-entry process, especially if the layout of the forms is not data entry friendly.

Both types of data sources might require reformatting, converting and coding of certain kinds of information, for example conversion of dates from different types of calendars or coding of geographic areas.

Understanding the format of the data sources is useful for anticipating the kind of challenges that the source is likely to pose for the data entry process. Knowing how and why the data was prepared and reformatted to accommodate the data entry will also help. There have been cases when data entry has failed because of poor preparation of the data source. Therefore, plans for such data entry should be open to review and comment by monitors from observer groups and political parties.

Manual Data Entry. Entering voter data into the voter database is a large undertaking because election authorities have to enter millions of records. The capacity of the data entry system is therefore an important issue. Planning of the data entry system should involve testing such capacities. Testing would involve load tests (to determine how much of the data can be processed in a given time period), performance tests (to determine if the data entry interfaces respond

well, if the networks are stable and the server can deal with large numbers of entries) and functionality tests (to determine if the interface design is appropriate and does not contribute to data entry errors). These tests, including review of testing results and recommendations, should be open to monitors from observer groups and political contestants.

Every data entry system should have different levels of access for operators, supervisors and administrators. Operators should not be able to access any records except those that they are currently entering. Supervisors and administrators should have higher levels of access, and their involvement should be necessary to correct and edit the data.

Every data entry system should include post-entry checking. This means that printed listings of the data should be given to a group of editors (verifiers), who would compare entered records with the data source (e.g., forms). Any errors should be marked and their findings passed onto supervisors and administrators, who take corrective action. This measure reduces greatly typing mistakes and other human errors. Another way to insure the quality of data entered is double entry. Double entry involves entering the same data by two separate groups of operators in two separate operations. Data are then compared and records that don't match are marked for inspection. Reports of the percentage of mistakes identified and corrected should be available to monitors from observer groups and political contestants.

As in every database operation, the complete audit trail should be recorded in the data entry software. Recorded information should include the time of the creation of the record, its source, the operator, each change and who authorized each change. Monitoring of such information could be done by experts or independent audit firms contracted by observer groups or political contestants and charged to evaluate whether proper procedures were followed in production of final voter lists.

Scanning — Optical Mark Recognition and Optical Character Recognition. The advantages of employing scanning technology over manual recording of voter data for voter registration are obvious — they significantly reduce the need for large infrastructure and data

operators. However, scanning machine error rates have to be known in advance, and plans are needed to identify and correct errors. Human "reading" of scanned data, back up manual entry and correction of the records must be considered.

VOTER REGISTRATION DATA ENTRY IN BOSNIA-HERZEGOVINA SCANNER VS. MANUAL ENTRY

	Scanner	Manual Entry
Registrations	3,500,000	3,500,000
Forms per hour	4,500	60
Work hours per day	16	12
Forms per day per person/scanner	72,000	720
Scanner/person days required	49	4,861
Number of scanners/persons	5	100
Total forms per day	360,000	36,000
Days to complete data entry	10	96
Error rate	0.10%	2.00%
Forms to be re-entered	3,500	70,000
Re-entry days	>1	2

Source: Final Report, OSEC Elections Assessment Team, Mission to Bosnia and Herzegovina, January 30 1996

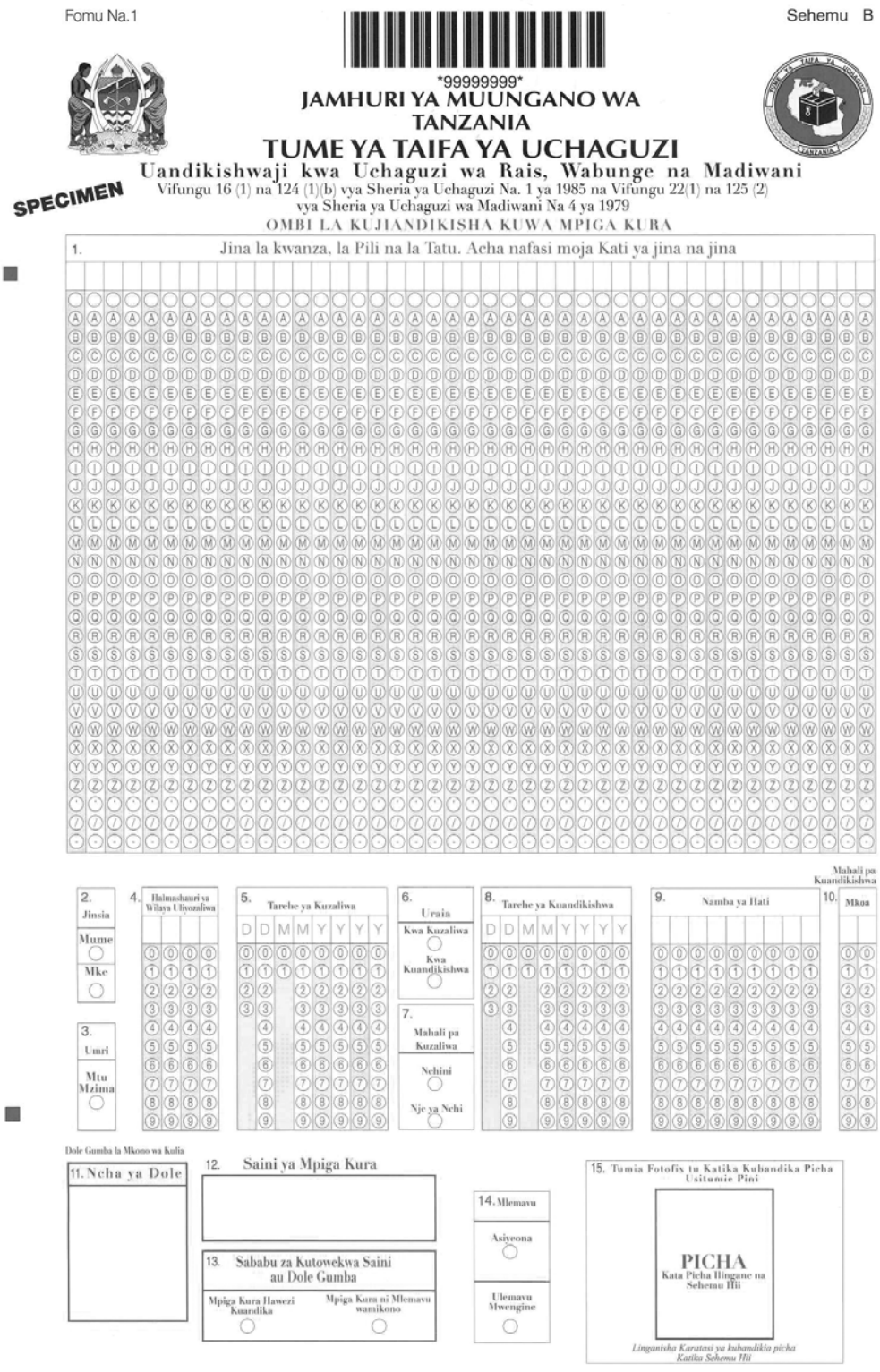
More than manual data entry, the quality of the scanning will depend greatly on the format of the data source. A data source that was not formatted for scanning will likely create so many corrupt records that the whole exercise could well be futile. The format of forms prepared for scanning is not user friendly for human readers because it is designed for the scanner and scanning software.

OMR systems are more accurate than OCR systems.[28] The OMRs recognize marks entered on forms, while OCRs are used for processing written data. To improve accuracy of the scanning process of OCR applications, it is advisable to numerically code as much information as possible; limiting input to just digits reduces the number of character options and therefore opportunities for misinterpretation.

It is possible for election authorities to use scanners without OCR software and create images of the form - these systems are much cheaper than those equipped with OCR software. Scanned images

[28] Please see Chapter 2, "Optical Mark and Optical Character Recognition," for further discussion of this subject.

Optical Mark Recognition (OMR) Form
Source: National Election Commission of Tanzania



Fomu Na.1

Sehemu B

99999999

JAMHURI YA MUUNGANO WA TANZANIA

TUME YA TAIFA YA UCHAGUZI

Uandikishwaji kwa Uchaguzi wa Rais, Wabunge na Madiwani

Vifungu 16 (1) na 124 (1)(b) vya Sheria ya Uchaguzi Na. 1 ya 1985 na Vifungu 22(1) na 125 (2) vya Sheria ya Uchaguzi wa Madiwani Na 4 ya 1979

SPECIMEN

OMBI LA KUJIANDIKISHA KUWA MPIGA KURA

1. Jina la kwanza, la Pili na la Tatu. Acha nafasi moja Kati ya jina na jina

2. Jinsia — Mume ○ Mke ○

3. Umri — Mtu Mzima ○

4. Halmashauri ya Wilaya Ulivozaliwa

5. Tarehe ya Kuzaliwa (D D M M Y Y Y Y)

6. Uraia — Kwa Kuzaliwa ○ Kwa Kuandikishwa ○

7. Mahali pa Kuzaliwa — Nchini ○ Nje ya Nchi ○

8. Tarehe ya Kuandikishwa (D D M M Y Y Y Y)

9. Namba ya Hati

10. Mahali pa Kuandikishwa — Mkoa

Dole Gumba la Mkono wa Kulia

11. Ncha ya Dole

12. Saini ya Mpiga Kura

13. Sababu za Kutowekwa Saini au Dole Gumba — Mpiga Kura Hawezi Kuandika ○ Mpiga Kura ni Mlemavu wamikono ○

14. Mlemavu — Asiyeona ○ Ulemavu Mwengine ○

15. Tumia Fotofix tu Katika Kubandika Picha Usitumie Pini

PICHA
Kata Picha Ilingane na Sehemu Hii

Linganisha Karatasi ya kubandikia picha Katika Sehemu Hii

are then transferred to a central location and processed by higher quality computers using OCR software, which can produce records with fewer errors. An audit trail of the scanning data entry is provided by the image of the registration form or other paper data source.

No matter what kind of database is used to store images of the form, it must connect the image and the paper record to provide accountability. If scanners without OCRs are used, a system for manual marking of the forms should be developed. Such a marking process would assign a unique identifier to the paper form that is recorded with the form's image (usually within the image file). If OCR or OMR is used, those filling out the form should be given sufficient instruction on how to complete the form in a way that will minimize error.

Forms that were not clearly and completely processed must be re-checked and entered manually. For that purpose, OCR software should have a built in error detection function and should be able to separate corrupt scans. Even forms that are properly scanned may require significant manual review to verify character interpretations. Most OCR software includes verification tools that allow a human operator to quickly view each character the computer wasn't able to match perfectly and compare it to the original scanned image.

VOTER DATABASE REQUIREMENTS FOR AUDITABILITY

Evaluation of the voter database should aim to review two interconnected aspects of the functional database: (1) database design; and (2) database management. It is not possible to separate these two elements because the database must be designed to address management requirements and some management policies are designed to address database structure. Election authorities should build evaluation and testing into the voter registration plan, and monitors from observation groups and political contestants should be allowed to review and comment upon the plan for such evaluations. Monitors should also be allowed to witness the testing and evaluations, or at a minimum be allowed to review reports presenting results of testing and evaluation. In addition, as discussed below, monitoring by observation groups and political contestants

COUNTRY NOTE:
Indonesia 2004 - Voter Registration Using Optical Character Recognition (OCR) Scanners and NGO Voter Registration Audit

In 2004, Indonesia held its first presidential elections, and second legislative elections, in its democratic transition process. A voter registration exercise was conducted across the country in April and May 2003 in preparation for the elections. The exercise faced the challenge of reaching the country's more than 17 thousand islands and over 150 million voters. Voter registration officers visited households during this period, capturing data on all eligible and ineligible citizens on optical character recognition (OCR) forms. The forms were processed at 45 state statistical bureau offices in all 30 provinces. A total of 92 scanners were used running 23 hours a day, seven days a week. During limited trials the scanners were 93 percent accurate at letter recognition and 97 percent accurate at number recognition. In February 2004, JURDIL Pemilu 2004 (The University and NGO Network to Monitor the 2004 Elections) and one of its member organizations LP3ES (Institute for Social and Economic Research, Education and Information) sent out 400 observers to conduct an audit of the voter registry. The audit used a statistical sample, comprising 5,592 voters from 375 randomly selected villages in 12 of the country's 32 provinces. It found that the registry contained approximately 91 percent of eligible voters, with some variance among provinces (81% - 96%) and a difference between certain marginalized groups (minorities, displaced persons and those in conflict or very isolated areas) versus the general population (86% v. 92%). The audit found a small incidence of persons on the list who did not exist; however, it identified a significant number of errors in dates of birth, which it noted could have resulted form many people not knowing their exact birth date. In part due to the audit, a follow-up voter registration exercise was conducted that increased the number registered voters to over 95 percent (an increase of several million voters).

Source: "Consolidating Democracy: Report on the UNDP technical assistance program for the 2004 Indonesian elections," United Nations Development Program (New York, undated); "Voter Registration Audit Report," JURDIL Pemilu 2004 (10 March 2004).

should extend to being allowed to examine policies and procedures concerning security of the technologies and the voter list itself, and to conduct independent audits of the voter list.

Evaluation should start with a review of the functional requirements that the election authority provided to programmers of the database. If the election authority does not define the functional requirements, it is likely that the programmers will create a database that is efficient in terms of computation and manipulation of data, but probably does not accommodate peculiarities of the electoral process. This potential shortcoming in the election authority's planning would create a circumstance where the technology will impose requirements on voter registration and force the electoral process to accommodate the information technology (IT), rather than vice versa. Definition of the functional requirements is best done upon discussion with observer groups and political contestants, including

review of "peculiarities" in the country's legal framework. Such input can provide important insights, and the participation can build confidence in the process.

In principle, the voter list database should be designed to meet the following requirements:

Primary Voters List Database Data - The proper basis for voter registration and voter data management is the legal framework for the election process. The legal framework will determine the types of data that need to be included in the voters list. These data may go beyond names, date of birth and addresses, if the legal framework requires information beyond such basic voter data. Additional voter information could be required for voters who vote abroad or in the military service or who vote by absentee ballot, or for voters who are excluded because of rulings of mental incompetence or penal reasons. The database must accommodate these provisions.

Secondary Voters List Database Data - The voter database rarely includes only the basic voter information required by the legal framework. In order to administer elections, election authorities need to integrate more data into the database to ensure proper management of voters. These data include information such as assigned polling stations, different coding information and record tracking data. The content and types of secondary data depend on the management policies of the electoral authorities and consequent requirements.

Accountability - Records or information should never be deleted in the database. Instead of deleting records, databases should be designed to have "flags" that will mark that the record as "deleted" or changed. Following the same principle of accountability, changes in the database have to be recorded, with information about who changed the data and who authorized the change. This is called the "*Audit Trail*" - that is, the record of changes in the voter list database.

The "*Audit Trail*" is important for resolving efficiently and accurately disputes that may be raised by prospective voters in the claims and objections period. The database should accommodate timely dispute resolution processes.

Security and Access - Security evaluation of the database should identify sensitive points in the process of adding, updating or deleting records as well as overall safety of the records. This includes the physical security of the premises where the database is housed. In order to address security concerns, election authorities must establish technical solutions and organizational policies that will prevent unauthorized and undetected manipulation of the data. Database design must have defined access levels that are reflected in the database. Responsibilities of operators, supervisors and administrators must be defined and transparent.

Monitors from political contestants and election observation groups should be allowed to review policies regarding the overall safety of the records and should be allowed to review procedures that election authorities established for safe storage of data, back ups, transfers and other related matters. This can be done without compromising the security of the database, and such reviews add significantly to confidence in the voter registration process.

Compatibility - In cases where the voter database is developed by using preexisting records, or it is developed to deliver data in an electronic format to another database (for example electronic poll books), the design has to define carefully how the database will effectively interface with the databases with which it must interact.[29]

Overall Database Structure - Beyond specific requirements of the database for voter list purposes, evaluation of the database should assess the database structure. This includes review of relations between different data and tables, coding and categorization of the data, application of primary keys, definition of fields, and format of tables, records and fields.

Content Testing - Conducting tests of the content of the voter list is a step beyond monitoring the design and functioning of the information technology used in creating the list. These tests examine the electronic voter list (or often a copy of it) to identify errors, such as duplicate records, records with missing data, records that show ineligible persons were entered onto the list or voters assigned to the wrong constituencies. Computer tests can also identify trends in the voter list data that may raise questions about the representativeness

[29] For more on compatibility issues please see "Use of Existing Records - Transfer of Records," above in this Chapter.

of the list, which could indicate that certain population groups are over or under represented (e.g., gender, age, language or ethnic groups or people from certain geographic regions). This could be the result of manipulation of the database, errors in data entry, manipulation in data collection or faults in the registration process. All of these possibilities call for remedies, from removing duplicate records to extending the claims and objections period for list correction to even reopening the registration process.[30]

[30] "Computer Tests" of the voter lists are described in Richard L. Klein, Patrick Merloe, *Building Confidence in the Voter Registration Process: An NDI Monitoring Guide for Political Parties and Civic Groups*, 32-34 (NDI 2001).

CHAPTER FOUR:

Monitoring Electronic Voting Technologies

INTRODUCTION

The introduction of electronic technologies is not a simple replacement of classic ballot boxes and ballot papers with electronic machines. The administration of elections with electronic voting is substantially different from elections with the paper ballot. It requires restructuring of the electoral administration in practically every critical aspect. The introduction of electronic voting creates a whole new set of relations between the election administration (election management bodies), certification bodies, vendors and various state institutions. This new arena in the electoral process presents, for everyone involved, such a large number of complications and risks, which accompany the benefits of new technologies, that the reasons for introducing electronic voting must be clear and compelling.

The decision to introduce electronic voting (e-voting) must be taken carefully, with broad participation and in light of a number of critical factors, if the introduction is to respect the rights and interests of voters and political contestants. Practice has demonstrated that - unless public confidence in the electoral process, particularly concerning the impartiality and effectiveness of election administration, is already high — the introduction of electronic voting is likely to cause suspicions and diminish public confidence.

Practice shows that public confidence in electronic voting has to be built over time, usually through a phased process of introducing the technology that allows voters to use paper ballots if they prefer. A critical issue is the "comfort" of voters in using electronic

technologies, which is as much a question of trust as it is the technical proficiency of voters in using the technology. Public confidence is best built through transparency concerning the technology—both toward the public and the political contestants—and through widespread civic education about the technology.

Public policy debate about reasons for the introduction of technology should be timely and broad. It should include representatives of election authorities, parties and candidates, observation groups and other civil society organizations concerned with political rights, as well as technology experts who can provide valuable input in the early stages of the debate. Because of difficulties with the observation of the electronic voting, it is likely that society will be skeptical toward e-voting systems in any country and particularly where there is not an established record of holding elections in accordance with minimum international standards.[31] Should the decision to introduce e-voting be hasty and not based on clearly compelling, legitimate needs, the consequences will likely be a deterioration of trust in the credibility of the electoral process.

EVALUATING THE RATIONALE FOR INTRODUCING ELECTRONIC VOTING

When evaluating the rationale for potentially introducing electronic voting technology, monitors from political contestants and civic organizations should examine the reasoning and claims provided by advocates of the specific electronic technology, for example, optical scanning or DRE voting systems. Some of the most common considerations are listed below.

Cost:

To understand whether the cost-benefit analysis is done properly, monitors must realize that calculating the price per unit of the voting equipment is not an adequate way to determine the costs of introducing electronic voting systems. Analysis must include the following costs beyond the price of equipment.

[31] See, for example, Organization for Security & Cooperation in Europe Office for Democratic Institutions and Human Rights, *Existing Commitments for Democratic Elections in OSCE Participating States* (October 2003), available at http://www.osce.org/publications/odihr/2003/10/12345_127_en.pdf; Southern African Development Community, *Norms and Standards for Elections in the SADC Region* (March 25, 2001), available at http://www.sadcpf.org/documents/SADCPF_ElectionNormsStandards.pdf; Council of Europe, Venice Commission, *Code of Good Practice in Electoral Matters* (October 30, 2002), available at http://www.venice.coe.int/docs/2002/CDL-AD(2002)023-e.pdf; Guy Goodwin-Gill *Democratic Elections under International Law, IPU* (Geneva 1994).

Development of Requirements. If the equipment is not "off the shelf" (that is, ready-made and available for sale), election authorities will have to engage contracted experts to develop equipment specifications and requirements. It should be noted that there is often a need to develop specifications to meet the particular circumstances of a country's elections, usually defined in the legal framework.

Development of Hardware and Software. In the case of the development of new equipment, delays and modifications may occur because intermediate tests show non-compliance with requirements. Delays may increase costs of the technology and also can necessitate actions in other areas of election administration that produce additional costs.

Distribution and Deployment of Equipment. Logistics behind the deployment of equipment are more sensitive than the distribution of ballot boxes. It requires additional security measures and additional care so that the equipment is not damaged. This also may produce additional costs. The equipment distribution scheme will probably require that polling stations receive the equipment farther in advance of election day than would be the case with paper voting. Polling officials may therefore need to be on payroll longer, and extra steps and personnel could also be needed to ensure that the polling stations are properly secured.

Infrastructure of the Polling Station and Counting Centers. Electronic equipment needs adequate infrastructure with a reliable power source. Outdoor polling stations, for example, may not be adequate. Some electronic voting equipment is designed to run on batteries, and extra batteries may be needed as well as recharging facilities.

Infrastructure for the Data Transmission. Equipment that transmits data over modems or computer networks requires installed telephone lines and reliable access to public networks.

Storage of the Equipment. Electronic equipment requires special storage facilities with a controlled climate and a high level of security.

Service, Maintenance, Replacement. Hardware does occasionally malfunction or break down. The cost-benefit analysis

should include projections of replacement costs, as well as costs of regular services and maintenance of the equipment. The lifespan of the electronic equipment is not indefinite and will depend upon the type of the equipment. Analyses should provide realistic projections of equipment lifespan. Election authorities usually keep a "strategic stock" of equipment in order to replace the equipment that malfunctions. The lifespan of software is also an important consideration, particularly in light of the rapid evolution of Information Technology.

Customization and Reprogramming. In many cases, equipment will have to be customized for use in different electoral units within a country, for example, if they have different list of candidates or elections for more than one office. For every election cycle, equipment will need to be programmed to comply with the requirements of the electoral process. Costs are incurred at each of these steps.

Certification. The certification process for electronic equipment and software is an additional cost, because it should be performed by an independent organization and not by the vendor or election authority.

Structuring of EMB. In order to properly operate electronic voting equipment, election officials' training will have to include how to ensure that the equipment functions properly. Trainings will likely have to be outsourced and performed by the vendor or, at a minimum, with vendor participation at certain levels. This could produce additional expenses at the first election using the technology and/or later elections. In addition, the election management body will have to establish an office of specialized IT personnel and take effective steps for their professional development and retention. It is vital to build capacities of electoral authorities in order to avoid over-reliance on vendors.

Voter Education. The cost of mounting widespread and effective voter education programs addressing the introduction and uses of electronic technologies must be taken into account.

Usability:

Usability issues are two-fold, and they relate both to the voters and election officials. The threshold questions for monitors from observer

groups and political contestants to ask are: Did authorities run usability tests with voting equipment models and a variety of types of voters, and what were the results? The following questions are among those that need to be asked and answered through usability testing.

Given the demographics of the voting population and frequency of using electronic equipment versus marking paper records, would it be easier for the vast majority of voters to use electronic voting technology or to mark a paper ballot? If the ballot is long and/or complicated (for example, because of preferential voting and/or the number of races), is it easier to understand and mark a paper or an electronic ballot? How will disabled voters benefit from the introduction of electronic equipment, and are there alternative and practicable ways to gain those benefits by modifying paper ballot procedures? Will the "electronic ballot" facilitate voting in multiple languages versus having paper ballots available in those languages?

Paper ballot elections produce certain levels of errors in voting and counting; for example, voters may make mistakes when marking the ballots. The more complex the ballots, the more mistakes are made. Is the historic error rate in balloting in a particular country significant enough to require reform of the voting methodology? If so, how would switching to e-voting be better than other possible reforms? Before answering that question, it must be noted that there is a principal difference between the responsibility of the voter to properly mark the ballot - which can be addressed through proper ballot design and adequate voter education - and the responsibility of the electoral authorities to accurately record the voters' choices. The choice of electronic voting as a methodology should affirmatively address both elements in a manner that outweighs the effectiveness of paper balloting and proves to be cost effective over a sustainable period.[32]

Fraud Prevention:

Often electronic voting is cited as an anti-fraud measure. This, however, is not a simple matter. Introduction of any new technology may eliminate some opportunities for fraud, but every technology, including electronic technologies, also opens possibilities for fraud.

[32] This calculation could differ between electronic voting that employs scanning technologies versus DRE technologies.

As with other factors, this element must receive careful evaluation. If the introduction of electronic equipment aims to eliminate fraud, authorities need to address security issues and explain to the public and monitors from observation groups and political competitors how the equipment and the electronic records will be protected from tampering.

For example, e-voting on direct recording electronic systems (DREs) eliminates marking a paper ballot (as compared to OMR systems that read paper ballots with predetermined types of marks). DRE technology would eliminate two relatively common forms of fraud known as ballot box stuffing and carrousel voting.[33] At the same time, DREs open the possibility for rigging the equipment's software to register votes differently than they were cast, and they create possibilities for switching data memory cards or corrupting data transmission.

Assuming that equipment is adequately protected from unauthorized access at the polling stations, manipulating votes becomes more complicated when DREs or OMRs are utilized. Manipulating such technologies requires that perpetrators exercise technical expertise. However, corrupting the software (or firmware) is possible in many phases of the development and operation of the equipment.

Count and Tabulation Facilitation:

There is no doubt that the counting of votes registered on electronic equipment is substantially faster and should be subject to fewer errors than manual counts. This applies especially to counting and tabulation of votes in preferential election systems. However, speed of the count is not a fundamental requirement for elections to be democratic and honest.

Before determining that speeding up counting and tabulation processes is a sufficient goal for moving to electronic technologies, advantages and disadvantages of the slower paper ballot process and slower count must be considered. For example, it is important to ask whether the speed of the count and tabulation has caused

[33] In carrousel voting, a ballot paper is smuggled out of the polling station; it is then pre-marked by a criminal conspirator, who gives it to a voter to smuggle into the polling station and place illegally in a ballot box. Then the voter smuggles out the blank ballot given to him or her by officials - and turns that blank ballot over to the conspirator for marking. Often, the voter is then paid a bribe. Ballot box stuffing could be approximated with DREs, if someone illegally entered multiple votes on the machines by using the DRE touch screen or with OMRs by scanning extra ballots.

tensions or significant problems in prior elections. If so, then it is important to consider how much faster the count would be and the influence this would likely have on confidence in the elections should electronic technologies be employed. (For example, would it make a difference of hours or days, and what would be the likely impact of the difference?)

It is also important to consider whether there are other ways to streamline the counting procedures when using paper ballots, such as simplifying tally sheets (sometimes referred to as protocols, *actas* or *procès verbaux*). Even more important perhaps is the need to consider whether electronic technologies would eliminate confidence building safeguards, such as providing copies of tally sheets to poll watchers and observers, as well as eliminating vote verification activities, like parallel vote tabulations (PVTs).[34]

Public confidence in the vote count and tabulation of results is perhaps the most sensitive element of the election process. Frequency and severity of past problems concerning accuracy of the count and tabulation should be considered in light of possible benefits of electronic counting and tabulation technologies before any decision is made to employ such technologies. Transparency and access of monitors from observer groups and political contestants to testing of the electronic technologies and operating safeguards is critical. Testing in the form of simulations, real time evaluations of tabulations and post-results verifications should be conducted and be transparent.

One of the most important transparency features is for electoral authorities to make data available publicly and immediately on a disaggregated (polling station by polling station) basis, concerning turnout and voting results, as well as on an aggregated basis for the election. This allows observer groups and political contestants to compare election administration data with election day/night information collected by their voting, counting and tabulation monitors (poll watchers and observers).

[34] Parallel vote tabulations are conducted by political parties and nonpartisan observers, usually based on a statistical sample, in order to evaluate the quality of voting and counting procedures and to project election results. PVTs play a critical role in building confidence and acceptance of election results in credible elections. This has a higher impact than post-election verifications.

LEGAL FRAMEWORK

One of the challenges of enacting sound election laws is determining how detailed the legislation should be and how much latitude should be given to election authorities to address matters through issuance of by-laws (regulations) and directives. There must be an appropriate balance between setting forth clear principles in the law, on the one hand, and, on the other hand, addressing the need of election authorities to make decisions about administering the election process in a practicable manner.

General principles for legislative drafting require that the election law anticipate all major issues in the election process and be specific about them (for example, it is not enough to say legislative seats are to be awarded according to proportional representation, the particular formula to be used for calculating the number of seats won must be specified). Use of electronic technologies, particularly concerning electronic voting and other sensitive election processes, therefore should be addressed in the law itself and not left to the discretion of electoral authorities. This is because the voting and tabulation (and other processes relating to the exercise of the electoral franchise) directly affect a fundamental right of citizens. The law also should be quite specific in requiring transparency mechanisms, including monitoring by political contestants and observer groups, for all elements of the election process.

The process of developing the legal framework should be inclusive of citizens and political contestants (including extra-parliamentary parties participating in elections) through open debate, use of hearings, public comment mechanisms, constituent outreach and other techniques for informing the public and gaining input.

The introduction of electronic voting technologies adds additional challenges to developing a proper election law and wider legal framework. Among the challenges are providing definitions and safeguards for universal and equal suffrage, secret and free voting, plus transparency, accountability and security concerning technologies that keep changing - and where "the devil is in the details" (very specific technical details in the design of the equipment that can change in relation to required principles).

The law itself, at a minimum, should specify whether electronic technologies may be employed in specific election processes (e.g., delimitation of election districts, voter registration, voting, counting and tabulation). If the law allows the application of electronic technologies, it should specify the goals for the application, the general types of technologies that would be permissible, transparency mechanisms (including access for monitors from observer groups and political contestants), accountability mechanisms (legislative oversight bodies, use of independent audits of the integrity and efficiency of the technologies, role of national technology standards bodies) and safeguards/security mechanisms (requirements for pre-testing, testing while electronic technologies are in use and post-use testing). As with every activity that affects a fundamental right, such as the electoral franchise, the law must include mechanisms that can provide effective remedies if the rights are abridged through application of electronic technologies.

It is likely that the election law will not be the only source of regulation for electronic voting. Other laws must be reviewed in the process of preparing the election law. Legislation that deals with information technology is also vital; these include regulation for digital certification authorities, digital signatures, IT communication and protocols standards, protection of data, data retention and other technical matters. Another area of critical importance is the country's laws regulating the issuance of government contracts, which will be a critical part of acquiring and maintaining electronic technologies. Transparency in this area is usually a special concern. The country's administrative code and criminal code should also be reviewed. In each case the review should ensure that there are not inconsistencies or conflicts of law between the election law and other relevant codes.

The election law also must provide the parameters within which election authorities may issue regulations (bylaws) and other guidance concerning the application of electronic technologies.

Evaluation of the legal framework should give answers to how the laws and regulations address the following issues:

Universal and Equal Suffrage, and Free and Secret Voting. How do basic election principles relate to changes in voting methodology? While these principles seem obvious and easy to

implement, technical details of the voting system might corrupt them; for example - if the e-voting equipment records the time when a specific vote has been cast, this can corrupt secrecy of voting. The same concern relates to the paper record that is printed on continuous tape.

Transparency. An electoral process that involves e-voting equipment presents a new set of issues concerning transparency in the process. While democratic standards for transparent elections mandate access of monitors from political contestants and observer groups to all elements of the electoral process, in practice this might challenge other important interests, such as security of the technologies and appropriate protection of intellectual property. In order to effectively administer elections, electoral administration may set some reasonable access limitations (for example, concerning the activities of poll watchers and observers in polling stations), but such limitations should be imposed only to ensure an unobstructed election process. Therefore, administration cannot limit access as a principle; according to international standards and best practice in national law, restrictions may not be "unreasonable."[35] For example, it would be reasonable if election authorities prevent monitors at the polling station from arbitrarily inspecting e-voting equipment software on election day (which would disrupt the voting process), but election authorities should not deny access to the e-voting equipment and software in principle and should cooperate with monitors from observer groups and political contestants to provide them access in a manner that will not obstruct the process.

Security. Security of the e-voting system will depend greatly on specific technical details. However, not all of the security aspects can be solved with technical solutions; organizational solutions will also be needed. In order to address transparency and accountability requirements, the legal framework therefore should emphasize security and protection of electronic records and should recognize that security relies on organizational solutions (the "four-eyes principle"), not on secrecy (the "security through obscurity principle").

For components of the system where security is delivered through cryptography, it is important to emphasize that cryptography

[35] See, for example, Article 25 of the *International Covenant on Civil and Political Rights* (reproduced in the Appendix 3 of this Guide).

applications should pass the "test of time" and that encrypted information should stay secure indefinitely. Cryptography specialists must be consulted by political contestants and observer groups in order to properly evaluate these issues.

Certification. Legal provisions that deal with the certification process should define fundamental issues related to that process. This includes definition of the certification process, institutions that are qualified to certify production processes and products, as well as access to certification procedures and certification reports by monitors from political contestants and observer groups.

Contractual Obligations and Intellectual Property. The legal framework should take into account that producers of e-voting equipment will claim intellectual property privileges to protect their hardware and/or software. The legal framework must balance transparency requirements necessary to protect and comply with fundamental rights of citizens, including electoral competitors and observer groups, and proprietary rights of commercial institutions. Solutions must be developed that will not unreasonably limit access to the software and hardware components. This can be done, for example by: defining e-voting software as part of the public domain, which would make it available based on the overriding public interest in electoral integrity; or requiring that information about certain proprietary elements of the technology not be disclosed, while allowing access/verification of the technology's integrity and making public findings and recommendations in this respect, and prohibiting reviewers of software from benefiting financially from knowledge they gain of the software.

Because of the technical nature of the equipment, election authorities usually do not have the capacities to produce e-voting systems. Outsourcing production of the e-voting equipment is a sensitive process. Poor performance of producers can substantially endanger the electoral process. Outsourcing also can instill dependency of election authorities on contracted producers.

For these reasons, it is important that legislation requires electoral authorities to maintain their legal obligation to the citizens to organize a credible democratic election process, and therefore they must only enter contractual relationships with producers, suppliers

and/or servicers of electronic technologies that ensure effective performance and give election authorities effective remedies where performance is in doubt. For example, legislation should state that contracts can only be entered with companies that have a demonstrated basis for reliable performance, such as rigorous testing of their equipment and/or use in elections, and that the producer must have enough units of equipment readily available to fulfill any contractual order on the dates specified for delivery in the contract or have a proven production record and no conflicting contracts so as to ensure timely delivery of equipment.

Challenges, Recounts and Audits. In order to provide a sound methodological basis for demonstrating the accuracy of e-voting, counting and tabulation and to eliminate the possibility for arbitrary decisions of election authorities concerning electoral outcomes, the legal framework should require mandatory audits of e-voting technologies. Such audits should be required whether or not there are legal challenges to election results. The audits, for example, would examine a statistical sample of e-voting equipment (such as DREs and OMRs) to determine whether the results recorded in the official tabulation were an accurate record of the votes registered on the specific piece of equipment (including review of the electronic recording of votes and the machine's paper trail).

Allowing for challenges to result from specific e-voting equipment or specific polling stations must be provided among the remedies in the election law. Such challenges, for example, could seek to exclude results from specific e-voting equipment or specific polling stations because of malfunctions, which might require holding new elections. Legal requests for recounts must also be addressed in the election law. This remedy relates to the necessity of maintaining a paper trail (or other effective auditable record), and to the paper record being the legal expression of the voter's choice.

DEVELOPMENT OF REQUIREMENTS

Development of e-voting systems is a process that has several stages. They should all be public and transparent. The process will be fundamentally different depending on whether election authorities choose to purchase "off the shelf" products or to pursue development of a custom built voting system or a system that

combines custom developed equipment with ready made products. Before that decision, election authorities should define general requirements of the electronic system, without proposing particular technical specifications. These general requirements should address secrecy, transparency, accountability, usability and security.

The second stage is to review options that address general requirements. In this stage, electoral authorities usually invite producers to present their ready made e-voting systems and prototypes and explain how these systems respond to the general requirements. Such presentations must be detailed, and concrete technical applications must be presented. This stage provides an opportunity to initiate usability tests and research how voters and polling officials would use the system and, thus, identify difficulties that appear concerning usability of the prototype systems.

In the third stage, election authorities will either decide to purchase "off the shelf" products or decide that none of the available products adequately matches their general requirements. In this case, the authorities will move to the next stage: development of the specific technical requirements for design and production of the electronic voting system. This stage will require involvement of experts who can produce technical requirements. The work of these experts should also be available to the public. Furthermore, their affiliation with any interested entities should be disclosed, because they must act based on their expertise and not affiliations with vendors and producers of the e-voting systems, which create conflicts of interest.

CERTIFICATION AND TESTING

Certification:

Certification is a process performed by an independent certification authority and serves the purpose of determining whether the equipment matches technical requirements developed by election authorities. It is important to understand that certification has limits and that certification of the equipment is not a guarantee that the systems will perform flawlessly. Evaluation of the certification process should consider the following issues.

Certification Body. The certification body should be an independent organization with sufficient technical expertise to

perform such certifications. This body should act as neutral reviewer of how the developer produced equipment based on technical requirements specified by the election authorities. Because of that, the certification body should not have any interest vested in whether the product complies with the requirements. Election authorities, as well as monitors from political competitors and observer groups, should therefore look into the independence, qualifications and potential conflicts of interests of the certification body. It is important to understand why a specific certification body is selected and if the selection of the certification body complies with the legal framework.

Certification and Requirements. If the technical specifications and requirements are poorly written and not specific, the certification will likely fail to contribute to the quality of the product, because the certification body will limit its examination of the equipment to the requirements. Monitors should carefully review how the certification matches the requirements.

In addition to certifying the product, certification could also examine the product's development and consider how the management of the equipment production relates to the technical requirements. (For example, it should consider access to security sensitive aspects of the development process.)

Post-Certification Development Process. Certification of the equipment is usually performed on prototypes. It is possible that the equipment will have to be additionally customized, for example programming of the ballots and user interfaces, installment of the access codes, calibration of the equipment and updates of the software. Monitors should understand how these processes relate to the certification and how much the equipment's hardware and software will likely change after certification.

Transparency of the Certification Process. The certification process is a part of the electoral process. The work of certification bodies should be transparent. This means that all of the certification procedures must be documented, and these documents should be available to monitors from observation groups and political contestants. Monitors need to understand what specific procedures, test and reviews were conducted and the findings of the certification process.

Testing:

The certification process does not eliminate the need for testing of equipment. Testing will depend on the specifics of the e-voting system, but all of the tests should be planned and documented. This includes development of test scenarios - detailed descriptions of what and how specific aspects and components of the e-voting system are tested. Analyses of the test scenarios will reveal to monitors if the test are designed properly.

While it is not the monitors' role to test the equipment, they should be able to observe the testing process. They should also have access to the results of testing.

Tests can also be done at the beginning of the development of the e-voting system, in order to decide upon the most appropriate system. There are different kinds of tests, including, among others, the following.

Usability Testing. Usability tests aim to determine if voters and polling officials can properly operate the equipment.

End-to-End Testing. End-to-end tests are actual simulations of the complete process. In this test, all of the components of the e-voting systems are tested as if it is election day.

Load Testing. Load or volume tests are those where the systems are run with the level of expected usage on election day. This demonstrates the differences where equipment may perform well when tested with 10 voters, but it could malfunction if tested with 500 or more voters.

Security Testing - Threats and Attacks. Security tests aim to expose potential vulnerabilities of the voting systems from threats that come from outside the election authorities and from inside election authorities. Proper security tests will include "penetration tests" (or "Red Team" tests) - which are simulations of malicious attacks on the system.

Parallel Testing. Parallel testing is a test that is conducted on voting day (sometimes known as "hot audits"). Actual voting equipment is

excluded from the voting process, isolated and monitored. Testers that register test votes on the equipment do not do so in secrecy, so that their choice can be manually counted and compared with the result of electronic "test vote."

Pilot Testing. Pilot tests are usually conducted in the early stages of the development of the electronic voting systems. They are end-to-end tests with real voters who are given the opportunity to vote with either paper ballots or e-voting equipment.

PRODUCTION, DELIVERY AND MAINTENANCE

Development and production of the e-voting equipment is a highly technical process that requires a substantial expertise and technical capacity. Even in paper based systems, election authorities usually outsource printing of ballots, production of ballot boxes, indelible ink and other materials used at the polling stations. Production of all of the sensitive election materials (such as ballots and e-voting equipment) should be closely supervised by the election authorities in order to insure the integrity of the materials. The processes should be transparent and provide for observation by monitors from observer groups and political contestants.

Production of e-voting equipment also requires attention from the election authorities, since e-voting equipment is highly sensitive. Monitors should also have the opportunity to evaluate the process. However, there are cases where producers of the equipment limit access to the production process or components of the product in order to protect their proprietary rights and "trade secrets." As discussed above, the balance of interests of protection of the fundamental rights of citizens and political contestants in holding genuine democratic elections generally should outweigh property rights, although some reasonable restrictions can be provided by election authorities in consideration of proprietary interests of providers of electoral technologies. The following are examples of some questions and issues that monitors should consider in this area.

Decision to Utilize Electronic Voting. As stated above, the decision to utilize electronic voting directly affects fundamental rights of citizens and electoral contestants, and the decision therefore

should be taken only after open public discussion that honors citizens' rights to participate in governmental and public affairs. Political contestants and nonpartisan election observer groups should have complete access to the process leading to the decision, and the process should allow for public input.

Selection of Producers/Suppliers. Monitors should be able to review procedures for selection of producers of the e-voting systems in advance of any selection. Laws and regulations concerning tenders for government contracts may apply and may deem such contracting procedures as public information. Monitors should be able to know how the producer was selected. They should be able to learn whether background checks of the producer's capacity and credibility were conducted and whether there are relationships between producers and election interlocutors that require review of conflicts of interests.

Production and Delivery Timeline. Monitors should have an opportunity to review and comment on whether the timelines in the proposed contract are realistic (for example, whether they allow enough time for tests, additional development and updates). They also should be able to review and comment on the contractual obligations of the producers if timelines are not respected.

Support and Maintenance of the System. The proposed contract should reveal the producer's obligations to service and maintain the system, what resources are assigned to troubleshoot before and on election day and how such support will be billed. It also should state explicitly the producer's obligations in cases where there are large scale failures, including their role in contingency planning.

Training. The proposed contract also should reveal the types of trainings that will be provided by the producers, the level of technical expertise to be transferred to election authorities and whether the production of manuals and trainings will be an additional expense.

Subcontracting. The proposed contract should specify whether the selected producer is allowed to outsource production of certain components or certain services, and should provide transparency for any outsourcing. It also should specify clearly the relationship of the subcontractor to the producer and electoral authorities, accountability mechanisms that apply to the subcontractor, including

remedies if the duties of the subcontractor are not performed on time and effectively, and include redress that the election authorities might seek.

Contractual Obligations and Other Issues. The proposed contract should specify how easy or difficult it would be to scale up or upgrade the system, how additional programming and customizing is to be regulated, who owns the product (material and intellectual), what level of detail must be submitted in technical documentation, what the warranty clauses must be and how liability is regulated.

HUMAN RESOURCES AND TRAININGS

By some estimates, the single greatest threat to an election is a human error on the part of the poll workers. Whether these estimates are accurate or not, poorly trained poll workers and bad management of the polling stations can lead to the complete breakdown of the voting process. Observation groups and political contestants therefore should be allowed to review plans for staffing polling stations, including required qualifications for recruitment of the polling staff, trainings and contracted services.

Trainings. Trainings of polling officials, including training materials and poll day guidebooks (manuals) should be available for evaluation by observation groups and political contestants. Monitors should evaluate the quality of trainings and polling day manuals. Monitors should also use these materials to learn about polling day procedures, which can help them to design their polling day observation strategy.

Staffing. Besides adequate trainings, election authorities must develop appropriate staffing and recruitment plans for voting operations. This does not only relate to polling officials, but also for middle level and high level administration officials. Election authorities must continuously build and develop internal capacity to administer elections with electronic voting equipment. Without proper staff infrastructure, election processes will be left in the hands of contracted private organizations. Monitors from observation groups and political contestants therefore should be able to review and comment upon staffing plans and steps to implement them,

including required qualifications for hiring applicants to be election administration staff at various levels.

Contracted Services. It is not unusual that election authorities outsource some phases of the election process to private organizations. However, monitors from observation groups and political contestants must understand the permissible level and types of outsourcing and how that influences the security of the elections. Complete outsourcing of the services relating to electronic technologies to private organizations raises many issues, and that level of outsourcing can damage the credibility of the election process because the public and the political contestants may feel that election authorities are not adequately controlling critical elements of the process and ensuring electoral integrity.

Beyond the level of involvement of private contractors, monitors should evaluate whether the responsibilities of the contractor (as defined in contract) adequately match the need for their services, especially on polling day and through the tabulation of results. The most simple and obvious example is troubleshooting malfunctions of the equipment on polling day. Some examples of questions that monitors should ask are: Does the contractor have the capacity to provide the services? Are there enough technicians assigned for each cluster of polling stations? What is the responsibility of the equipment producers in trainings and providing training materials?

TRANSPARENCY

Transparency throughout the election process is one of the basic requirements for democratic elections, as noted in Chapter 1 of this Guide. In elections with paper ballots, monitors and election authorities have knowledge of what constitutes a transparent election and which stages of the electoral process may require certain reasonable limits on transparency.

How the principle of transparency applies to elections with electronic voting depends greatly on the type of e-voting systems that are used. Stages of the voting, counting and tabulation processes are in fact different depending on the type or types of equipment used. For that reason, it is not practical to attempt to provide step by step guidelines and benchmarks for each type of technology in a guide of this type.

Moreover, as the technologies rapidly evolve, such detailed "checklists" would be immediately outmoded. Beyond the general principles presented for consideration, expert guidance would be needed as e-voting technologies are being considered (before decisions are made) and as soon as any specific technology is chosen.

COUNTRY NOTE:
Belgium 2006 - Reviewing E-Voting Systems

Since 1999, approximately 44 per cent of Belgium's electorate has electronically recorded their electoral choices. The Ministry of Interior certifies the electronic voting system before each election is conducted, based on tests carried out and audit reports provided by companies that are selected by the technology vendors from a list approved by the Ministry. Also, software used in the e-voting system is provided to an independent College of Experts, which is appointed by the Chambers of Parliament. Members of the College of Experts may request any information from the vendors and authorities concerned with the elections and may examine the source codes used in the e-voting systems. They also may visit polling stations, copy software in use on election day and conduct other activities. The College must report its findings to Parliament within 15 days following elections. In addition, each political party or formation that has at least two Members of Parliament may designate an IT expert to receive the source codes of the e-voting systems and examine them, while such experts must keep the source codes confidential. Some political parties and civil society organizations have demanded, among other things, a voter verified paper audit trail (VVPAT), access to certification reports, strengthening of the College of Expert's role and a comprehensive vulnerability study of the system, and observers also have called for avoiding excessive reliance on vendors for running the system.

Sources: "Belgium: Federal Elections 10 June 2007, OSCE/ODIHR Election Assessment Report" (19 October 2007); "OSCE Office for Democratic Institutions and Human Rights Expert Visit on New Voting Technologies, 8 October 2006 Local Elections Kingdom of Belgium."

Another reason why it is impractical to create a specific "checklist" of indicators by which transparency would be measured is the lack of specific internationally recognized standards for voting with electronic systems. Issues like disclosure of the equipment's software codes and providing an auditable paper trail are still being debated, although a consensus is emerging concerning the need for independent verification of the integrity of electronic electoral technologies and that there must be a paper trail for e-voting applications.

Even though internationally recognized technology standards are not settled, the right to access to information about essential elements of an election process is a component of internationally recognized

rights to seek information, to participate in governmental and public affairs and to have genuine democratic elections. Election observation groups and political contestants therefore have a clear basis to seek transparency in electronic electoral technologies; the challenge is determining how to properly and effectively exercise those rights.[36]

Experience in monitoring electronic voting is demonstrating that two central challenges to address are: how monitors can gain sufficient access to evaluate electronic technologies at various stages of the process, without disrupting the process; and how to do so with proper consideration of other interests.

If sufficient access is not provided, or if the monitors do not have the required expertise needed to evaluate certain technologies, it is the monitor's responsibility to state which stages of the process were not properly observed. Monitors must address honestly the question of whether the observation can be effective if the most critical stages in the process cannot be properly observed. The following are among issues that should be considered in this respect.

Software Source Codes. Producers of the e-voting equipment (especially in cases where the equipment is not developed on demand from election authorities and is "off the shelf" equipment) often seek to protect their investment by not disclosing their software source codes. Claims of proprietary rights as well as security requirements are the most common reasons given for nondisclosure of source codes. These concerns can be addressed by providing protection of the intellectual property through other means, such as confidentiality agreements regarding certain proprietary elements - though such agreements should allow public disclosure of general analysis, conclusions and recommendations concerning the effectiveness and integrity of the technology. In the alternative, election authorities may require that the source codes be placed in the public domain.[37] Demands for security can be addressed, as discussed above, with the election authority's requirement that the security of the system be provided through openness, rather than by secrecy of the software (the "security through obscurity" approach).

[36] Please see Chapter 1 for further discussion of these points.

[37] There is a longstanding debate in the computer industry concerning an "open source" approach to software codes (where source codes are publicly available and can be used and modified) versus protecting proprietary interests in software. Irrespective of that debate, there is a clear and compelling public interest in having electronic electoral technologies be publicly inspected, and that can be accommodated through a variety of means noted in the sections above.

Even if the source code is made available to monitors for verification, critical challenges exist. Experience has shown that the complexity of the software may prevent monitors from verifying that the software will perform its tasks. It is practically impossible to positively verify that the software does not contain code lines that, for example, manipulate the vote or corrupt the secrecy of voting. Many ideas have been offered about how to make software more transparent and secure (including limiting the size of the "trusted computing base" and making software less complex), but none of them so far has provided practical solutions.

This does not mean that the software codes should not be transparent and available for verification by monitors; it means that the objectives of a software review are somewhat different from verification of software performance. Review of the software codes will probably tell monitors something about obvious potential problems and inappropriate use of various technologies and shortcomings in security solutions.

In summary, observation of the electronic voting systems should not focus naively on the software source codes, but the review of the software is still useful.

Paper Record. Different types of electronic voting equipment were discussed above - DRE, OMR, OCR and punch card devices. These technologies can be categorized as either electronic voting or electronic counting devices, depending on which type of record is created first - paper or electronic.[38] In the case of scanning devices, a voter first creates a paper record of his or her vote, and then the machine "reads" (counts) the paper record. In the case of DREs, a voter first creates an electronic record of her or his vote, and whether the electronic device will produce a paper record depends on the design of the equipment.

Surprisingly, the requirement for the paper record is still a matter of some debate. Advocates against paper record argue that:

- The paper record is an inefficient method for verification of the vote.

[38] Except in the case of a Digital Pen, when both records are created simultaneously.

- Introduction of the paper record unnecessarily complicates the voting operation.

- The paper record duplicates the paper ballot voting system, which dissipates the advantages of electronic voting.

- The process of creating paper records introduces a greatly enhanced risk of system failures on election day, since printers are typically the least reliable aspects of most computing systems.

- Virtually all countries that have successfully deployed electronic voting have done so at least initially without paper record.[39]

The requirement that the electoral process must be transparent and verifiable means an easily auditable record of the voters' choices is required; therefore the lack of proper paper record is unacceptable. The issue of what constitutes a "proper" paper record is a matter of discussion. As noted above, many proponents of paper records argue that the paper record constitutes the legal representation of the voter's choice, as long as the voter has the opportunity or requirement to review the paper record before registering the vote. A system that would provide this approach is sometimes referred to as a Voter Verified Paper Audit Trail (VVPAT). A VVPAT system must include the following design elements:[40]

- The system should maximize the probability that voters will actually verify their votes.

- The order of votes in the paper audit trail should be randomized to protect voter privacy.

- There should be procedures in place for when a voter claims that the paper record does not match the way he or she voted.

[39] See, for example, the First Report of the Irish Commission on Electronic Voting (December 2004), available at http://www.cev.ie/htm/report/first_report.htm; see also, Second Report of the Irish Commission on Electronic Voting (July 2006), available at http://www.cev.ie/htm/report/download_second.htm.

[40] See Aviel D. Rubin, Testimony, U.S. Election Assistance Commission (June 30, 2005), available at http://avirubin.com/vote/eac2.pdf.

- Ballots should contain no information that is not "human readable" (for example, barcodes).

- The system, including the verification step, must be accessible to voters that face some physical challenge, such as blind voters and deaf voters.

COUNTRY NOTE:
United States - Voter Verified Paper Audit Trail (VVPAT)

Following the establishment of the Help America Vote Act (HAVA) in 2002, the use of Direct Recording Electronic systems (DREs) increased rapidly across the United States. The 2004 general elections and the 2006 mid-term elections witnessed the hurried and often abrupt introduction of electronic voting equipment. In both elections, poor training and technical problems with voting equipment forced many stations to revert to paper ballots. In addition, irregularities reported in some circumstances led to concerns about possible electoral manipulation, though fraudulent practices were not substantiated. Many states utilizing DREs had no voter verified paper audit trail (VVPAT) requirements, and therefore many irregularities that arose could not be reconciled. Despite the initial goal to quell voter distrust lingering from the 2000 elections, DREs without VVPATs seemed to diminish many voters' confidence in the process. Following these developments, many U.S. states passed legislation requiring VVPATs with DREs, while others amended their voting systems entirely. As of 2007, the majority of states (38 of 50, or 76%) either use or will use VVPATs with DREs, or have opted for other forms of voting (mostly paper-based ballots counted by optical scanning equipment, using Optical Mark Recognition (OMR) equipment, or paper ballots with technologies made available that allow blind and other physically challenged voters to cast ballots without assistance of another person). As a consequence of the 2004 and 2006 problems, election reform legislation on the national and state levels is being further considered. These reforms, if enacted, could lead to, among other things, greater standardization and increased transparency in any electronic equipment used in U.S. elections.

Source: "United States of America Mid-Term Elections 7 November 2006 OSCE/ODIHR Election Assessment Report," (9 March 2007); "VVPAT, Paper Record Laws and Regulations," Election Online.org, http://www.electionline.org/Default.aspx/?tabid=290

SECURITY

Analyses of the security of the electronic voting systems should be a central part of the monitoring process, and monitors from observer groups and political contestants should evaluate the effectiveness and vulnerabilities of the mechanisms that have been put in place to guarantee security and integrity of the electronic votes.

Perhaps more than any other aspect of electronic voting technology, the security aspect is where the "devil is - truly - in the details." Even

minor changes in security policies, access limits and the type of environment can lead to serious security breaches. Proper security analyses will require engagement of an IT security expert, who understands implications and limits of usage of technical security applications.

COUNTRY NOTE:
Netherlands 2007 - E-Voting Suspended in Part Due to Civil Society Efforts

In October 2007, the Netherlands decertified electronic voting machines used in the vast majority of its polling stations and moved, at least temporarily, to voting systems that will employ a form of paper ballot, such as traditional ballots marked with red pencil or perhaps a form of electronic counting of ballots. The decision was made by the Ministry of Interior and Kingdom Relations following a report by a special advisory commission led by Minister of State F. Korthals Altes. The advisory commission was formed in part due to the efforts of civil society monitors. The Korthals Altes Commission report entitled "Voting with Confidence" was released on September 27, 2007, and found that: on the grounds of transparency and verifiability, paper balloting is preferable over electronic voting without a paper trail, though a method of electronic voting that meets required safeguards is conceivable, if it produces a ballot that can be checked by the voter. The report also noted that the present Dutch electronic voting regime does not properly regulate development of requirements for equipment used in voting, enforcement of those requirements or the security and management of the equipment. It found that transparency and verifiability of the election process need to be improved and called for subjecting the preparations for, and conduct of, every election to an audit by independent experts. On October 1, 2007, the District Court of Alkmaar decertified the Dutch-made voting machine due to security flaws. The decision was the result of a March 2007 administrative law procedure brought by the Dutch citizen organization "We do not trust voting computers" (Wijvertrouwenstem-computersniet), which demonstrated through controlled "hacking" that the device's security could be breached. Electronic voting has been part of the Dutch electoral process, beginning with pilot projects over a decade ago.

Sources: "Voting with confidence," Report of the Election Process Advisory Commission ("Stemmen met vertrouwen," Adviescommissie inrichting verkiezingsprocess) (The Hague: 27 September 2007); "Dutch Minister: no computer voting until concerns are resolved," Associated Press (AP) (27 September 2007); "Electronic Voting, Section 3.12 Netherlands," Wikipedia (30 October 2007) (http://www,wikipedia.org).

Security analysis starts with the design of the voting system. An inappropriate design will make both organizational and technical security solutions useless.[41] Analyses of the system design examines the architecture of the software and hardware of the electronic equipment, and it should go a step further and look at how the

[41] Organizational security solutions limit access of certain individuals to sensitive aspects of the process by establishing access limitations, "four eyes" or "double key" requirements. An example of an organizational security solution would be a requirement that representatives of competing candidates inspect the voting machine, while technical security solutions are built into software and hardware of the voting equipment. An example of a technical security solution is the use of cryptography.

equipment interacts with the election process. Analyses should identify "security sensitive" points of the equipment and stages of the process, from production of the equipment, through phases of testing and use on election day. Once analysis defines security sensitive points, it should also attempt to identify possible threats to the system at these points, including the impact if security is corrupted. At the end, monitors should evaluate security solutions that are in place to block these possible threats. This includes evaluation of written security policies, observation of security sensitive procedures and evaluation of response measures.

RECOUNTS AND CHALLENGES

The first step in evaluating how election authorities might effectively respond to demands for recounts is to determine if meaningful recounts are possible at all. Simply stated - if there is no paper record of the electronic vote, there is nothing to recount. Recounts that are performed by "re-reading" the votes from the memory module by another machine do not provide certainty that the vote was properly recorded by the equipment - therefore such exercises do not meet the basic requirement for an effective remedy concerning challenges to the accuracy of the count and tabulation of results.

If meaningful recounts are possible under the technology used, monitors have to understand the legal provisions that trigger or that must be proven to warrant a recount. For example, some legislation prescribes that recounts be conducted automatically if the results of the elections are very close. Monitors should review legislation well before an election in order to evaluate it and seek reforms if they determine that the legal thresholds are set too high or too low. Also, observers must have a good understanding of post election day time lines in order to evaluate if deadlines were respected by the challenger and by the electoral administration.

In cases of discrepancy between the paper record and electronic record, the paper record should be taken as the legal representation of the voter's choice and should be determinative unless there is adequate evidence that the paper records were corrupted (for example, altered, substituted or "stuffed" as has been done with

paper ballots).[42] Where it appears that the paper ballots are uncorrupted and there is a discrepancy with the electronic record, even where the paper record is legally dispositive, investigation of the cause of the failure of the electronic record is necessary.

That investigation is likely to fall into the domain of computer forensics. Specialized investigators should attempt to determine why the discrepancy occurred. The investigation is necessary to determine, if possible, whether the discrepancy was the result of a malfunction, design failure or deliberate corruption of the technology, and, if that, which safeguards failed. This will help to address questions about confidence in the technology and the potential for correcting the problem in the future.

Even if there are no electoral challenges, a sound statistical sample of the electronic equipment should be included in a mandatory comparison of paper records to the machine's recorded electronic records. This provides verification of the integrity of the electronic technology and should reveal otherwise undetected problems that may not have effected electoral outcomes in the present election but which, nonetheless, could have distorted the results and which could pose critical problems in future elections. Such verifications also have an important benefit of building public confidence in the technology and in the rigor of election authorities for protecting electoral integrity.

OBSERVATION CAPACITY—STAFFING THE TEAM

Election observation organizations and political contestants should start developing their capacities to understand electronic election technologies well before they are introduced into the election system. It is necessary to do this in order to be able to play a role during the initial phases, while the debate on reasons for and against introduction of electronic voting is taking place. In the initial phase, there is no need to staff the organization with IT experts, though

[42] There are credible arguments that, where DREs are used, as compared to OMR or punch card voting and counting systems, the electronic record should be taken as the legal representation of the vote. These arguments note that the electronic record is the one originally created by the voter, and forensic computer tests can demonstrate whether the machine's software and firmware were free of flaws and whether the electronic record stored on the machine's memory device was tamper free. However, unless it is possible to rapidly complete forensic computer investigations in manners that are accepted by standards bodies and the courts as reliable "best evidence" of the voter's choice and in time to offer effective remedies to challengers, the paper record is the best basis to determine voter choice. Issues of monitoring for "paper trail tampering" (or stuffing the paper record box) and other issues related to the paper record can be addressed effectively and in a timely fashion, based on long-established monitoring techniques.

should IT experts be available their opinions can be valuable. The principles of transparency and accountability can be properly understood by political party and election observation experts, and the organizations and parties should be in position to advocate for the best public policies concerning use of electronic electoral technologies, including e-voting.

The phase that follows initial public policy debates is usually amendment of the legal framework. This phase will require combining legal and legislative expertise with good understanding of the information technology area. If legislation is to provide for electronic electoral technologies, it will have to properly address the following issues:

- information security;
- data protection;
- legal controls over encryption;
- computer crimes;
- issues of intellectual property law (including software patents);
- information access policies (sometimes called freedom of information issues); and
- similar matters.

Legal expertise also will be needed to ensure that legislation properly addresses issues of liability of equipment producers and effective remedies, including those needed to address electoral challenges and recounts.

Developing the capacity for evaluation of information technologies that may be introduced and used in the election system will require organizing a small team of experts. Ideally, the team would be led by an election monitoring expert, who has a good understanding of information technology. The role of the team leader will be to analyze the overall design of the system, to identify what type of expertise is

required for detailed evaluation of the proposed voting system technologies and to identify the needed experts. In addition, the role of the team leader will be to design the observation strategy and serve as the main analyst of the observation findings. While the information technology team will vary depending on different technologies, one position is necessary regardless of which technologies are used — a computer security expert.

The last pieces of the puzzle are the election day monitors (or observers for the observation groups and "poll watchers" for the political contestants). It is not required that the election day monitors be IT experts, since their role will not be to analyze the equipment but to evaluate adherence to the procedures, identify problems that may be visible and monitor the response of polling official to malfunctions of the equipment and other problems. More than with any other type of voting, it is important that election day observers and poll watchers are not simply trained on abstract principles, but that training actually allows them to become familiar with the equipment. This requires trainings to include simulations of the polling procedures that are as close as possible to real situations. While it is unlikely that the monitors will obtain the actual electoral equipment for their training sessions, the trainers for observation groups and political contestants should design their presentations using as many video and graphic tools as possible to help make poll watchers become familiar with the equipment.

ELECTION DAY OBSERVATION

By the time monitors are planning their observation of polling, they should have a clear idea of the limits the observation will face concerning electronic equipment. Also, before developing plans for observation of the polling, monitors should have good understanding of the electronic voting system that will be used at the polls, in order to develop an appropriate observation strategy. The observation strategy should be designed for specific election equipment and technologies. Trainings and reporting forms for election day poll watchers observers must take into account specifics of the equipment and should not be generic or simply focus on principles.

While some of the procedures at the polling station may be similar to paper ballot processes (such as the authentication of voters identity), some will be unobservable (such as casting the vote), and some will be specific for electronic voting (such as troubleshooting of equipment malfunctions). One of the absolutely critical procedures - the vote count — will be beyond access of the poll watchers and observers. However, while understanding the limits of the election day monitoring, observation groups and political contestants should still include polling operations in their election monitoring efforts.

Turnout Monitoring. One activity that poll watchers and observers can do on polling day that could provide an important indicator of one aspect of the integrity of the process is to closely monitor the number of individuals who cast their vote at the polling station. That number should at least closely correspond to the number of electronic votes registered. A significant variation would indicate a problem.

COUNTRY NOTE:
Venezuela 2006 - Electronic Voting in the Presidential Election

The Venezuelan electoral authorities employed touch screen voting machines that produced a paper ballot trail in over 99 percent of polling stations for the 2006 presidential elections. Early concerns were raised about electronic voting. In response, a number of pre-election audits of the hardware and software were conducted by the electoral authorities. They also agreed to keep the voting machines "disconnected" until counting was completed to prevent transmission of data to the machines, and did not initiate transmission of results until authorization was received from the National Electoral Council (CNE). Each voting machine also had a unique electronic signature, copies of which were given to political party representatives, to help verify the authenticity of the transmitted results. Representatives of the two principle presidential candidates, as well as nonpartisan domestic election monitors, observed activities in the CNE's National Tabulation Center and verified compliance with the pre-determined rules and procedures. As part of a pilot program, The Carter Center observed the use of electronic technologies in the election. While its report included recommendations for possible improvements, it did not note serious problems with the electronic voting system. The European Union found that the elections generally conformed to international standards and potentially opened the way forward for future improvements in the electoral process, and the domestic nonpartisan organization Ojo Electoral noted that election day processes went well.

Sources: "Developing a Methodology for Observing Electronic Voting," The Carter Center (October 2007); "Presidential Elections Venezuela 2006: Preliminary Statement, European Union Election Observation Mission" (December 2006); "Second Presidential Election Bulletin from 3 December 2006," Ojo Electoral (Electoral Eye)(4 December 2006).

Authentication of Voters. Polling stations equipped with electronic voting machines might also be equipped with an electronic voters list. These voter lists are sometimes called "Electronic Poll Books." While the basic function of an electronic poll book is similar to the paper voter list, sometimes the electronic poll books have additional functions and abilities. One of the capabilities of the electronic poll book is networking and connection with main voter databases. This enables the "e-book" to have access to updated voters list and to provide information to voters who showed up at the wrong polling station, telling them the location of the correct station where he or she should vote. As in the case of voting equipment, electronic poll books' design should be understood by observers well in advance, in order to plan observation strategy.[43]

Setup of the Equipment. Before any election procedure is conducted, the equipment is first "initialized" or "activated." Initialization is a procedure that enables equipment to perform election functions. Initialization will vary for different equipment, and monitors should become familiar with requirements for the specific equipment to be used. Some of the examples of setup elements are loading the software, calibration of scanners and unlocking the equipment. After initialization, voting equipment usually emulates the "empty ballot box procedure," meaning polling officials check that there are no recorded votes in the equipment and demonstrating this to monitors from political contestants and observation groups. This is sometimes called "printing of the zero tape" or "setting counters on zero."

Functionality of the Equipment and Troubleshooting Procedures. Machines malfunction, and this must be built into plans of the election authorities and the monitors of polling day procedures. The election day observer and poll watcher's role, beyond trying to identify any problems that voters may be experiencing without interfering in the process, is to observe the response of polling officials, contracted technicians and headquarters staff as malfunctions are detected. In order to do that properly, poll watchers and observers should be acquainted with the troubleshooting procedures that polling officials must follow.

[43] Please see Chapter 3 for discussion of related issues in voter registration processes. Procedures must be in place to address potential problems should e-book technologies break down, or should a voter be able to establish her/his identity and the e-book shows that the person already voted, and to address other challenges.

Security of the Equipment. It is practically impossible for monitors to evaluate security of the equipment at the polling station from any set of abstract security principles. Election day observers and poll watchers must be familiar with specific potential security breaches in order to observe the security aspect of polling. For that reason, they have to be educated concerning the potential, feasible and observable threats to the security of the equipment (i.e., what are the "entry points" and weaknesses of the equipment). In addition, monitors from political contestants and observation groups must be acquainted with organizational security procedures to which polling officials should adhere. The role of poll watchers and observers, however, is not to review security procedures — this should be evaluated before the polling — their role is to observe if the security procedures are respected.

Adherence of the Polling Officials to Procedures. It is not unusual in paper ballot elections for election officials on polling day to sometimes improvise and somewhat deviate from prescribed procedures. Trained election day observers and poll watchers should understand the impact of such deviations and whether they corrupt the polling process. With the introduction of electronic equipment, monitoring incidences of non-adherence to the prescribed procedures is particularly important. Simply said, non-adherence to procedures by the polling officials could jeopardize the security and integrity of equipment in ways that are not detectable. For this reason, it is of great importance that election day observers and poll watchers be familiar with prescribed procedures and that they closely observe whether procedures are correctly followed. As with the security procedures, evaluation of all of the procedures themselves should be done well in advance of polling, and monitors should simply observe adherence/non-adherence to the procedures.

Handling of the Equipment after Close of the Polls. Observation of the handling of the equipment after the polls are closed belongs under the security domain, however, it should be noted that the electronic voting equipment is classified as "sensitive election material." This means that even after the polls are closed, the equipment and parts of it must be secured with tamper proof or tamper evident tools and devices. This is necessary to preserve forensic evidence in cases where the equipment is inspected. Security procedures should guarantee that the equipment is stored in the same condition as it was during the voting.

Polling Day Testing. If the election officials conduct testing of the equipment during the polling day, monitors from observation groups and political contestants should have the right to observe it. These kinds of tests are sometimes called "hot audits." The test is usually done by excluding a machine from the polling process and testing the machine. If hot audits are performed, procedures must insure that the records and votes on the tested machine are preserved and secured. Hot audits are security sensitive for two main reasons.

- If the equipment is reintroduced to the polling process after the testing, procedures should insure that equipment's integrity was not corrupted during the testing (maliciously or by accident).

- If the election authorities replace the tested equipment with a new unit, the replacement unit should be scrutinized the same way as the other units at the polling station.

Any equipment that was used for testing on polling day (and any replacement units) should be treated as sensitive material and should be secured because it was part of the election process.

INTERNET VOTING

Internet voting for public offices is rare and the risks to the integrity of elections and the questions related to public confidence lead to a predominant opinion among electoral experts that Internet voting for public office is not appropriate. The main reasons cited for this are: problems for ensuring secrecy of the vote (which interrelates with problems concerning verification of the identity of the voter and potentials for coercion of voters); and electoral security problems related to the Internet. Because Internet voting is a topic of some discussion, a brief description will be presented below concerning approaches to monitoring it.[44]

[44] As noted earlier in this Guide, Estonia conducted elections in 2006 that extended the opportunity for Internet voting to all voters. See Republic of Estonia Parliamentary Elections 4 March 2007 OSCE/ODIHR Election Assessment Report (ODIHR.GAL/56/07, 28 June 2007). While the report held that the elections appeared to have been conducted generally in regard with OSCE commitments for democratic elections, it pointed to risks to the integrity of elections posed by Internet voting and noted that although election authorities made considerable efforts to minimize the risks, testing and auditing could have been more comprehensive, and there was almost no oversight by political parties or civil society groups. It stated that unless a number of factors are effectively addressed, authorities should reconsider whether Internet voting should be widely available as a voting method.

COUNTRY NOTE:
Estonia 2006 - Internet Voting Raises Issues of Ballot Secrecy and Systems Reliability

Estonia's 2006 parliamentary elections provide the only example to date where all voters could choose to register their vote via the Internet. This option was available only for early voting. Anyone who had registered a vote by Internet could recast it electronically, thus cancelling an earlier electronic vote, or could go to a polling station during the early voting period and cancel their electronic vote by casting a ballot. Approximately 5.4 percent of voters chose to use the Internet to register their electoral choices. While the overall election process was generally seen as acceptable, observers noted that critical problems were posed by the Internet voting method. Among the issues noted was the impossibility of ensuring secrecy of the ballot to those using uncontrolled environments for voting, such as in homes or public places. This opens the potential for various types of coercion of voters. Observers also noted that real risks to electoral integrity posed by the possibilities for external attacks on the electronic technology and/or by internal malfeasance. Observers also highlighted: the existence of a log that recorded the time each vote was cast, which created the perception that voting secrecy could be negated; the lack of proper full scale end-to-end testing, thereby missing opportunities to identify potential problems in the voting system; the lack of systematic monitoring for and planned responses to potential Internet threats; and a lack of monitoring, observation and involvement of the political parties and civil society organizations concerning the Internet voting system. If such issues cannot be effectively resolved, it was recommended that Estonian authorities consider carefully whether the Internet should be widely available as a voting method or whether it should be limited or not used at all.

Source: "Republic of Estonia Parliamentary Elections 4 March 2007," OSCE/ODIHR Election Assessment Mission Report (28 June 2007).

Monitoring of voting via the Internet does not differ greatly in the initial phases from other types of electronic voting. Issues concerning the legal framework, development of the system requirements, testing, certification, transparency, security and more are applicable to Internet voting as well. However, a few issues make voting by the Internet substantially different than any other type of electronic voting, and the observation strategy must focus on these issues.

Voting Servers. In other types of electronic voting, electronic votes are recorded and stored with an electronic voting unit at the polling stations. Votes are then transferred to counting computers, either by network or by transporting them in some type of memory storage device.

When voting via the Internet, computers that voters use do not store the votes. These computers serve only as a type of "interface" between voter and the server. The electronic record is created at the

voter's computer, but these votes are immediately transferred to the server via the Internet and stored there. An observation strategy will necessarily have to be focused on security of the voting servers — systematic observation of voter's actions and ballot casting at computers on the polling day will be nearly impossible, which leave important gaps that themselves have implications for electoral integrity.

Internet as a Public Network. Any type of networking of electronic voting equipment opens the possibility for security breaches. If the network is a global public network, as the Internet is, possibilities for security breaches are virtually endless. Internet voting systems simply inherit all the security threats and attacks that are characteristic for the Internet. Election authorities therefore should have a robust and formal monitoring operation of the potential threats to the voting servers. The other component of this operation should be threat response plans. Monitors from political contestants and observation groups should be able to review the election administration's monitoring activities and threat response plans.

Assuming that election authorities cannot provide Internet service themselves; they will have to rely on Internet service providers (ISP) for the connection to the vote servers. Effectively, this means that the ISPs are providing substantial and crucial service to the election administration. Relationships between election authorities and ISPs, quality of the ISP service, ISP obligations and related matters must be evaluated by monitors. Monitors need to understand that ISPs will have to be involved in threat response plans and that these response plans might even involve third parties — other ISPs, backbone providers and others.

Uncontrolled Environment. Voting in an uncontrolled environment is in fact not only an Internet voting issue. The same types of considerations related to voting in uncontrolled environments apply to, for example postal voting. The two most problematic issues are authentication of the voter's identity and secrecy of the vote. For those reasons, many object to a general franchise by the Internet and postal voting.

Internet voting systems, however, could theoretically develop answers to these considerations. Authentication of voters perhaps

could be established by using biometric tools, personal identification numbers (PIN), passwords and digital certificates. Secrecy of the vote perhaps could be strengthened by discouraging those who organize vote buying and intimidation through allowing voters to recast their vote any time and thus cancel their Internet vote (though this presents challenges as well). However, while in principle there are some good ideas about how to address these issues, practicable solutions are not available.

Internet Voting and Internet Shopping. Very often Internet voting is compared to Internet shopping or Internet banking (e-commerce). It is important to understand that these are substantially different activities for a few reasons. The most important one is secrecy of the vote. E-commerce systems are built to record every action of every component of the system. E-commerce transactions are "traceable" and analyses of each transaction can be done quickly and thoroughly, and the systems are built to prevent anonymity. On the other hand, Internet voting has a completely opposite and fundamental requirement - "transactions" (vote casting) should not be traceable, and the vote should not be connected to the voters. For these reasons, it would be extremely difficult to detect security failures of an Internet voting system, while in e-commerce detection is much easier because e-commerce is not anonymous.

APPENDICES

APPENDIX ONE:

List of International Organizations that Monitor Information Technology (IT) in the Electoral Process

INTERGOVERNMENTAL ORGANIZATIONS

Council of Europe's European Commission for Democracy through Law (Venice Commission):

http://www.venice.coe.int/

Since its creation, the Venice Commission has been active in the electoral field, in particular, through the adoption of opinions on draft electoral legislation. In 2004, the Council of Europe's Committee of Ministers adopted Recommendation Rec (2004)11 to member states on legal, operational and technical standards for e-voting.

European Commission:

http://ec.europa.eu/index_en.htm

Election observation plays a major role in the European Union's policy of promoting human rights and democratization throughout the world. In September 2000, the European Commission launched the CyberVote project to demonstrate fully verifiable on-line elections with voter privacy using fixed and mobile Internet terminals. In 2006, the European Commission published a report titled Methodological Guide to Electoral Assistance that, among other things, introduced the factors to consider when dealing with electoral technology.

International IDEA:

http://www.idea.int/elections/index.cfm

International IDEA provides support for making electoral administration more professional. It supports the design of professionally managed independent electoral processes which are tailored to local circumstances and engender public confidence in legitimate and credible elections and referenda. International IDEA has developed a three-day Electoral Assistance Training course for reorienting development agencies for long-term electoral planning. One aspect of the course focuses on introducing the cross-cutting issues and the factors to be considered when embracing technology for electoral processes.

Organization for Security and Cooperation in Europe, Office for Democratic Institutions and Human Rights (OSCE/ODIHR):

http://www.osce.org/odihr-elections/

The ODIHR deploys election observation missions to OSCE participating States to assess the implementation of OSCE commitments relating to elections. The Office also conducts technical-assistance projects and legislative reviews. With an increasing number of OSCE participating States using electronic technology in the electoral process, the organization has expanded its monitoring efforts to address these issues. For instance, an OSCE mission followed the use of remote voting by Internet during the 2007 Estonian Parliamentary elections, which was the first countrywide use of the Internet as a voting method in an OSCE participating State.

Organization of American States (OAS):

http://www.oas.org/

In many of the region's elections, the OAS acts as an international observer, working with the Member States to strengthen the democratic process and promote fairness and transparency. With Member States increasingly using electronic technology, and as part of the Plan of Action of Quebec City handed down by the Third Summit of the Americas, the OAS Heads of State and Government created the Inter-American Electoral Technology Program (PITE), which focuses the inter-American system on the holding of elections that are more modern, transparent and efficient throughout the hemisphere. The program covers such areas as service to voters, automating electoral procedures and adopting information technology.

NONGOVERNMENTAL ORGANIZATIONS

The Carter Center:

http://www.cartercenter.org/

The Carter Center observers analyze election laws, assess voter education and registration processes and evaluate fairness in campaigns. Of particular note, the Carter Center sent a medium term observer group to assess preparations, including the use of new automated voting and fingerprint machines for Venezuela's 2004

Presidential referendum. The Carter Center organized a meeting in Atlanta, Georgia, in November 2006 that discussed approaches to observing electronic voting technologies.

IFES:

http://www.ifes.org/

IFES provides countries with the technical advice and tools they need to run democratic elections. For instance, IFES designed a program in Information Technology training which includes training in Windows NT and in Visual Basic for the Nigerian Election Commission (INEC) in 1999. In addition, IFES assisted and trained INEC in software design to manage a voter registry with 60 million records.

National Democratic Institute for International Affairs (NDI):

http://www.ndi.org/

The National Democratic Institute for International Affairs (NDI) is a nonprofit organization working to strengthen and expand democracy worldwide. Since 1987, NDI has supported nonpartisan domestic election monitors and political parties in safeguarding the electoral process and advocating for democratic reform in more than 90 countries. In addition, NDI has observed more than 100 elections in over 50 countries, before, during and after election day. Included in these efforts is promoting understanding of the need for transparency, fairness and accountability, including verification of the integrity of electronic technologies in elections. NDI has produced over 300 documents to assist these efforts, including this Guide on Monitoring Electronic Technologies in Election Processes and other guides and handbooks on election monitoring.

APPENDIX TWO:

Organizations and Agencies Working Towards Standardization in Information Technology

International Organization for Standardization (ISO):

http://www.iso.org/

ISO is a network of the national standards institutes of 154 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. It is a non-governmental organization and its members are not, as is the case in the United Nations system, delegations of national governments. Nevertheless, ISO occupies a special position between the public and private sectors. This is because, on the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations. Therefore, ISO is able to act as a bridging organization in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users.

Institute of Electrical and Electronics Engineers (IEEE):

http://www.ieee.org/

The IEEE, a non-profit organization, is a professional association for the advancement of technology. Through its global membership, the IEEE is a leading authority on areas ranging from aerospace systems, computers and telecommunications to biomedical engineering, electric power and consumer electronics among others. Members rely on the IEEE as a source of technical and professional information, resources and services. To foster an interest in the engineering profession, the IEEE also serves student members in colleges and universities around the world. Other important constituencies include prospective members and organizations that purchase IEEE products and participate in conferences or other IEEE programs.

Organization for the Advancement of Structured Information Standards (OASIS):

http://www.oasis-open.org/

OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.

The Consortium hosts two widely respected information portals on XML and Web services standards, Cover Pages and XML.org. OASIS Member Sections include CGM Open, IDtrust, LegalXML, Open CSA and SGML Open.

National Institute of Standards and Technology (NIST):

http://www.nist.gov/

From automated teller machines and atomic clocks to mammograms and semiconductors, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology. Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life.

United States Election Assistance Commission (EAC):

http://www.eac.gov/

The EAC was established by the Help America Vote Act of 2002 (HAVA). Central to its role, the Commission serves as a national clearinghouse and resource for information and review of procedures with respect to the administration of Federal elections. According to the text of HAVA, the law was enacted to establish a program to provide funds to States to replace punch card voting systems, to establish the Election Assistance Commission to assist in the administration of Federal elections and to otherwise provide assistance with the administration of certain Federal election laws and programs, to establish minimum election administration

standards for States and units of local government with responsibility for the administration of Federal elections, and for other purposes. Among other things, HAVA requires the EAC to:

- Generate technical guidance on the administration of federal elections.
- Produce voluntary voting systems guidelines.
- Research and report on matters that affect the administration of federal elections.
- Provide grants for election technology development and for pilot programs to test election technology.
- Develop a national program for the testing, certification, and decertification of voting systems.

APPENDIX THREE:

International Human Rights Provisions Supporting Transparency in the Electoral Process through Freedom of Information and Expression

INTERNATIONAL TREATIES AND UN DOCUMENTS

Universal Declaration of Human Rights

Article 2

Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Article 19

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 21

1. Everyone has the right to take part in the government of his country, directly or through freely chosen representatives.

2. Everyone has the right to equal access to public service in his country.

3. The will of the people shall be the basis of the authority of government; this shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.

International Covenant on Civil and Political Rights

Article 2

1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

2. Where not already provided for by existing legislative or other measures, each State Party to the present Covenant undertakes to take the necessary steps, in accordance

with its constitutional processes and with the provisions of the present Covenant, to adopt such legislative or other measures as may be necessary to give effect to the rights recognized in the present Covenant.

3. Each State Party to the present Covenant undertakes:

    a. To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;

    b. To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;

    c. To ensure that the competent authorities shall enforce such remedies when granted.

Article 19

1. Everyone should have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expressions; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary

    a. For respect of the rights or reputations of others;

    b. For the protection of national security or of public order (ordre public), or of public health or morals.

Article 25

Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions:

a. To take part in the conduct of public affairs, directly or through freely chosen representatives;

b. To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors;

c. To have access, on general terms of equality, to public service in his country.

International Convention on the Elimination of All Forms of Racial Discrimination

Article 5

In compliance with the fundamental obligations laid down in Article 2 of this Convention, States Parties undertake to prohibit and to eliminate racial discrimination in all its forms and to guarantee the right of everyone, without distinction as to race, colour, or national or ethnic origin, to equality before the law, notably in the enjoyment of the following rights:

...

c. Political rights, in particular the rights to participate in elections - to vote and to stand for election - on the basis of universal and equal suffrage, to take part in the Government as well as in the conduct of public affairs at any level and to have equal access to public service;

d. Other civil rights, in particular;

...

viii. The right to freedom of opinion and expression... .

Convention on the Elimination of All Forms of Discrimination Against Women

Article 7

States Parties shall take all appropriate measures to eliminate discrimination against women in the political and public life of the country and, in particular, shall ensure to women, on equal terms with men, the right:

(a) To vote in all elections and public referenda and to be eligible for election to all publicly elected bodies;

(b) To participate in the formulation of government policy and the implementation thereof and to hold public office and perform all public functions at all levels of government;

(c) To participate in non-governmental organizations and associations concerned with the public and political life of the country.

Article 8

States Parties shall take all appropriate measures to ensure to women, on equal terms with men and without any discrimination, the opportunity to represent their Governments at the international level and to participate in the work of international organizations.

Convention on the Political Rights of Women

Article I

Women shall be entitled to vote in all elections on equal terms with men without any discrimination.

Article II

Women shall be eligible for election to all publicly elected bodies, established by national law, on equal terms with men, without any discrimination.

Article III

Women shall be entitled to hold public office and to exercise all public functions, established by national law, on equal terms with men, without any discrimination.

UN Convention Against Corruption

Article 10

Public reporting

Taking into account the need to combat corruption, each State Party shall, in accordance with the fundamental principles of its domestic law, take such measures as may be necessary to enhance transparency in its public administration, including with regard to its organization, functioning and decision-making processes, where appropriate. Such measures may include, inter alia:

(a) Adopting procedures or regulations allowing members of the general public to obtain, where appropriate, information on the organization, functioning and decision-making processes of its public administration and, with due regard for the protection of privacy and personal data, on decisions and legal acts that concern members of the public;

(b) Simplifying administrative procedures, where appropriate, in order to facilitate public access to the competent decision-making authorities; and

(c) Publishing information, which may include periodic reports on the risks of corruption in its public administration.

Article 13

Participation of society

(1) Each State Party shall take appropriate measures, within its means and in accordance with fundamental principles of its domestic law, to promote the active participation of individuals and groups outside the public sector, such as civil society, non-governmental organizations and community-based organizations, in the prevention of and the fight against corruption and to raise public awareness regarding the existence, causes and gravity of and the threat posed by corruption.

This participation should be strengthened by such measures as:

(a) Enhancing the transparency of and promoting the contribution of the public to decision-making processes;

(b) Ensuring that the public has effective access to information;

(c) Undertaking public information activities that contribute to non-tolerance of corruption, as well as public education programmes, including school and university curricula;

(d) Respecting, promoting and protecting the freedom to seek, receive, publish and disseminate information concerning corruption. That freedom may be subject to certain restrictions, but these shall only be such as are provided for by law and are necessary:

(i) For respect of the rights or reputations of others;

(ii) For the protection of national security or order public or of public health or morals.

(2) Each State Party shall take appropriate measures to ensure that the relevant anti-corruption bodies referred to in this Convention are known to the public and shall provide access to such bodies, where appropriate, for the reporting, including anonymously, of any incidents that may be considered to constitute an offence established in accordance with this Convention.

REGIONAL INSTRUMENTS: AFRICAN UNION

African Charter on Human and Peoples' Rights

Article 9

1. Every individual shall have the right to receive information.

2. Every individual shall have the right to express and disseminate his opinions within the law.

Article 13

1. Every citizen shall have the right to participate freely in the government of his country, either directly or through freely chosen representatives in accordance with the provisions of the law.

Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa
(ACHPR - PW)(2003)

Article 9 Right to Participation in the Political and Decision-Making Process

1. States Parties shall take specific positive action to promote participative governance and the equal participation of women in the political life of their countries through affirmative action, enabling national legislation and other measures to ensure that:

    (a) women participate without any discrimination in all elections;

    (b) women are represented equally at all levels with men in all electoral processes;

2. States Parties shall ensure increased and effective representation and participation of women at all levels of decision-making.

African Charter on Democracy, Elections and Governance[1]

Article 2

The objectives of the Charter are to:

...

3. Promote the holding of regular free and fair elections to institutionalize legitimate authority of representative government as well as democratic change of governments;

...

[1] Not yet entered into force.

10. Promote the establishment of necessary conditions to foster citizen participation, transparency, access to information, freedom of the press and accountability in the management of public affairs;

...

13. Promote best practices in the management of elections for purposes of political stability and good governance.

Article 3

State parties shall implement this Charter in accordance with the following principles:

...

4. Holding of regular, transparent, free and fair elections;

...

8. Transparency and fairness in the management of public affairs;

...

Article 12

State parties undertake to implement programmes and carry out activities designed to promote democratic principles and practices as well as consolidate a culture of democracy and peace.
To this end, State Parties shall:

1. Promote good governance by ensuring transparent and accountable administration.

2. Strengthen political institutions to entrench a culture of democracy and peace.

3. Create conducive conditions for civil society organizations to exist and operate within the law.

4. Integrate civic education in their educational curricula and develop appropriate programmes and activities.

Article 27

In order to advance political, economic and social governance, State Parties shall commit themselves to:

...

2. Fostering popular participation and partnership with civil society organizations;

...

7. Promoting freedom of expression, in particular freedom of the press and fostering a professional media;

Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights, 32nd Session

Principle IV, Freedom of Information:

1. Public bodies hold information not for themselves but as custodians of the public good and everyone has a right to access this information, subject only to clearly defined rules established by law.

2. The right to information shall be guaranteed by law in accordance with the following principles: everyone has the right to access information held by public bodies; everyone has the right to access information held by private bodies which is necessary for the exercise or protection of any right ...

REGIONAL INSTRUMENTS: ORGANIZATION OF AMERICAN STATES

American Convention on Human Rights

Article 13. Freedom of Thought and Expression

1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other media of one's choice.

2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but

shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure:

a. respect for the rights or reputations of others; or

b. the protection of national security, public order, or public health or morals.

Article 23. Right to Participate in Government

1. Every citizen shall enjoy the following rights and opportunities:

   a. to take part in the conduct of public affairs, directly or through freely chosen representatives;

   b. to vote and to be elected in genuine periodic elections, which shall be by universal and equal suffrage and by secret ballot that guarantees the free expression of the will of the voters; and

   c. to have access, under general conditions of equality, to the public service of his country.

2. The law may regulate the exercise of the rights and opportunities referred to in the preceding paragraph only on the basis of age, nationality, residence, language, education, civil and mental capacity, or sentencing by a competent court in criminal proceedings.

American Declaration of the Rights and Duties of Man

Article IV.

Every person has the right to freedom of investigation, of opinion, and of the expression and dissemination of ideas, by any medium whatsoever.

Article XX.

Every person having legal capacity is entitled to participate in the government of his country, directly or through his representatives, and to take part in popular elections, which shall be by secret ballot, and shall be honest, periodic and free.

...

It is likewise his duty to hold any public office to which he may be elected by popular vote in the state of which he is a national.

Inter-American Democratic Charter

Article 4

Transparency in government activities, probity, responsible public administration on the part of governments, respect for social rights, and freedom of expression and of the press are essential components of the exercise of democracy.

Inter-American Convention on the Granting of Political Rights to Women

Article 1

The High Contracting Parties agree that the right to vote and to be elected to

Declaration of Principles on Freedom of Expression
Approved by the Inter-American Commission
on Human Rights
(108th regular session)

RECOGNIZING the need to protect freedom of expression effectively in the Americas, the Inter-American Commission on Human Rights, in support of the Special Rapporteur for Freedom of Expression, adopts the following Declaration of Principles:

PRINCIPLES

1. Freedom of expression in all its forms and manifestations is a fundamental and inalienable right of all individuals. Additionally, it is an indispensable requirement for the very existence of a democratic society.

2. Every person has the right to seek, receive and impart information and opinions freely under terms set forth in Article 13 of the American Convention on Human Rights. All people should be afforded equal opportunities to receive, seek and impart information by any means of communication without any discrimination for reasons of race, color, sex, language, religion, political or other opinions, national or social origin, economic status, birth or any other social condition.

...

4. Access to information held by the state is a fundamental right of every individual. States have the obligation to guarantee the full exercise of this right. This principle allows only exceptional limitations that must be previously established by law in case of a real and imminent danger that threatens national security in democratic societies.

...

10. Privacy laws should not inhibit or restrict investigation and dissemination of information of public interest...

REGIONAL INSTRUMENTS: EUROPEAN UNION

Charter of Fundamental Rights of the European Union

Article 11 Freedom of Expression and Information

1. Everyone has the right to freedom of expression. This right shall included freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected.

Article 12 Freedom of Assembly and of Association

1. Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, in particular in political, trade union and civic matters,

2. Political parties at Union level contribute to expressing the political will of the citizens of the Union.

Article 39 Right to vote and to stand as a candidate at elections to the European Parliament

1. Every citizen of the Union has the right to vote and to stand as a candidate at elections to the European Parliament in the Member State in which he or she resides, under the same conditions as nationals of that State.

2. Members of the European Parliament shall be elected by direct universal suffrage in a free and secret ballot.

Article 40 Right to vote and to stand as a candidate at municipal elections

Every citizen of the Union has the right to vote and to stand as a candidate at municipal elections in the Member State in which he or she resides under the same conditions as nationals of that State.

REGIONAL INSTRUMENTS: COUNCIL OF EUROPE

European Convention for the Protection of Human Rights and Fundamental Freedoms

Article 10

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are proscribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Protocol (No. 1) to the [European] Convention for the Protection of Human Rights and Fundamental Freedoms

Article 3

The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature.

Framework Convention for the Protection of National Minorities

Article 4

2. The Parties undertake to adopt, where necessary, adequate measures in order to promote, in all areas of economic, social, political and cultural life, full and effective equality between persons belonging to a national minority and those belonging to the majority. In this respect, they shall take due account of the specific conditions of the persons belonging to national minorities.

3. The measures adopted in accordance with paragraph 2 shall not be considered to be an act of discrimination.

Article 7

The Parties shall ensure respect for the right of every person belonging to a national minority to freedom of peaceful assembly, freedom of association, freedom of expression, and freedom of thought, conscience and religion.

Article 9

1. The Parties undertake to recognise that the right to freedom of expression of every person belonging to a national minority includes freedom to hold opinions and to receive and impart information and ideas in the minority language, without interference by public authorities and regardless of frontiers. The Parties shall ensure, within the framework of their legal systems, that persons belonging to a national minority are not discriminated against in their access to the media.

Article 15

The Parties shall create the conditions necessary for the effective participation of persons belonging to national minorities in [...] public affairs, in particular those affecting them.

European Charter of Local Self-Government

Article 3 Concept of local self-government

1. Local self-government denotes the right and the ability of local authorities, within the limits of the law, to regulate and manage a substantial share of public affairs under their own responsibility and in the interests of the local population.

2. This right shall be exercised by councils or assemblies composed of members freely elected by secret ballot on the basis of direct, equal, universal suffrage, and which may possess executive organs responsible to them. This provision shall in no way affect recourse to assemblies of citizens, referendums or any other form of direct citizen participation where it is permitted by statute.

Code of Good Practice in Electoral Matters (Venice Commission)

3.2.2.3. Mechanical and electronic voting methods

42. Several countries are already using, or are preparing to introduce mechanical and electronic voting methods. The advantage of these methods becomes apparent when a number of elections are taking place at the same time, even though certain precautions are needed to minimise the risk of fraud, for example by enabling the voter to check his or her vote immediately after casting it. Clearly, with this kind of voting, it is important to ensure that ballot papers are designed in such a way as to avoid confusion. In order to facilitate verification and a recount of votes in the event of an appeal, it may also be provided that a machine could print votes onto ballot papers; these would be placed in a sealed container where they cannot be viewed. Whatever means used should ensure the confidentiality of voting.

43. Electronic voting methods must be secure and reliable. They are secure if the system can withstand deliberate attack; they are reliable if they can function on their own, irrespective of any shortcomings in the hardware or software. Furthermore, the elector must be able to obtain confirmation of his or her vote and, if necessary, correct it without the secrecy of the ballot being in any way violated.

44. Furthermore, the system's transparency must be guaranteed in the sense that it must be possible to check that it is functioning properly.

Recommendation Rec (2004)11 of the Committee of Ministers to Member States on Legal, Operational and Technical Standards for E-voting

(Adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and promoting the ideals and principles, which are their common heritage;

Reaffirming its belief that representative and direct democracy are part of that common heritage and are the basis of the participation of citizens in political life at the level of the European Union and at national, regional and local levels;

Respecting the obligations and commitments as undertaken within existing international instruments and documents, such as:

- the Universal Declaration on Human Rights;
- the International Covenant on Civil and Political Rights;
- the United Nations Convention on the Elimination of All Forms of Racial Discrimination;
- the United Nations Convention on the Elimination of All Forms of Discrimination against Women;
- the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), in particular its Protocol No. 1 (ETS No. 9);
- the European Charter of Local Self-Government (ETS No. 122);
- the Convention on Cybercrime (ETS No. 185);
- the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108);

- Committee of Ministers Recommendation No. R (99) 5 on the protection of privacy on the Internet;

- the document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE;

- the Charter of Fundamental Rights of the European Union;

- the Code of Good Practice in Electoral Matters, adopted by the Council for democratic elections of the Council of Europe and the European Commission for Democracy through Law;

Bearing in mind that the right to vote is one of the primary foundations of democracy, and that, consequently, e-voting system procedures shall comply with the principles of democratic elections and referendums;

Recognising that as new information and communication technologies are increasingly being used in day-to-day life, member states need to take account of these developments in their democratic practice;

Noting that participation in elections and referendums at local, regional and national levels in some member states is characterised by low, and in some cases steadily decreasing, turnouts;

Noting that some member states are already using, or are considering using e-voting for a number of purposes, including:

- enabling voters to cast their votes from a place other than the polling station in their voting district;

- facilitating the casting of the vote by the voter;

- facilitating the participation in elections and referendums of all those who are entitled to vote, and particularly of citizens residing or staying abroad;

- widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;

- increasing voter turnout by providing additional voting channels;

- bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;

- reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;

- delivering voting results reliably and more quickly; and

- providing the electorate with a better service, by offering a variety of voting channels;

Aware of concerns about certain security and reliability problems possibly inherent in specific e-voting systems;

Conscious, therefore, that only those e-voting systems which are secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build the public confidence which is a pre-requisite for holding e-voting,

Recommends that the governments of member states, where they are already using, or are considering using, e-voting comply, subject to paragraph iv. below, with paragraphs i. to iii. below, and the standards and requirements on the legal, operational and technical aspects of e-voting, as set out in the Appendices to the present Recommendation:

i. e-voting shall respect all the principles of democratic elections and referendums. E-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means. This general principle encompasses all electoral matters, whether mentioned or not in the Appendices;

ii. the interconnection between the legal, operational and technical aspects of e-voting, as set out in the Appendices, has to be taken into account when applying the Recommendation;

iii. member states should consider reviewing their relevant domestic legislation in the light of this Recommendation;

iv. the principles and provisions contained in the Appendices to this Recommendation do not, however, require individual member states to change their own domestic voting procedures which may exist at the time of the

adoption of this Recommendation, and which can be maintained by those member states when e-voting is used, as long as these domestic voting procedures comply with all the principles of democratic elections and referendums;

v. in order to provide the Council of Europe with a basis for possible further action on e-voting within two years after the adoption of this Recommendation, the Committee of Ministers recommends that member states:

- keep under review their policy on, and experience of, e-voting, and in particular the implementation of the provisions of this Recommendation; and

- report to the Council of Europe Secretariat the results of their reviews, who will forward them to member states and follow up the issue of e-voting.

In this Recommendation the following terms are used with the following meanings:

- authentication: the provision of assurance of the claimed identity of a person or data;

- ballot: the legally recognised means by which the voter can express his or her choice of voting option;

- candidate: a voting option consisting of a person and/or a group of persons and/or a political party;

- casting of the vote: entering the vote in the ballot box;

- e-election or e-referendum: a political election or referendum in which electronic means are used in one or more stages;

- electronic ballot box: the electronic means by which the votes are stored pending being counted;

- e-voting: an e-election or e-referendum that involves the use of electronic means in at least the casting of the vote;

- remote e-voting: e-voting where the casting of the vote is done by a device not controlled by an election official;

- sealing: protecting information so that it cannot be used or interpreted without the help of other information or means available only to specific persons or authorities;
- vote: the expression of the choice of voting option;
- voter: a person who is entitled to cast a vote in a particular election or referendum;
- voting channel: the way by which the voter can cast a vote;
- voting options: the range of possibilities from which a choice can be made through the casting of the vote in an election or referendum;
- voters' register: a list of persons entitled to vote (electors)...

REGIONAL INSTRUMENTS: ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE COMMITMENTS

Document of the 1990 Copenhagen Meeting of the Conference on the Human Dimension (Copenhagen Document of the OSCE)

[The participating States] recognize that pluralistic democracy and the rule of law are essential for ensuring respect for all human rights and fundamental freedoms, the development of human contacts and the resolution of other issues of a related humanitarian character. They therefore welcome the commitment expressed by all participating States to the ideals of democracy and political pluralism as well as their common determination to build democratic societies based on free elections and the rule of law.

...

In order to strengthen respect for, and enjoyment of, human rights and fundamental freedoms, to develop human contacts and to resolve issues of a related humanitarian character, the participating States agree on the following:

...

(3) They reaffirm that democracy is an inherent element of the rule of law. They recognize the importance of pluralism with regard to political organizations.

...

(5) They solemnly declare that among those elements of inherent dignity and of the equal and inalienable rights of all human beings are the following:

(5.1) - free elections that will be held at reasonable intervals by secret ballot or by equivalent free voting procedure, under conditions which ensure in practice the free expression of the opinion of the electors in the choice of their representatives;

(5.10) - everyone will have an effective means of redress against administrative decisions, so as to guarantee respect for fundamental rights and ensure legal integrity;

(6) The participating States declare that the will of the people, freely and fairly expressed through periodic and genuine elections, is the basis of the authority and legitimacy of all government. The participating States will accordingly respect the right of their citizens to take part in the governing of their country, either directly or through representatives freely chosen by them through fair electoral processes.

(7) To ensure that the will of the people serves as the basis of the authority of government, the participating States will:

(7.1) - hold free elections at reasonable intervals, as established by law;

(7.5) - respect the right of citizens to seek political or public office, individually or as representatives of political parties or organizations, without discrimination;

(7.6) - respect the right of individuals and groups to establish, in full freedom, their own political parties or other political organizations and provide such political parties and organizations with the necessary legal guarantees to enable them to compete with each other on a basis of equal treatment before the law and by the authorities;

(7.8) - provide that no legal or administrative obstacle stands in the way of unimpeded access to the media on a non- discriminatory basis for all political groupings and individuals wishing to participate in the electoral process;

(8) The participating States consider that the presence of observers, both foreign and domestic, can enhance the electoral process for

States in which elections are taking place. They therefore invite observers from any other CSCE [now OSCE] participating States and any appropriate private institutions and organizations who may wish to do so to observe the course of their national election proceedings, to the extent permitted by law. They will also endeavour to facilitate similar access for election proceedings held below the national level. Such observers will undertake not to interfere in the electoral proceedings.

(9) The participating States reaffirm that

(9.1) - everyone will have the right to freedom of expression including the right to communication. This right will include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The exercise of this right may be subject only to such restrictions as are prescribed by law and are consistent with international standards. In particular, no limitation will be imposed on access to, and use of, means of reproducing documents of any kind, while respecting, however, rights relating to intellectual property, including copyright....

...

(10) In reaffirming their commitment to ensure effectively the rights of the individual to know and act upon human rights and fundamental freedoms, and to contribute actively, individually or in association with others, to their promotion and protection, the participating States express their commitment to:

(10.1) - respect the right of everyone, individually or in association with others, to seek, receive and impart freely views and information on human rights and fundamental freedoms, including the rights to disseminate and publish such views and information;

...

(10.3) - ensure that individuals are permitted to exercise the right to association, including the right to form, join and participate effectively in non-governmental organizations which seek the promotion and protection of human rights and fundamental freedoms, including trade unions and human rights monitoring groups;

(10.4) - allow members of such groups and organizations to have unhindered access to and communication with similar bodies within and outside their countries and with international organizations, to engage in exchanges, contacts and co-operation with such groups and organizations and to solicit, receive and utilize for the purpose of promoting and protecting human rights and fundamental freedoms voluntary financial contributions from national and international sources as provided for by law.

...

(24) The participating States will ensure that the exercise of all the human rights and fundamental freedoms set out above will not be subject to any restrictions except those which are provided by law and are consistent with their obligations under international law, in particular the International Covenant on Civil and Political Rights, and with their international commitments, in particular the Universal Declaration of Human Rights. These restrictions have the character of exceptions. The participating States will ensure that these restrictions are not abused and are not applied in an arbitrary manner, but in such a way that the effective exercise of these rights is ensured.

Any restriction on rights and freedoms must, in a democratic society, relate to one of the objectives of the applicable law and be strictly proportionate to the aim of that law.

In addition to the provisions of these international human rights instruments, which create obligations for the states that are parties to the documents, there are a number of other significant declarations and documents of associations of states and of the associations of the legislative branches of governments. Included among those that are directly relevant to democratic elections are the following: The Harare Declaration of the Commonwealth of Nations; Documents of the Summit Meetings of the Organization of Security and Cooperation in Europe subsequent to the 1990 Copenhagen Document; the 2001 Norms and Standards for Elections in the SADC Region adopted by the Southern Africa Development Council Parliamentary Forum; and the 1994 Declaration on Criteria for Free and Fair Elections of the Inter-Parliamentary Union.

APPENDIX FOUR:

International Human Rights Tribunals

United Nations Human Rights Committee: States that have signed the First Optional Protocol to the International Covenant on Civil and Political Rights have agreed to allow persons within the Member State to obtain an opinion from the Committee regarding violations of that Covenant. For those countries, the Human Rights Committee can thus function as a mechanism for the international redress of human rights abuses.

European Commission of Human Rights: In addition to alleged breaches of the Convention for the Protection of Human Rights and Fundamental Freedoms referred by State Parties to the Convention, the Commission may receive petitions from any person, NGO or group of individuals claiming to be a victim of a violation by a State Party that has accepted the jurisdiction of the Commission to receive such petitions.

European Court of Human Rights: The Court's mission is to enforce the Convention for the Protection of Human Rights and Fundamental Freedoms, by ruling over complaints against human rights violations committed by States Parties, and brought to the Court either by other States Parties or by individuals subject to the jurisdiction of a State Party.

Inter-American Commission on Human Rights: The Commission reviews human rights petitions based on the OAS Charter, the American Declaration of the Rights and Duties of Man and the American Convention on Human Rights.

Inter-American Court of Human Rights: The Court receives human rights cases submitted to it by States Parties to the American Convention on Human Rights (ACHR) and the Inter-American Human Rights Commission. Member States of the Organization of American States and certain organs of the OAS may consult the Court regarding the interpretation of the ACHR or of other treaties concerning the protection of human rights in the American states.

UNITED NATIONS HUMAN RIGHTS COMMITTEE

Analysis

The United Nations Human Rights Committee oversees compliance of State Parties to the International Covenant on Civil and Political Rights as well as considers claims under the provisions of the First Optional Protocol to the Covenant. The Committee issues General Comments to help clarify provisions of the Covenant and obligations of State Parties to it. The Committee's General Comment 10 relates to

the freedom of expression, including the right to seek, receive and impart information under Article 19 of the Covenant, and its General Comment 25 relates to the right to participate in public affairs, including the rights to vote and be elected in genuine elections. A number of claims under the First Optional Protocol have related to one or other of the Articles but not to the interface of the two.

The Committee has made clear in General Comment 25 that any conditions (restrictions) that State Parties apply to the rights covered in Article 25 of the Covenant must be based on objective and reasonable criteria. The Article itself states that the rights must be enjoyed without any bases of discrimination noted in Article 2, including political opinion, and without unreasonable restrictions. The Committee also stated in General Comment 25 (paragraph 20) that "votes should be counted in the presence of the candidates or their agents. There should be independent scrutiny of the voting and counting processes and access to judicial review or other equivalent process so that electors have confidence in the security of the ballot and the counting of votes."

The views of the Committee have held that restrictions of Article 19 rights that meet a legitimate objective pursuant to Article 19 may violate the rights protected if they are not demonstrated to be "necessary" to achieve that purpose (Mukong v. Cameroon) and that Article 19 rights may not be frustrated where their exercise does not threaten public order, national security or the rights and reputation of others (Velichkin v. Belarus).

It is likely therefore that the Commission would support a proposition that State Parties to the Covenant must allow access to electronic technologies that are used to register and count votes, as well as technologies that are central to the exercise of the franchise, such as those used in voter registration and other processes vital to the right to vote and to be elected. Independent verification of technologies also would be consistent with the Committee's reasoning.

Jurisprudence

Schetko v. Belarus
(CCPR/C/87/D/1009/2001, 87th Session (8/8/06)) available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that, while freedom of expression is not absolute, when a State Party imposes sanctions against citizens distributing leaflets encouraging voters to boycott parliamentary elections, such action constitutes an infringement of the authors' right to freedom of speech pursuant to Article 19.

Bodro ić v. Serbia
(CCPR/C/85/D/1180/2003, 85th Session (1/26/06)) available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that the conviction of a Serbian journalist for criminal insult against a prominent public and political figure violated Article 19 insofar as the punishment disproportionately restricted the author's ability to participate in the public debate necessary for a democratic society.

Velichkin v. Belarus
(CCPR/C/85/D/1022/2001, 85th Session (11/23/05)) available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that the Belorussian government violated Article 19 when it arrested, held, and fined a citizen who stood on a street corner passing out copies of the Universal Declaration of Human Rights. The Committee further noted that, irrespective of its domestic legal qualification, the state's actions constituted a "de facto limitation of the author's" Article 19 right to impart information because his activities did not threaten public order, national security or the rights and reputation of others.

Jong-Cheol v. Republic of Korea
(CCPR/C/84//D/968/2001, 84th Session (8/23/05)) available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that a Korean election law barring the publication of polling results 23 days prior to the presidential election does not violate Article 19 as it serves a legitimate aim-to provide the public with a limited period of reflection-and does not punish disproportionately to that aim.

Svetik v. Belarus
(CCPR/C/81/D/927/2000, 81st Session (8/25/04)), available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that punishing a call to boycott a particular election, whether criminally or administratively, violates Article 19, despite the fact that the punishment is provided by law, because it is neither necessary for the respect of the rights and reputation of others nor for the protection of national security or public order.

Laptsevich v. Belarus
(CCPR/C/68/D/780/1997, 68th Session (4/13/00)), available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that arresting a citizen for passing out leaflets violates Article 19 when the State Party can show no compelling justification to protect national security, public order or the respect of the rights and reputations of others.

Guthier v. Canada
(CCPR/C/65/D/633/1995, 65th Session (5/5/99)), available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that the right to take part in the conduct of public affairs pursuant to Article 25 read together with Article 19 implies that citizens should have wide access to information and the opportunity to impart that information about elected bodies and their members.

Park v. Republic of Korea
(CCPR/C/64/D/628/1995, 64th Session (11/3/98)), available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that for a State Party to claim the protection of national security as a justification for infringing upon a citizen's Article 19 right to free expression, it must specify the "precise nature" of the threat to its national security.

Auayom et al v. Togo
(CCPR/C/57/D/423/1990, 57th Session (8/19/96)), available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that the freedom of information and expression are the cornerstones in any free and democratic society. As a result, the Togolese government's imprisonment of a university professor for possessing material critical of the regime's economic, foreign and domestic policy violated Article 19.

Miha v. Equatorial Guinea
(CCPR/C/51/D/414/1990, 51st Session (8/10/94)), available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that when a State Party detains a citizen solely or primarily because of the author's membership in a political party in opposition to the regime in power, it violates the right to free expression protected by Article 19.

Mukong v. Cameroon
(CCPR/C/51/D/458/1991, 51st Session (8/10/94)), available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for proposition that while attempting to safeguard national unity under difficult political circumstances constitutes a legitimate objective pursuant to Article 19, oppressing advocates of multi-party democracy, democratic principles, and human rights is not "necessary" to achieve that legitimate purpose.

Kalenga v. Zambia
(CCPR/C/48/D/326/1988, 48th Session (8/2/93)), available at http://www.unhchr.ch/tbs/doc.nsf

This case stands for the proposition that when a State Party arrests a citizen for promoting campaigns and protests against government policy, it violates Article 19's protection of freedom of speech.

EUROPEAN COURT OF HUMAN RIGHTS

Analysis

The European Court of Human Rights (Court) analyzes potential violations of the right to "receive and impart information" under two scenarios. First, the Court determines whether the government has interfered with this right. If the Court determines that the government has not interfered with the right to "receive and impart information" but instead has failed to take positive action to provide individuals with information, the Court interprets Article 10 narrowly. The Court adheres to the general rule that Article 10 prohibits State Parties from interfering with the dissemination of information while not imposing a positive obligation on the government to collect and disseminate information on its own initiative.

Once the Court determines that a State Party has interfered with this right, it must determine whether the interference is consistent with Article 10. To determine whether a State Party's interference with an applicant's right to "receive and impart information and ideas" is consistent with Article 10, the Court uses a three-part test based on section 2. Section 2 provides exceptions to section 1 for restrictions that "are prescribed by law and are necessary in a democratic society." First, the Court examines whether relevant domestic law mandates such a restriction on the right to receive and impart information. Second, the Court determines whether the restriction is proportionate to a legitimate aim pursued. Finally, the Court analyzes whether the restriction is "necessary in a democratic society," which implies the existence of a "pressing social need" that justifies the restriction.

While the issue is currently pending before the court (Please see *Geraguyn Khorhurd Patgamavorakan Akumb v. Armenia*), Article 10 likely protects the right of domestic monitoring organizations and political competitors to verify the integrity of electronic technology in elections. First, activities such as parallel vote tabulations (PVTs) and conducting voter database audits do not "impose a positive obligation" on states to collect and disseminate information on its own accord, *Guerra and Others v. Italy*, nor does it implicate matters of national security. *Sîrbu and Others v. Moldova*. Therefore, if governments impose restrictions on the collection and dissemination of this type of information, the Court would likely apply the three part test to determine whether the restrictions "are prescribed by law and are necessary in a democratic society."

Even if the relevant domestic law prohibits access to electoral information, such laws would likely fail the remaining two prongs of the three part test. First, denying the public access to information concerning electoral transparency does not serve a "legitimate aim." In effect, denying political contestants and/or nonpartisan domestic monitoring groups access to election information subverts rather than serves a "legitimate aim." Electoral transparency is essential to fulfilling the letter of Article 10. Even if a State Party successfully articulated a "legitimate aim" for such restriction on information, imposing restrictions that undermine transparency in the electoral process is not "necessary in a democratic society" because there is no "pressing social need" that justifies restricting such information. *Radio ABC v. Austria*. Protection of intellectual property and other legitimate private interests therefore would have to be narrowly tailored in order to provide transparency to a maximum practicable extent.

Jurisprudence

Geraguyn Khorhurd Patgamavorakan Akumb v. Armenia (decision pending),
(App. No. 11721/04)

This case addresses whether the alleged failure of an Armenian election authority to provide a domestic election monitoring organization information related to its decision-making processes, as well as campaign contribution data and information about the expenses of certain political parties violates Article 10.

Radio Twist, A.S. v. Slovakia (12/19/06),
(App. No. 62202/00) available at http://hudoc.echr.coe.int

This case stands for the proposition that allowing a civil action against a radio company for broadcasting a taped recording of a private telephone conversation between two high ranking government officials obtained illegally by a third party constituted a violation of Article 10. The Court held that the interference with the company's right to impart information was neither a pressing social need nor propořtionate to the legitimate aim pursued and, therefore, not within the exceptions articulated in Article 10(2).

Sdru eni Jihoceské Matky v. Czech Republic (07/10/06),
(App. No. 19101/03) available at http://hudoc.echr.coe.int

This case stands for the proposition that the refusal by the Czech authorities to grant an NGO access to administrative documents relating to a nuclear power station in Temelin interferes with the right to receive information held by public authorities as guaranteed by Article 10.

Roche v. United Kingdom (10/19/05),
(App. No. 32555/96) available at http://hudoc.echr.coe.int

This case reaffirms the proposition that while Article 10 prohibits governments from restricting the dissemination of information, it does not create a positive obligation to disseminate information on its own motion. The Court found that the British government had satisfied its obligation under Article 10 by releasing the applicant's medical records concerning his exposure to mustard gas testing as a former Royal Engineer upon request and that it had no positive obligation to do so on its own accord.

Sîrbu and Others v. Moldova (6/15/04),
(Apps. No. 73562/01, 73565/01, 73712/01, 73744/01, 73972/01, 73973/01) available at http://hudoc.echr.coe.int

This case stands for the proposition that while governments may not restrict information from a person that others may impart to her, they do not possess positive obligations to disclose to the public any secret documents or information concerning its military, intelligence service or police force as it falls within the exception concerning the interests of national security in Article 10(2). The Court held the Article 10 claim inadmissible since the applicants sought information classified secret within the Ministry of Defence, Ministry of National Security, and Ministry of Internal Affairs.

Guerra and Others v. Italy (2/19/98),
(App. No. 14967/89) available at http://hudoc.echr.coe.int

This case affirms the proposition that Article 10 prohibits government interference with the dissemination of information on matters of public interest but found no violation of Article 10 when applicants alleged the failure of the competent authorities to provide information about the inherent risk and how to proceed in the event of a major accident in a nearby high-risk chemical factory. The Court held that while states must not interfere with the dissemination of information, Article 10 does not impose a positive obligation on the state to collect and disseminate information on its own initiative.

Gaskin v. United Kingdom (7/7/89),
(App. No. 10454/83) available at http://hudoc.echr.coe.int

This case stands for the proposition that Article 10 does not prohibit governments from partially restricting access to a former ward of the state's case-file held by a local social authority relating to his period in care by the Liverpool City Council following the death of his mother when the wider public interest in maintaining an effective child care system by protecting the confidentiality of third parties, such as doctors, police officers, and foster parents, overrides the applicant's private interest. However, the Court held that in restricting such information, the United Kingdom violated Article 8, which protects "the right to respect for his private and family life."

Leander v. Sweden (3/26/81),
(App. No. 9248/81) available at http://hudoc.echr.coe.int

This case stands for the proposition that while Article 10 prohibits governments from restricting information that others may be willing to impart to an individual, it does not confer upon a former Swedish Communist Party member the right to obtain information from a police registry that caused the government to deem him a "security risk" and subsequently exclude him from an employment position within Sweden's national security apparatus. The Court invoked the "national security" exception under section 2 of Article 10.

INTER-AMERICAN COMMISSION AND COURT OF HUMAN RIGHTS

Analysis

Article 13 of the American Convention for Human Rights (ACHR) supports the right of election monitoring organizations to verify the integrity of elections. Article 13 provides for the right to freedom of thought and expression as well as the right to seek, receive and impart information and ideas of all kinds.

The Inter-American system has recognized an explicit right of access to government information within the right to "seek, receive, and impart information." In *Claude Reyes et al v. Chile*,[1] the Inter-American Court of Human Rights (Court) ruled broadly in favor of a "right to access" and it imposed upon OAS Member States a "positive obligation" to "disclose public information so as to encourage democratic debate and control by civil society." *Claude Reyes v. Chile* (36) Therefore, the Inter-American Court would likely find that access to government held electoral information-such as voter registry lists, vote tabulations, and the issues related to the use of electronic technologies made available under Article 13 of the ACHR.

The 2006 ruling in *Claude Reyes et al v. Chile* consolidated the trend towards the expansive view of "freedom of information" that the Inter-American Commission on Human Rights (Commission) had developed over time. The Commission noted that Article 13 is "intended to protect and promote access to information, ideas, and expression of all types, and thus, strengthen the operation of pluralist democracy." In *Baruch Ivcher Bronstein v. Peru* the Commission determined that an OAS Member State violates an individual's right to freedom of expression if that individual is not free to express his own ideas and opinions and is not free to seek and receive information and ideas of all kinds. (Please also see *Francisco Martorell v. Chile*).

The Commission regards freedom of expression as having an "individual and social dimension." As the Commission noted in *Alejandra Marcela Matus Acuna ET AL. v. Chile*, when restrictions on expression occur, the Member State party violates both the individual rights and the collective rights of society as a whole to receive the information. Under Article 13, the State may not restrict information from individuals, unless the restriction is "prescribed by law and necessary for a legitimate aim." (Please see also *Victor Manuel Oropeza v. Mexico*).

[1] Please see case annotations below concerning all decisions noted in the analysis.

The Commission has also stated that disseminating information and knowledge and fostering freedom of expression is "an essential pillar of democratic society and a fundamental condition for progress and the personal development of each individual," and society as a whole. (Please see *Baruch Ivcher Bronstein v. Peru*).

Article 23 of the ACHR provides individuals with the right to free and fair elections. Political contestants and domestic monitoring groups may argue that verifying the integrity of electronic technology in elections is soundly within Article 13's purpose of receiving and imparting information and strengthens the underlying principles of Article 23. Thus, coupled with the ACHR's Article 23 right to free and fair elections, Article 13 requires access to information and provides individuals with the right to determine the integrity of elections through a transparent electoral process.

Jurisprudence

Inter-American Court

Marcel Claude Reyes, et al. v. Chile (09/19/06)[2]

This case stands for the proposition that Article 13 protects citizens' fundamental right to access information. The Court further noted that State Parties possess a positive obligation to disclose government held information, when disclosing such information benefits the public interest, and the burden of proof rests on the State Party to show that any restrictions conform with the Inter-American standards of free expression.

López Álvarez v. Honduras (02/01/06)

This case stands for the proposition that the expression and dissemination of thoughts and ideas "are indivisible." Therefore, when a State Party restricts the possibilities of spreading information, it in fact limits the right to express oneself freely and violates Article 13.

[2] The Chilean Constitutional Court (Court) followed this ruling subsequently in Casas Cordero et al v. the National Customs Service (08/16/07) in holding that the Chilean constitution protects the right of access to information as an integral part of the broader right to freedom of expression. The Court came to this conclusion despite the fact that the constitution does not explicitly articulate such a right. In this case, the Court struck down a statutory provision that provided government officials with excessive discretion to withhold information from the public.

Ricardo Canese v. Paraguay (08/31/04)

This case stands for the proposition that State Parties must take extra efforts to protect the exercise of freedom of expression in the political debate that precedes elections. The Court further noted that the expression of different opinions presented throughout the campaign nourishes the formation of the collective will of the people in that the free exchange of ideas and information is necessary in a democratic society.

Baruch Ivcher Bronstein v. Peru (02/06/01)

This case stands for the proposition that by separating Mr. Ivcher from the control of Channel 2 and excluding the journalists from reporting, the Peruvian government not only restricted their right to circulate news, ideas and opinions, but also affected the right of all Peruvians to receive information, thus limiting their freedom to exercise political options and develop fully in a democratic society.

Olmedo Bustos et el. v. Chile ("The Last Temptation of Christ" Case) (02/05/01)

This case stands for the proposition that Article 13 protects the right and the freedom to express their own thoughts, but also the right and freedom to seek, receive and impart information and ideas of all kinds. The Court further noted that, as a result, freedom of expression has both an individual and a social dimension. First, it requires that State Parties abstain from arbitrarily limiting or impeding expression. In that sense, it is an individual right. Its second aspect, freedom of expression, implies a collective right to receive any information whatsoever and to have access to the thoughts expressed by others.

Inter-American Commission

Nicolas Estiverne v. Haiti (3/24/88),
Case 9855, Resolution No. 20/88 available at
http://www.cidh.org/annualrep/87.88eng/haiti9855.htm

This case stands for the proposition that the declaration of the complainant as persona non grata by the Haitian government and the subsequent barring of his candidacy violated Article 13 (freedom of thought and expression), Article 20 (right to nationality), Article 22 (freedom of movement and residence), Article 23 (right to participate in government) and Article 25 (right to judicial protection) of the ACHR.

GLOSSARY

Audit Trail—Please see Paper Record

Black Box Voting—A term used to refer to the practice of recording votes using a Direct Recording Electronic (DRE) system that does not provide a subsequent paper record of the voter's action.

Candidate Agent—Please see Political Party Agent.

Certification—A process of approving voting equipment for use by determining that the equipment meets a number of pre-approved standards. Certification should be performed by an independent certification authority.

Certification Body—An independent organization that oversees certification of election-related technologies.

Civil Registries—A list of all national citizens maintained by the government. Civil registries are sometimes used as the basis of a voter list, however, they may not contain all information relevant to the voting process.

Controlled Environment—A voting environment that meets the following criteria:

- Representatives of political contestants, nonpartisan domestic election monitoring organizations and other appropriately authorized persons are physically present, and are able to access and observe the environment.
- Election officials are present, in charge of the process and have legal responsibilities and powers to ensure the accuracy and integrity of the electoral process.
- Access (whether physical or virtual) to the environment, including the technological devices, is secured and controlled, and is regulated by a process that is independently auditable and verifiable.

Data Migration—The transfer of data from one database, such as a civil registry, to another, such as a voter database.

Database Accountability—A database design requirement that directs the database to keep records of changes, deletions and insertions for review purposes.

Database Design Requirements—Standards set by the election authorities that inform the specifications used by programmers to build the database.

Database Exports—Electronic versions of some or all of the records in a database intended to be used by another database and thus not "usable" by people.

Database Product (or Report)—An output of a database containing a compilation of information available in a variety of formats intended for the end user.

Denial of Service Attack (DoS Attack)—An attempt to make a computer or computer service inaccessible to its intended users by flooding it with illegitimate requests that overwhelm it, rendering regular use impossible.

Digital Pen—An input device that creates an electronic record while simultaneously marking specialized paper. The device recognizes and records the movement of the pen's point and at the same time leaves an ink trail on the paper. The paper contains microscopic dot patterns that allow the digital pen to recognize the position of the mark on the digital paper. Data stored in the pen can then be uploaded to a computer and software transforms the data into text.

Direct Data Capture (DDC) Device—A device that allows on-the-spot entry of information in an electronic format. This data can be transmitted immediately or at a later date from the device to a centralized repository. DDCs can be used to enter and store voter information during the voter registration process.

Direct Recording—The creation of an electronic voter record in the moment and at the location that the voter (or his or her proxy) submits data to the election officials in accordance with laws and regulations, for example, during voter registration.

Direct Recording Electronic (DRE) Systems—A voting technology that allows the voter to use a keyboard or touch-screen machine to indicate their choice and records that information in electronic format on that device. This is to be distinguished from systems that use a computer interface to print a scanable ballot and do not record voter choices. DRE systems may, however, produce a paper record.

Domestic Nonpartisan Election Monitor—Someone who, as part of a nonpartisan domestic monitoring organization, observes election-day activities and election-related processes to promote electoral integrity and ensure that the rights of voters are respected in the electoral process (sometimes called a "Domestic Observer").

Domestic Observer—Please see Domestic Nonpartisan Election Monitor.

Double Entry—A data entry technique where data is entered by two separate operators and compared for inconsistency. Double data entry is used to ensure quality of data.

Election Officials—National election administrators, regional election officers, voting-site officials and counting officials that administer all election-related processes.

Electoral Competitors—Political parties and candidates competing for elected office and organized groups supporting or opposing propositions presented in referendums.

Electronic Poll Books—An electronic voter list that may have additional functions and abilities, such as connection to a network or central voter database.

End-to-End Test—A test that conducts actual simulations of the complete voting process that will occur on election day.

Elections Markup Language (EML)—A standard for tagging and organizing election information in a way that can be exchanged among hardware, software and service providers, that are built to utilize the EML standard.

Environment—As used in this publication, the broad context or set of circumstances surrounding the use of electronic technologies.

Firmware—Instructions and data which are directly and semi-permanently programmed into the circuitry of an electronic device.

Flat Database—A simple database in which all information is in a single table. Flat databases are easily observed but not practical for managing large amounts of data.

Format of the Voter Record—The style of data organization that determines the possible operations that may be conducted using the database.

Functionality Test—A test that determines if the data entry interface design is appropriate and does not contribute to data entry errors.

Hardware—The mechanical, magnetic, electronic and electrical components making up a computer system. For example: hard discs; screens; keyboards; and wires.

Help America Vote Act (HAVA)—A U.S. law mandating federal standards for functionality, accessibility and security of voting.

Hot Audit—Please see Parallel Test.

Independent Testing Authority—Used in a limited manner in this Guide, to mean an organization that has been qualified by the U.S. Election Assistance Commission to test and/or certify voting equipment.

Indirect Recording—The creation of an electronic voter record at a later date and/or separate location using previously collected voter registration data.

Intellectual Property—A product of the intellect that has commercial value, such as software programming.

International Election Observation—The systematic, comprehensive and accurate gathering of information concerning the laws, processes and institutions related to the conduct of elections and other factors concerning the overall electoral environment, combined with the impartial and professional analysis of such information and the drawing of conclusions and reporting about the character of electoral processes based on the highest standards for accuracy of information and impartiality of analysis. The elements of this activity are delineated in the "Declaration of Principles for International Election Observation and Code of Conduct for International Election Observers" endorsed by over 30 international organizations and available at www.ndi.org.

International Election Observation Mission (or Delegation)—The organized efforts of intergovernmental and international nongovernmental organizations and associations to conduct international election observation.

International Election Observer—A foreign national individual, who as part of an international election mission or delegation engages in international election observation

International Organization for Standards—A prominent institution that develops standards for the information technology (IT) field.

Kiosk Voting—Internet voting that is conducted at any voting center within a voter's electoral district on designated computers that are controlled and monitored by election officials.

Load Test—A test to determine how well electronic equipment can perform under the level of usage that can be expected on election day.

Nonpartisan Domestic Election Monitoring Organization (or Group)—A domestic organization that, on the basis of political impartiality, monitors election processes to promote electoral integrity and ensure that the rights of voters are respected in the electoral process. Such an organization is comprised of nationals of the country where the voting is taking place and does not support or detract from any competitor in an election.

Nonpartisan Domestic Election Monitor (or Observer)—A national of a country who monitors election processes, including observing procedures inside polling places, as part of a nonpartisan domestic election monitoring organization.

Nonpartisan Domestic Election Observer Organization (or Group)—Please see Nonpartisan Domestic Election Monitoring Organization.

Optical Character Recognition (OCR) Devices—Machines that capture data by scanning and recognizing hand-written letters and numbers rather than pre-determined marks.

Optical Mark Recognition (OMR) Devices—Machines that capture data by scanning and recognizing a set of predetermined marks, such as filled-in circles or completing arrows that point to specific electoral competitors.

Paper Record—A printed record of the voter's electronic vote (sometimes called a Paper Trail, Audit Trail or Voter Verifiable Paper Audit Trail VVPAT).

Polling Day Test—Please see Parallel Test.

Paper Trail—Please see Paper Record.

Parallel Test—A test that is conducted on voting day in which actual voting equipment is excluded from the voting, isolated, tested and monitored. Parallel tests are designed to "convince" the machine that it is being used in an actual election environment to determine how it would behave in an actual election.

Pilot Test—A test of the electronic voting systems in an actual electionenvironment in a limited number of locations. Unlike a parallel test, this equipment is actually used in conducting the election. During a pilot test voters may be given the option of using a paper ballot rather than the electronic voting equipment.

Political Contestants—Please see Electoral Contestants.

Political Party Agent—A partisan representative that observes election-day activities and election-related processes to ensure the rights of particular candidates and/or political parties are respected in the electoral process (sometimes called Scrutineers, Proxies, Party Poll Watchers).

Poll-Site Internet Voting—Internet voting that is conducted at a voter's polling-site on designated computers that are controlled and monitored by election officials.

Poll Watcher—Please see Political Party Agent.

Primary Key—Please see Unique Identifier.

Primary Voters List Database Data—Information on individual voters that is required by electoral law.

Proxies—Please see Political Party Agent

Punch Card System—A method of voting which requires voters to punch a hole in the paper ballot to indicate their choice.

Relational Database—A complex database intended to increase efficiency in computing and data manipulation processes in which sets of data are stored in different tables with relationships between each table.

Remote Internet Voting—Internet voting from any computer (for example, a home computer), rather than specific computers under the control of a polling authority, as in Poll-Site Internet Voting or Kiosk Voting.

Scrutineer—Please see Political Party Agent.

Secondary Voters List Database Data—Information that is not required by the legal framework but is useful in the overall administration of the electoral process. For example: assigned polling station; information on temporary residence; and assigned electoral district.

Security Test—A test that aims to expose the vulnerabilities of the voting systems from threats that come from outside the election authorities and from inside the election authorities.

Smart (Chip) Card—A card with a built-in microprocessor and memory used to store, provide and process information.

Smart Card Reader—A device that reads the data saved on a Smart (Chip) Card and serves to authenticate the identity of a voter.

Software—Written coded commands that tell a computer what tasks to perform.

Technical Requirement—Specification for election-related technologies that are developed by the electoral administration.

Touch Screen—A user interface where voters indicate choices by touching them on a computer screen rather than using a keyboard or mouse.

Uncontrolled Environment—A voting environment that exhibits one or more of the following characteristics:

- Representatives of political contestants, nonpartisan domestic election monitoring organizations and other appropriately authorized persons are not physically present, and/or are unable to access and observe the environment.

- Election officials are not present, are not in charge of the process or do not have legal responsibilities and powers to ensure the accuracy and integrity of the electoral process.

- Access (whether physical or virtual) to the environment, including the technological devices, is not secured and controlled, and is not regulated by a process that is independently auditable and verifiable.

Unique Identifier—An entry in a database that serves to unmistakably identify a record; a Voter ID number can be a unique identifier in a table of voters, if every voter has exactly one Voter ID, and every Voter ID matches exactly one voter (also called Primary Keys).

Usability Test—A test that determines how easily and intuitively a voter or polling official can operate a piece of equipment without confusion and mistakes.

Voter Database—A list of eligible voters that may contain personal information relevant to the voting process (for example, the voter's address).

Voter List—The list of eligible voters entitled to vote at a specific polling station, which can appear as an Electronic Poll Book or paper record.

Voter's Record—Information located within a database that relates to an individual voter.

Voter Registry—The national list of all eligible voters, which can take the form of one unified database or a compilation or series of databases from governmental subdivisions.

Voting Server—An electronic unit that records electronic votes at a specific polling station.

Voter Verifiable Paper Audit Trail (VVPAT)—Please see Paper Record.

SELECTED NDI PUBLICATIONS ON ELECTION MONITORING

NDI Handbook on How Domestic Organizations Monitor Elections: An A to Z Guide (1995). This handbook provides a comprehensive overview of how to organize a nonpartisan domestic election monitoring effort. It covers: planning and organizational issues; recruiting, training and logistical issues in building a communications network for reporting; various subjects to monitor in the pre-election, election day and post-election periods; and considerations for how the organization and skills developed through monitoring efforts can be applied to non-election activities. The Guide is designed for election monitoring by civic organizations but can be used by political parties in designing their efforts to ensure electoral integrity and protect their vote.

Building Confidence in the Voter Registration Process: An NDI Monitoring Guide for Political Parties and Civic Organizations, by Richard L. Klein and Patrick Merloe (2001). This voter registration monitoring guide addresses: the role of voter registration and the principle types of voter registration systems; why it is important for political parties and civic organizations to monitor these systems; and specific techniques for monitoring processes for collecting names, creating a voter registry and polling station voter lists, correcting errors in the lists and use of the lists on election day.

Media Monitoring to Promote Democratic Elections: An NDI Handbook for Citizen Organizations, by Robert Norris and Patrick Merloe (2002). This handbook takes a step-by-step approach to media monitoring. It covers: the importance of determining who controls the media and the difference between state-controlled versus private and broadcast versus print media; issues to address in deciding what media and what subjects to monitor; planning and organization of a media monitoring project; monitoring methodology, including specific instructions for monitoring different types of media; and considerations for the presentation of findings and recommendations.

The Quick Count and Election Observation: An NDI Handbook for Civic Organizations and Political Parties, by Melissa Estok, Neil Nevitte and Glenn Cowan (2002). This handbook addresses importance of developing systematic observation of vital election day processes, including the quality of voting, ballot counting and tabulation of election results, as well as the projection of electoral results with extremely narrow margins of error and high degrees of statistical confidence. It covers planning and organizational issues, recruiting and training, communications systems, developing a random statistical sample of polling stations for rapid and exacting analysis, analytical techniques and the considerations for the release of quick count findings. The handbook is designed for civic organizations but can easily be used by political parties. It also is designed for use by civic organizations that decide not to undertake projection of electoral results. As an organizer's guide, it reviews many of the issues covered by NDI's 1995 "A to Z" handbook.

Promoting Legal Frameworks for Democratic Elections: An NDI Guide for Developing Election Laws and Law Commentaries, by Patrick Merloe (forthcoming 2008). This Guide addresses the importance of developing legal frameworks that promote democratic elections; why it is important for political parties, civic organizations and others to analyze the strengths and weakness of existing and proposed laws affecting election processes; the importance of developing an open and inclusive political process to address those laws so that political competitors may agree on the "rules of the game" and the public can develop confidence in the process. The Guide presents the main issues to examine when evaluating the legal framework and over 300 questions to consider, as well as sources of international law on the subject and samples of NDI election law commentaries.

In addition to these materials, NDI has produced over 300 reports, papers and statements concerning ways in which to promote democratic elections generally and concerning the election process within specific countries. See NDI's website: www.ndi.org "Access Democracy" and "Global Programs/Elections and Political Processes" for more information about these and other NDI publications.

WHAT IS THE SIGNIFICANCE OF ELECTRONIC TECHNOLOGIES IN ELECTIONS?

Electronic technologies are increasingly important to election processes around the world. Without doubt they will be used ever more broadly in future elections, and the integrity of elections will increasingly depend on their proper functioning.

WHY SHOULD POLITICAL PARTIES AND NONPARTISAN CITIZEN GROUPS MONITOR THE ROLE OF ELECTRONIC ELECTORAL TECHNOLOGIES?

The introduction of electronic technologies into voting and election results tabulation is not a simple replacement of classic ballot boxes and ballot papers with electronic machines. It requires restructuring of electoral administration in practically every critical aspect and creates a whole new set of relations between election management bodies, certification bodies, vendors and various state institutions. Introducing electronic technologies into voter registration and other processes also creates important issues for electoral integrity. The reasons for introducing electronic technologies therefore must be clear and compelling, and the role of the technologies must be scrutinized.

WHAT IS THE BASIS UPON WHICH PARTIES AND CITIZEN GROUPS SHOULD ACCESS INFORMATION ABOUT AND DECISIONS CONCERNING WHETHER TO EMPLOY ELECTRONIC TECHNOLOGIES IN ELECTIONS?

Citizens have a fundamental right to genuine elections, manifested in the right to vote and to be elected, and citizens have a right to seek and impart information that informs the public concerning whether elections are genuine, somehow tainted or fraudulent. Monitoring elections is a matter of exercising fundamental rights that form part of the core of sovereignty, which ultimately belongs to and derives from the people of a country. All of these rights come into play when the role of electronic technologies in elections is evaluated.

National Democratic Institute for International Affairs
2030 M Street, N. W., Fifth Floor
Washington, D.C. 20036-3306, USA
Tel +1 202 728 5500
Fax +1 202 728 5520
E-mail contactndi@ndi.org
Website http://www.ndi.org

ISBN: 978-1-880134-36-8