Implementing and Overseeing
Electronic Voting and Counting Technologies

Introduction and Overview Section

Lead Authors

Ben Goldsmith
Holly Ruthrauff

NDI
NATIONAL
DEMOCRATIC
INSTITUTE

IFES
International Foundation
for Electoral Systems

USAID
FROM THE AMERICAN PEOPLE

This publication is made possible by the generous support of the American people through the United States Agency for International Development (USAID) under Award No. DFD-A-00-08-00350-00. The opinions expressed herein are those of the authors and do not necessarily reflect the views of USAID or the United States Government.

Requests for permission should include the following information:

- A description of the material for which permission to copy is desired.
- The purpose for which the copied material will be used and the manner in which it will be used.
- Your name, title, company or organization name, telephone number, fax number, e-mail address and mailing address.

Please send all requests for permission to:

International Foundation for Electoral Systems
1850 K Street, NW, Fifth Floor
Washington, D.C. 20006
Email: editor@ifes.org
Fax: 202.350.6701

National Democratic Institute
for International Affairs
455 Massachusetts Avenue NW, 8th Floor
Washington, D.C. 20001
Email: kgest@ndi.org
Fax: 888.875.2887

Disclaimer: The author's views expressed in this publication do not necessarily reflect the views of the International Foundation for Electoral Systems, the National Democratic Institute and the U.S. Agency for International Development.

ISBN: 978-0-9910142-0-0

ABOUT IFES

The International Foundation for Electoral Systems (IFES) supports citizens' right to participate in free and fair elections. Our independent expertise strengthens electoral systems and builds local capacity to deliver sustainable solutions.

As the global leader in democracy promotion, we advance good governance and democratic rights by:

- Providing technical assistance to election officials
- Empowering the underrepresented to participate in the political process
- Applying field-based research to improve the electoral cycle

Since 1987, IFES has worked in over 135 countries – from developing democracies, to mature democracies. For more information, visit www.IFES.org.

ABOUT NDI

The National Democratic Institute (NDI) is a nonprofit, nonpartisan, nongovernmental organization that responds to the aspirations of people around the world to live in democratic societies that recognize and promote basic human rights.

Since its founding in 1983, NDI and its local partners have worked to support and strengthen democratic institutions and practices by strengthening political parties, civic organizations and parliaments, safeguarding elections, and promoting citizen participation, openness and accountability in government.

With staff members and volunteer political practitioners from more than 100 nations, NDI brings together individuals and groups to share ideas, knowledge, experiences and expertise. Partners receive broad exposure to best practices in international democratic development that can be adapted to the needs of their own countries. NDI's multinational approach reinforces the message that while there is no single democratic model, certain core principles are shared by all democracies.

The Institute's work upholds the principles enshrined in the Universal Declaration of Human Rights. It also promotes the development of institutionalized channels of communications among citizens, political institutions and elected officials, and strengthens their ability to improve the quality of life for all citizens. For more information about NDI, please visit www.ndi.org.

ACKNOWLEDGMENTS

As a growing number of countries at various stages of development consider the use of electronic technologies in electoral processes, they face opportunities and challenges. This Guide was prepared by IFES and NDI to help election authorities, civil society, political parties and other stakeholders engage in inclusive, transparent and accountable decisionmaking, implementation and oversight of electronic voting and counting technologies. It is also intended to help inform international and local democracy and governance support communities in designing and implementing effective electoral assistance programs in countries adopting or considering the use of electronic technologies.

The Guide is the product of close collaboration between IFES and NDI, each with complementary areas of expertise. It reflects IFES' 25 years of experience – in over 135 countries – of strengthening electoral systems and building local capacity to deliver sustainable electoral solutions by providing technical assistance to election officials; empowering the underrepresented to participate in political processes; and applying field-based research to improve the electoral cycle. It also draws from NDI's 30 years of experience in international election observation and in supporting the efforts of political parties and nonpartisan citizen election monitoring groups in more than 125 countries to promote electoral integrity and popular political participation.

Ben Goldsmith, IFES Electoral Technology Advisor, and Holly Ruthrauff, formerly with NDI's Elections and Political Processes team, were the authors of the Guide. Ben primarily concentrated on issues related to the design and implementation of electronic technologies, while Holly focused mainly on issues related to the oversight of such technologies. Ben has 15 years of experience advising and managing election administration projects in post conflict and developing democracies. Ben has helped to conduct elections and provided technical assistance in various countries including Afghanistan, Bosnia, Iraq, Kosovo, Kenya and the United Kingdom. He is an expert on electronic voting and has advised electoral officials in several countries on the design and use of these technologies. He is the author of Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies and was the lead IFES researcher on the evaluation of various facets of the internet voting pilot in Norway. Holly has more than 15 years of experience with electoral assistance and observation. She has organized observer missions, developed more than 10 publications and handbooks for both international and domestic observers, and provided technical assistance to domestic observer efforts around the world through her work at NDI, Election Reform International Services (ERIS) and the Organization for Security and Co-operation in Europe's Office for Democratic Institutions and Human Rights (OSCE/ODIHR).

Rakesh Sharma, IFES Director of Applied Research, and Michael McNulty, NDI Senior Program Manager in Elections and Political Processes, were the editors of the Guide and managers of its publication. Rakesh and Michael also drafted elements of the Guide. Pat Merloe, NDI Senior Associate and Director of Electoral Programs, provided guidance and editing throughout the drafting process. NDI Program Assistant Sunila Chilukuri and IFES Research Coordinator Ayesha Chugh supported the editors and played important roles in text revisions and additions.

NDI's Michael McNulty and IFES' George Carmona conducted the Philippines case study and drafted the report. The Brazil case study was conducted and drafted by NDI consultant Ambassador Ecaterine Siradze-Delaunay and IFES consultant F. Daniel Hidalgo. The Netherlands case study was researched and drafted by IFES consultant Susanne Caarls and Guide co-author Holly Ruthrauff.

IFES and NDI express appreciation for the valuable recommendations provided, in their personal capacities, by noted electronic voting and counting technologies experts Vladimir Pran, Democracy Reporting International; Jonathan Stonestreet; Rokey Suleman; Ole Holtved; Ronan McDermott, and Mike Yard.

The writing, editing, production and publication of this Guide were made possible by a grant from the United States Agency for International Development (USAID). We hope that those who use this Guide will contact IFES and NDI with any comments, suggestions and requests.

William R. Sweeney, Jr., President & CEO, IFES and
Kenneth Wollack, President, NDI

Implementing and Overseeing Electronic Voting and Counting Technologies

LIST OF ACRONYMS

Center for People Empowerment in Governance	CenPEG
Council of Europe	CoE
COMELEC Advisory Council	CAC
Commission on Elections	COMELEC
Direct Recording Electronic	DRE
Electronic Ballot Printer	EBP
Election Commission of Pakistan	ECP
Election Management Body	EMB
Electronic Voting Machines	EVM
Frequently Asked Questions	FAQ
Help America Vote Act	HAVA
Information and Communications Technology	ICT
Information Technology	IT
International Foundation for Electoral Systems	IFES
International Republican Institute	IRI
International Standards Organization	ISO

Internet Service Provider	ISP
La Oficina Nacional de Procesos Electorales	ONPE
National Citizens' Movements for Free Elections	NAMFREL
National Democratic Institute	NDI
National Software Reference Library	NSRL
Nederlandse Apparatenfabriek NV	NEDAP
New Voting Technologies	NVT
Ordem dos Advogados do Brasil	OAM
Organization for Security and Cooperation in Europe	OSCE
Organization of American States	OAS
Optical Character Recognition	OCR
Optical Mark Recognition	OMR
Parish Pastoral Council for Responsible Voting	PPCRV
Precinct Count Optical Scan	PCOS
Request for Proposals	RFP
Technical Guidelines Development Committee	TGDC
Toegepast Natuurwetenschappelijk Onderzoek	TNO
Tribunal Superior Eleitoral	TSE
U.S. Election Assistance Commission	EAC
Voluntary Voting System Guidelines	VVSG
Voter-Verified Paper Audit Trail	VVPAT
Web Accessibility Initiative	WAI

HOW TO USE THIS MANUAL

This manual has been designed to provide a critical source of information on electronic voting and counting technologies for specialists in Democracy & Governance, as well as Election Management Bodies (EMBs), civil society organizations (CSOs), political parties and other key stakeholders engaged in electoral processes around the world. The manual provides a guide to the challenges, opportunities and considerations involved in decision-making, design and implementation of the technologies to assist EMBs as they move through the process or seek to understand it better, as well as to help other stakeholders, including civil society and electoral contestants, understand how to engage in and monitor these processes.

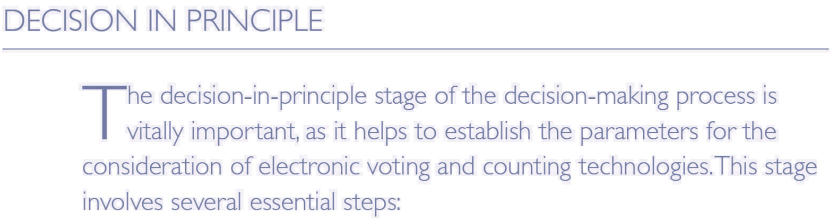
IFES and NDI have designed the manual to provide both a brief primer as well as detailed exposition on the key issues related to electronic voting and counting. As such, the manual is adaptable for use by readers at different levels of engagement with these technologies. The guide below indicates how two different types of readers can use this manual.

FOR READERS INTERESTED ONLY IN A BRIEF PRIMER ON ELECTRONIC VOTING AND COUNTING TECHNOLOGIES

- The Overview chapter (Chapter 1) provides a brief introduction to the main issues involved in the effective design, implementation and oversight of these technologies. The chapter has been written to provide enough coverage of these issues so that the reader can gain a solid understanding of these issues without the need to read the detailed descriptions of each issue. For readers that would like to explore a particular issue or process in more depth, each issue covered in Chapter 1 has footnotes that guide the reader to specific subsections and page numbers of Chapter 2 that address the issue in more detail.

- Chapter 2 addresses the key issues in much more depth by outlining in a chronological manner the processes of deciding on, designing, implementing and observing electronic voting or counting projects. While it is more detailed than Chapter 1, the general reader can still use two specific design elements of this chapter to quickly gain a general understanding of the most important points, as explained below.

    1. Each of the key issues related to electronic voting and counting is addressed in subsections in Chapter 2. For each subsection, a summary of the discussion in this subsection is provided in brief text that is formatted as below:



DECISION IN PRINCIPLE

The decision-in-principle stage of the decision-making process is vitally important, as it helps to establish the parameters for the consideration of electronic voting and counting technologies. This stage involves several essential steps:

2. Additionally, at the end of each subsection, a list of key considerations is provided for both EMBs and oversight groups. This quick reference list can be used by EMBs, oversight groups, or a general audience to identify the questions that should be considered for the issue highlighted in the preceding subsection. This checklist is formatted as below:

KEY CONSIDERATIONS:
CHALLENGES AND RECOUNTS

FOR IMPLEMENTING BODIES

☑ Does the legal framework clearly define who can lodge a challenge against the results, to which body the challenge should be lodged, in what circumstances an investigation will be conducted and in what situation a recount of the results will occur?

FOR READERS INTERESTED IN A MORE DETAILED UNDERSTANDING

- Chapter 2 addresses each of the key issues related to electronic voting and counting technologies in much more depth than Chapter 1. Each of the key issues related to electronic voting and counting is addressed in sub-sections in Chapter 2.

- For EMBs and oversight groups engaged in the implementation or oversight of these technologies, there is a checklist of important questions that should be considered by both EMBs and oversight groups for the issues addressed in each of the Chapter 2 subsections (please see Example 2 above). EMBs and oversight groups can use these checklists to ensure that they are considering the significant aspects of each phase of the decisionmaking, design, implementation and evaluation of electronic voting and counting technology projects.

- Chapter 2 also provides text boxes with brief case studies of how a particular issue related to electronic voting and counting technologies was addressed in practice. These case studies provide the reader with practical examples and lessons learned that can help inform their thinking on key issues.

- Appendices 1 – 3 contain detailed cases studies on the use of electronic voting and/or counting technologies in the Philippines, Netherlands, and Brazil. These case studies provide descriptive narratives on how these countries addressed many of the issues detailed in the manual. These case studies also give the reader an appreciation of the challenges and complexity involved in the design, implementation and monitoring of e-voting and counting technologies, as well as the many lesson learned that have emerged from these three countries' experiences.

- Appendix 4 provides a list of additional resources on electronic voting and counting technologies.

CONTENTS

2.2
BUILDING THE SYSTEM FOR E-VOTING OR E-COUNTING 101

2.3
IMPLEMENTING ELECTRONIC VOTING OR ELECTRONIC COUNTING IN AN ELECTION 153

CHAPTER 1 OVERVIEW OF ELECTRONIC VOTING AND COUNTING TECHNOLOGIES

Traditional electoral procedures involving casting and hand counting paper ballots have come to dominate elections since their introduction in the mid-19th century. Technology increasingly offers new mechanisms for conducting traditionally-manual processes, and elections are no exception. There are many different technologies that can be used to support the electoral process. This guide will focus on electronic technologies that assist voting and the subsequent counting of votes.

The current discourse on these technologies includes such terms as electronic voting machines, e-voting, e-enabled elections, new voting technologies (NVT), remote voting, precinct count optical scanning (PCOS), and e-counting. This array of terminology relates to different technological solutions. The field of election technologies concerning voting and counting is developing, and the conceptual framework is still emerging. Therefore, it is easy to find the same terms being used in different ways in different countries or regions, which can create confusion.

When discussing electronic voting, two separate, but sometimes related technologies are generally referred to – electronic voting and electronic counting. The traditional paper-based voting system consists of a voter manually marking the paper ballot and then the ballot being counted by hand by election officials. In elections using electronic voting or counting technologies, one or both of these processes are automated electronically.

FRAMEWORK FOR THE GUIDE AND OVERVIEW SECTION

This guide and the overview section will focus on the most commonly-used electronic voting and counting technologies: namely, non-remote EVMs used in the supervised environment of the polling station and electronic counting machines. Much that is discussed in the guide and overview is also relevant for remote electronic voting from unsupervised environments. However, the use of such remote voting technologies presents complex challenges in implementation. This is especially the case for remote voter identification and authentication, audit mechanisms, data secrecy and security. At the same time, the logistics of implementing remote voting may be much simpler than for non-remote voting.

The overview section of this guide is meant to be useful for election administrators, electoral stakeholders, including oversight actors and those in the donor community who might be considering the merits of introducing electronic voting and/or counting technologies in a country. It is important to note that electronic voting and counting technologies can create new and important stakeholder groups in the electoral process. These groups include technology vendors, who often play a very important role in the election, certification bodies, academia and IT experts. All of these groups may play a key role in providing, checking or overseeing the use of new technologies.

This overview provides an introduction to the key considerations and themes to be assessed when contemplating the use of electronic voting and counting technologies – issues that will be explored in more detail in the next section of the manual. These include practical considerations related to the use of electronic voting and counting technologies, such as the legality of using such technology under existing legal frameworks; timeline for consideration and implementation; sustainability of the technology; integrity of elections using this technology; trust in the technologies; and the security of the technologies and data. Key issues also include normative aspects of the electoral process, such as inclusiveness, transparency, accountability and ballot secrecy in elections when using electronic voting and counting technologies. Finally, a section is included that attempts to summarize what can be characterized as emerging electoral standards related to the use of electronic voting and counting technologies.

Consideration of the use of electronic voting or counting technologies is an incredibly complex topic. In highlighting the many issues that need to be assessed when considering the use of these technologies, it is hoped the overview will provide electoral stakeholders with the tools needed to give electronic voting and counting technologies the due consideration they deserve.

WEIGHING THE BENEFITS AND CHALLENGES

The increasing adoption of these new technologies in some regions comes in part from the recognition that technology may offer benefits over traditional methods of voting and counting. Such benefits may include:

- eliminating the cost and logistics involved with paper ballots; improved voter identification mechanisms;
- improved accessibility to voting;
- easy conduct of complex elections; increase in voter turnout;

- eliminating invalid ballots;
- faster, more accurate and standardized counting of ballots; and
- prevention of certain forms of fraud.[1]

However, the use of new technologies brings new challenges. These challenges may include:

- lack of transparency;
- negative impact on confidence in the process;
- confusion for the illiterate or uneducated voters on process;
- need to conduct widespread voter education, how to use it and its impact on the process;
- difficulties in auditing results;
- secrecy of the ballot;
- security of the voting and counting process;
- cost of introducing and maintaining the technology over the lifecycle of the equipment;
- potentially losing control over the process to outside technology vendors; recruitment of staff with specialized IT skills;
- added complexity in the electoral process and the ability of the EMB to deal adequately with this complexity; and
- consequences in the event of equipment or system malfunction.

In addition to these challenges, it is also vitally important that electronic voting and counting systems are implemented in such a way as to not violate core electoral standards.

The challenges need to be carefully considered and balanced against anticipated benefits when deciding whether to use such technologies for elections.

[1] While the use of electronic voting and counting technologies can serve to prevent some kinds of fraud, it also opens up the possibility for new kinds of fraud. The use of these technologies should certainly not be seen as the means by which fraud is eliminated entirely from the electoral process.

The relevance of each of these possible advantages and disadvantages will vary from country to country, as will the challenges and issues presented by the existing system being used for elections. Therefore, there is no one answer on the appropriateness of using election technologies. Rather, each electoral jurisdiction will need to fully assess possible advantages and disadvantages to see whether using such technologies is beneficial.

Because the decisions on these matters will profoundly affect voters' confidence in electoral results, the assessment should be made through a broadly consultative process and be based on equally broad consensus. Without such inclusive and transparent deliberations, suspicions that often exist in competitive political environments may undermine the decision to use electronic voting or counting systems, and erode the legitimacy of the electoral process.

ELECTRONIC VOTING

In electronic voting, an electronic device is used by the voter to make and record their ballot choice. The choice is either recorded on the machine itself, or the machine produces a token on which the choices are recorded. The token is then placed in a ballot box (internal or external to the machine). The token can be a printout of the ballot choice, or the ballot choice can be recorded on another medium. For example, in Belgium a magnetic card has been used for this purpose. Electronic voting devices include voting machines placed in polling stations (sometimes referred to as direct recording electronic (DRE) voting machines), SMS voting and Internet voting.

There are two other distinctions (Figure 1) to be made when it comes to electronic voting machines, which are also important in implementation:

- Remote and non-remote voting machines
- Supervised and unsupervised environments

FIGURE 1 – KEY DISTINCTIONS FOR IMPLEMENTATION OF ELECTRONIC VOTING

- Remote Voting: An electronic device used to cast a vote, and then transmits the ballot choice across a communication channel. The ballot choice is then recorded in a central location, e.g. Internet voting and SMS voting.

- Non-Remote Voting Machines: An electronic device used to cast a vote, which records the ballot choice made on a local medium, e.g. the machine itself or a printed ballot.

- Supervised Environments: A voting machine used in a location where election staff is present to manage the voting process, such as a polling station.

- Unsupervised Environments: A voting device used in a location where no election staff is present to manage the voting process, such as any computer the voter uses for Internet voting.

It is possible to combine remote voting with supervised environments, for example, Internet voting computers set up in polling stations. This allows polling staff to verify the identity of voters by using voter lists before allowing them to vote, and to ensure secrecy of the vote – two significant challenges with other forms of remote voting.

ELECTRONIC COUNTING

Electronic counting involves the use of a device to count votes cast. The most common such counting machines use scanning technologies, such as optical mark recognition (OMR) or optical character recognition (OCR), to count ballots that have been completed manually by voters. This broad category of technologies also includes punch card counting machines and electronic ballot boxes used to count electronic records on tokens produced by electronic voting machines.

Electronic voting and electronic counting technologies, while representing different stages of the electoral process, can be combined, as is done by the DRE voting machine. It not only enables the voter to make his or her ballot choices, but also records them directly on the machine and produces results on the machine at the end of the voting process.

It is not mandatory, however, to combine the technologies. It is possible to have electronic voting without electronic counting and electronic counting without electronic voting. It is also possible to have voting and counting on entirely different devices, whereby a voting machine is used to produce tokens with the ballot choices made and a separate counting device tallies the votes recorded on these tokens.

COMMON ELECTRONIC VOTING AND COUNTING TECHNOLOGIES

There are many different electronic voting and counting technologies being used globally. The variety of technologies used makes it difficult to easily categorize them. The most common types of technologies are identified are as follows:

DIRECT RECORDING ELECTRONIC (DRE) SYSTEM

Often referred to as electronic voting machines (EVMs), DRE systems use a keyboard, touch-screen, mouse, pen or other electronic device to allow a voter to record his or her vote electronically. DREs are used in non-remote, supervised locations (polling stations). The DRE system captures the voter's choices and stores an electronic record of their vote in the machine. The data captured by each individual DRE unit is then transmitted by either electronic means (i.e., Internet, cellular network or memory card) or manually (i.e., by printing the results from each machine and tabulating them) to capture the total number of votes cast for specific parties or candidates. DRE systems may or may not produce a paper record to allow the voter to verify their voting choices. This paper record, also called a voter verified paper audit trail (VVPAT), has been implemented in multiple ways in different countries.

DREs with VVPATs are perceived to have an advantage over DREs without VVPATs, because paper trails provide greater transparency to the voter, which can engender greater trust. DRE voting without VVPATs, which is a form of "black box voting," does not provide sufficient means for voters and stakeholders to verify votes have been accurately recorded. DREs with VVPAT provide election management bodies (EMBs) and those who provide oversight with the potential to audit the results or conduct a meaningful recount. However, DREs with VVPATs also introduce greater technological complexity into the process, which may result in greater challenges for EMBs in terms of reliability of the machine, training for staff and sustainability of the overall system.

DREs can be confusing for voters who are not familiar or comfortable with information technology (IT). However, in some contexts, voters may benefit from a streamlined presentation of ballots on DREs in complicated voting systems – with or without VVPAT – where a paper ballot design may lead to a significant number of spoilt and invalid ballots. It is important to note that ballot design may be a challenge no matter which voting system is used.

ELECTRONIC BALLOT PRINTERS (EBPS)

EBPs are similar to DREs, in that the voter uses a DRE-type interface for the act of making voting choices. However, unlike DREs, an EBP does not store vote data. Instead, it prints out a paper receipt or produces a token containing the voting choice(s). The voter then takes this receipt or token and places it into the ballot box, which may be electronic and automatically count the vote.

EBPs are considered easier to understand and more user-friendly for the voter than DREs, as they split the actions of marking the voter's choice and casting the ballot in the same way a voter marks and casts a ballot in traditional paper voting. The first machine (ballot printer) only marks the voter's choice, but does not record the vote, while the second machine (ballot scanner or "electronic ballot box") only records and tallies the votes. Like the DREs with a VVPAT, the voter can verify their vote, either on a printed paper ballot or by inserting the ballot token into another voting machine. There is the possibility of a recount of the paper receipt or token if the electronic results are challenged or audited. However, because they involve two separate machines, EBP systems may entail higher costs, require greater IT capacity from EMBs and encounter more challenges to ensuring sustainability than other systems.

OPTICAL MARK RECOGNITION (OMR)

OMR counting machines combine aspects of paper ballot voting with electronic counting. The voter uses a pen or pencil to mark his or her choices (usually by filling in an oval or connecting an arrow) on a special machine-readable paper ballot. The ballot is then read by an OMR machine that tallies votes using the marks made by the voter. There are two methods used to tally votes using an OMR system. The tallying can be done at the polling station with the voter feeding the ballot into the machine, or votes can be tallied at a central/regional counting facility where votes from more than one polling station are counted.

OMR systems provide greater ability for recounts than DREs without VVPAT. Generally, OMR systems cost less than DREs and may put less strain on EMBs in terms of sustainability of the systems. On the other hand, these systems entail significant focus on details such as ballot design, type of ink used, paper stock thickness and other factors that may inhibit the ability of OMR machines to accurately count votes. OMR machines are always used in a supervised, non-remote location.

INTERNET VOTING SYSTEM

In an Internet voting system, the voter casts his or her vote using a computer with access to the Internet. Internet voting generally takes place in an unsupervised, remote location, from any computer that has Internet access, such as a voter's home or work. It can also take place in supervised, non-remote locations if, for example, electoral authorities provide Internet kiosks at polling stations.

Convenience and greater access are the two key benefits cited for a move to Internet voting. In terms of access, Internet voting is perceived to provide access to specific populations that may have difficulty in voting at polling stations, e.g. persons with disabilities and eligible voters living outside a country. However, Internet voting from unsupervised locations requires voting systems to place a greater emphasis on voter authentication to avoid impersonation, and also elicits concerns about the secrecy of the ballot. Internet voting also raises security concerns with regard to hacking into the system or other ways of corrupting data. Similar to DREs without VVPAT, Internet voting also raises questions about verifiability, may not allow recounts and presents challenges for adjudication of electoral complaints. Finally, transparency in Internet voting systems may be compromised to an even greater extent than with DREs. Such challenges are not beyond solution, but to date remain significant.

ELECTRONIC VOTING AND COUNTING AROUND THE WORLD

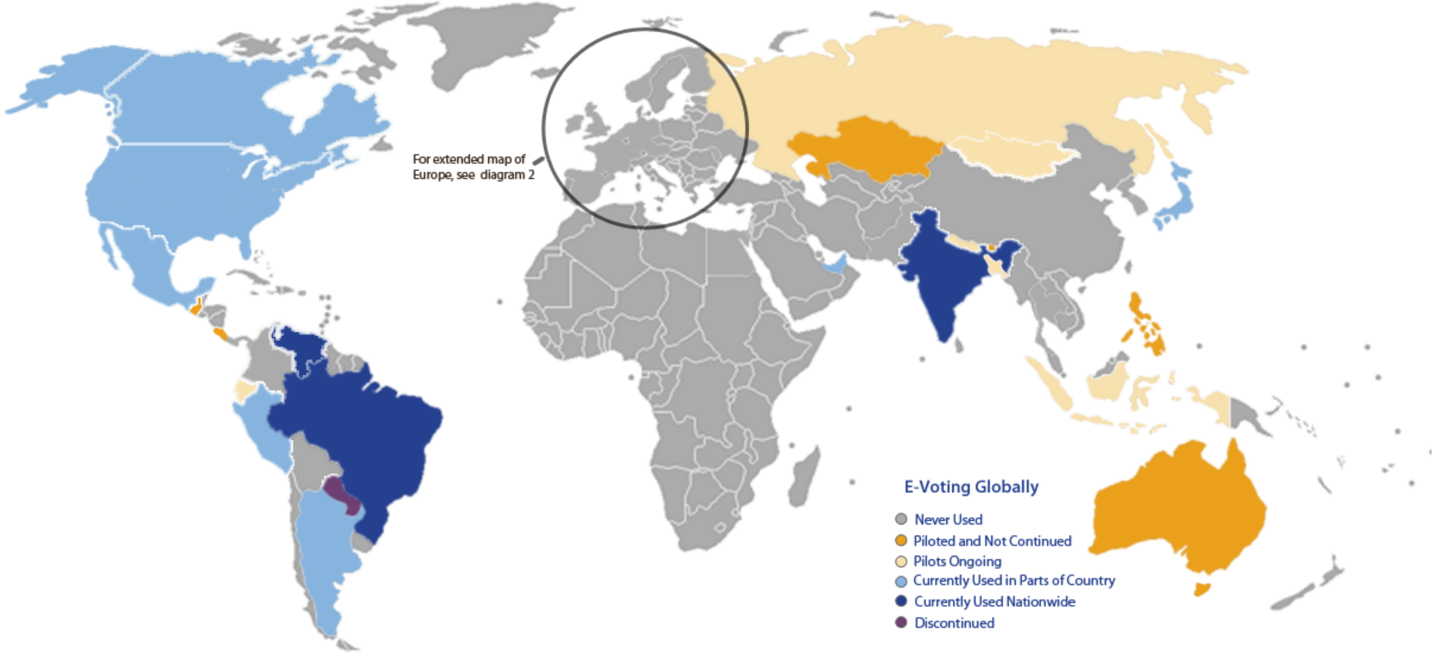
This guide will use the terminology "electronic voting and counting technologies." As already demonstrated, there are a wide range of technology options covered by electronic voting and counting technologies. Suppliers also implement technologies in different ways, creating a confusing array of alternatives available to EMBs within and between these two broad categories. The variety of offered technologies might be one factor that has led to very different experiences in countries, which have used or attempted to use electronic voting and counting technologies.

Voting technologies have a surprisingly long history. In the United States, mechanical lever voting machines were first used for elections in 1892 and were commonly used in U.S. elections until the 1990s. Electronic technologies began to appear in the 1960s with punch card counting machines. In the following decades, technologies such as DRE voting machines, ballot scanning machines and Internet voting began to appear. The U.S. was at the forefront of adopting many of these technologies. Through the 1990s and the first decade of the new millennium, an increasing number of countries around the world also started to adopt these technologies.

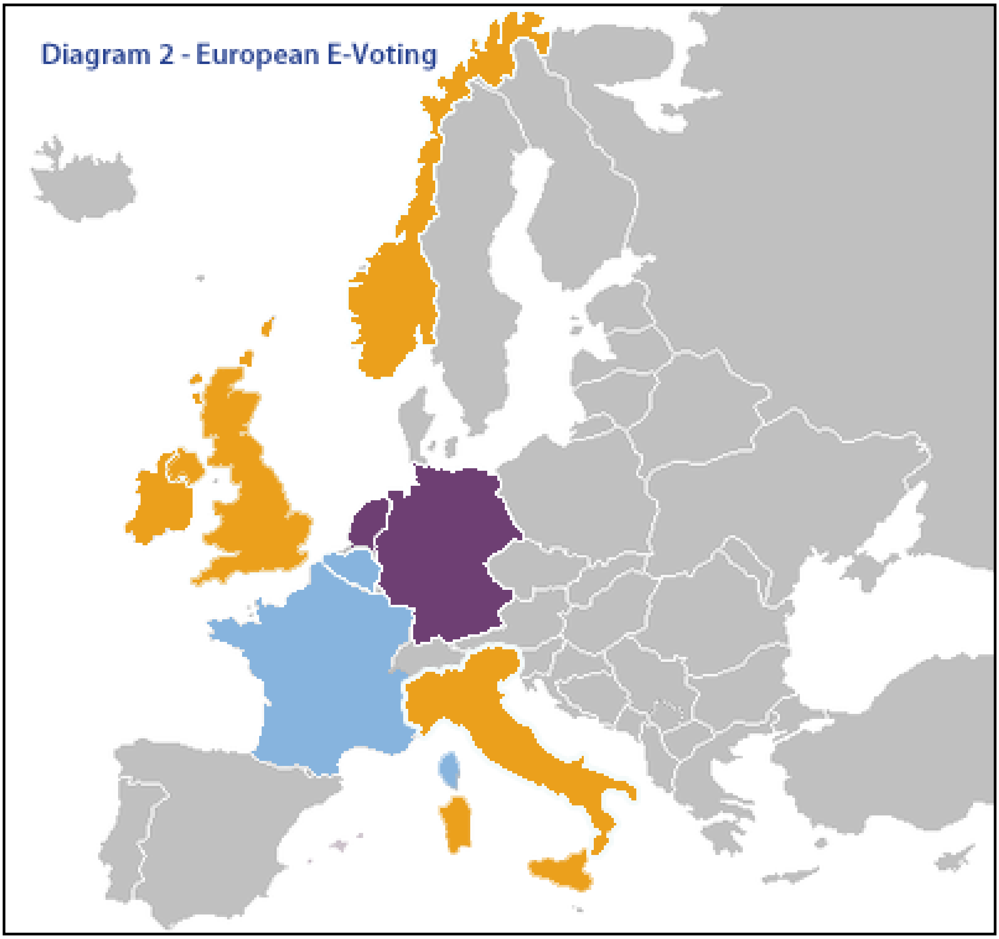
Recent research has shown that 31 countries around the world have used non-remote electronic voting machines for binding political elections at some point.[2] Some of these countries have experimented with EVMs and then decided not to continue with their use, in some cases after using them for many years. EVMs are being used in 20 countries, with six of these countries still piloting the technology. Globally, very different trends are seen in different

[2] Esteve, Jordi Barrat I, Ben Goldsmith and John Turner. International Experience with E-Voting. Norwegian E-Vote Project. IFES, June 2012.

FIGURE 2: MAP OF GLOBAL NON-REMOTE ELECTRONIC VOTING EXPERIENCE


For extended map of Europe, see diagram 2
E-Voting Globally
● Never Used
● Piloted and Not Continued
● Pilots Ongoing
● Currently Used in Parts of Country
● Currently Used Nationwide
● Discontinued

regions. Europe and North America can be seen as moving away from the use of EVMs, while South America and Asia show increasing interest in using electronic voting technologies. Unfortunately, no similar research is available for the global use of electronic counting technologies.



KEY ELECTRONIC VOTING AND COUNTING CONSIDERATIONS

As outlined previously, there are an increasing number of countries around the world that have implemented or piloted electronic voting and counting technologies. While each country's experience is different, there are some common themes that surface across these experiences. This section provides a summary of thematic issues that often arise when electronic voting and counting technologies are used. The considerations identified here are explored in more detail in part two of the manual, but it is hoped the following discussion will provide a basic understanding of each issue and the challenges electronic voting and counting technologies present in each regard.

LEGALITY OF E-VOTING[3]

When considering the use of electronic voting and counting technologies, the compatibility of these technologies with a country's existing constitutional and legal framework needs to be considered very carefully. The use of these technologies may not only be contradictory to existing provisions in the legal framework, but may require additional provisions be drafted to cover the ways in which technologies impact electoral processes.

It may well be that the existing legal framework makes reference to physical ballot boxes and ballot box seals, to actual ballot papers and the ways in which ballots are counted and adjudicated. All of these processes can occur with an electronic voting or counting machine, but in a different way.

[3] For more detailed information on this topic, please refer to the following sections in Part 2: Decision in Principle, pgs. 77-81; Legal and Procedural Framework, pgs. 106-113.

Therefore, the electoral legal framework needs to be reviewed to determine whether the use of electronic voting or counting technologies is in compliance with the law. It is highly likely that if only paper balloting has been used in the past, then the laws will have been written in such a way as to preclude the use of these technologies. Parts of the legislation requiring amendment will need to be identified, and suitable amendments will need to be passed before a trial or full use of electronic voting and counting technologies can be implemented. The consequence of not doing so could be to invalidate any election held with electronic voting or counting technology.

However, rather than simply addressing electoral framework issues that might be inconsistent with using electronic voting or counting technologies, it would be advisable to conduct a comprehensive review of relevant legislation to ensure all aspects of using electronic technologies in a country's elections are lawful and appropriately regulated. The review could also cover issues such as transparency mechanisms, security mechanisms, certification requirements, audit requirements and procedures for challenging results generated by electronic voting or counting machines. It may also be relevant to review other legislation that might not be directly related to elections, such as laws dealing with information technology; administrative and criminal codes; data security and protection; procurement; and the issue of government contracts. Such legislation may have an impact on the legal framework for using electronic voting or counting technologies, or may require an amendment to permit their use.

A balance needs to be established in drafting legislation to enable electronic voting or counting. A similar level of detail to paper based voting should be included in this legislation. Those drafting the legislation must also ensure the EMB has sufficient flexibility to respond to changes in technology and the way in which it is implemented. The EMB needs to be aware that, not only will legislation and regulations be required for proper implementation of electronic voting or counting technologies, but procedures and protocols for internal use and management are also vital.

If legal changes are required to use electronic voting or counting technologies, it is prudent to start the process of making legal amendments as early as possible, as the process may be lengthy. This will allow sufficient time to develop or amend legislation in a manner inclusive of citizens and political contestants.

At least as important as revising the law substantively is the process by which it is addressed. An open and inclusive process for deliberating any legal amendments concerning these issues is vital to winning public confidence and reaching an agreement with potential electoral contestants on the new rules of the electoral competition. The importance of a transparent and inclusive approach cannot be overstated.

TIMEFRAME[4]

The timeframe for consideration and possible adoption of electronic voting and counting technologies is an issue that needs to be carefully considered. It is easy to underestimate the time that proper consideration and implementation can take, even for a pilot project. A full assessment of electoral requirements; availability of technologies; and identifying benefits and challenges of using such technologies can take many months. Once suitable technologies are identified, they must be procured – ideally and initially on a small scale – for a pilot. When pilots are held, a full and thorough evaluation of the process must be conducted before any plans or decisions are made for further implementation.

Legislation and regulations need to be drafted and passed, which in many countries could take months or even longer. Consultations should take place in the ini-

[4] For more detailed information on this topic, please refer to the following section in Part 2: Project and Risk Management, pgs. 153-161.

tial stages and throughout the process with stakeholders regarding whether the technology should be implemented and, if so, in what form. Technology suppliers need adequate time to develop and deliver equipment and systems, including testing and certification of desired systems. Election officials need to be trained and voter education needs to be conducted on use of the technologies.

The complexity involved in implementation of such technology projects also means that even where comprehensive project plans and timelines are developed, there should be flexibility within the timeline to cope with unforeseen problems and challenges. Such complications often occur. Unlike other technology implementation projects, there is little room for delaying the completion date where elections are concerned. The election must take place on a certain date, and if the technology is not ready, it presents a serious problem.

EMBs considering the use of electronic voting or counting technologies need to be fully aware of these time challenges and plan accordingly. In most cases, the timeline for proper implementation of such technologies is likely to be measured in years rather than months, even for pilots.

SUSTAINABILITY[5]

Electronic voting and counting systems result in implementing elections in very different ways than traditional paper-based systems. These differences may have many benefits to offer in the conduct of elections, but they can also carry many disadvantages. The importance attached to the benefits vis-à-vis the challenges of using such technologies will vary from country to country. These country-specific circumstances will have a significant impact on the overall feasibility and desirability of using electronic voting and counting technologies.

[5] For more detailed information on this topic, please refer to the following sections in Part 2: Decision in Principle, pgs. 77-81; and Recruitment and Training of Personnel, pgs. 147-151.

Even if the use of such technology is both technically feasible and desirable, it needs to be sustainable in the long run. There are a number of contributing factors to the long-term sustainability of implementing electronic voting and counting, including financial aspects, project management and staffing arrangements.

The implementation of electronic voting or counting systems is usually an expensive exercise. Estimating the full cost of implementing the systems is not as easy as it may first seem, and the costs involved go far beyond just the procurement of voting or counting machines. Such additional costs include ongoing supplier support for contracts; management facilities for central/local tabulation of results; special booths/stands for voting machines; securing environmentally-controlled storage; maintenance and repair; replacement for expired equipment; consumables, such as ink cartridges and paper; testing and certification; specialized staff/technicians required to configure; testing and support for the technology; and voter and stakeholder education costs.

While a significant component of these costs is involved in the initial investment, there are many ongoing costs that need to be covered. A full appreciation of the costs involved over the life cycle of the electronic voting and counting machines needs to be factored into the estimate of financial sustainability for the technology. This is especially the case where a donor might be assisting a country in piloting or implementing a voting or counting system. The EMB needs to be confident it can provide the finances to continue implementation of the technology in absence of donor support.

From a project management perspective, the implementation of an electronic voting and counting technology project is complex, even if only for a small pilot project. The EMB will need to coordinate a range of tasks to implement the project, including procurement, logistics, procedural development, training, voter education, testing and IT configuration and support.

Not only will implementing the technology require special project management skills, it will require sufficient resources. The temptation to add management responsibilities to existing staff duties must be avoided, or the implementation of the technology will be at risk for poor management and could prove unsuccessful.

Another aspect of managing a technology project of this nature is that the transition from one system (e.g. paper-based elections) to another (e.g. electronic voting) needs to be executed effectively. Staff at all levels of the EMB, including polling and counting staff, will need to be properly trained in the new system and adequate support provided as they begin to use the technology. Political parties, candidates, media and observers will need to be educated about how the electronic voting or counting technology works, and the opportunities they have for oversight. Finally, and most importantly, voters will have to be informed about the use of technology and the ways in which it will affect their interaction with the electoral process.

The use of electronic voting and counting technologies also changes the skill sets required by some EMB and temporary staff conducting polling and counting. If polling and counting staff are to be able to set up voting or counting machines and deal with common problems encountered with these machines, then it may make it significantly more difficult in some places to recruit sufficiently qualified staff. Technical staff will also need to be hired by the EMB to provide support for less common faults with the technology. To be useful on Election Day, technical staff should be deployed nationwide to respond quickly to problems. Such resources may be difficult to recruit in some places.

Suppliers of electronic voting or counting technologies may be willing to assist with the challenge of recruiting qualified technical staff by providing staff themselves. When such assistance is provided by a supplier, the EMB must be careful that it does not effectively cede control of key parts of the electoral process to the supplier (addressed below in the section on accountability). While this support may often be provided in the interest of implementing the project successfully, it represents an abdication of responsibility on the part of the EMB and creates an unhealthy dependency on the supplier. It also indicates a lack of sustainability in the use of the voting or counting technology. This lack of sustainability is not insurmountable, but it must be recognized and addressed.

All of these challenges to sustainability need to be carefully deliberated by any EMB and other stakeholders involved in making important public policy decisions concerning the use of these technologies.

INCLUSIVENESS[6]

Elections should be as inclusive as possible, for voters and contestants alike. Inclusiveness is closely linked to the right to vote and the right to run for office, as well as the obligation of governments to facilitate these rights. There should be no discrimination toward any group in regard to voting rights or their implementation. An inclusive election process is also one that is based on open, broad consultation with stakeholders.

Innovations offered by electronic voting and counting can create opportunities for a more inclusive election process. Increased accessibility is one of the arguments in favor of the adoption of such technologies. Certain groups of voters struggle to participate in traditional elections. For example, voters with disabilities may only be able to vote with assistance, which can violate their right to a secret ballot. Electronic voting machines can be designed with features to assist voters with disabilities to cast ballots unaided, enabling a country to better meet international electoral standards. For instance, voting machines may be designed with audio explanations to

[6] For more detailed information on this topic, please refer to the following sections in Part 2: Decision in Principle, pgs. 77-81; Design Requirements, pgs. 116-123; and Voter Education/Information, pgs. 162-169.

allow blind voters to vote unaided; font size can be adjusted for the visually impaired; and sip/puff solutions can be used for voters with limited or no motor capacity.

Electronic voting machines may also facilitate the provision of ballots in other languages, with little additional cost, which may enfranchise linguistic minorities. Remote Internet voting may increase participation among military personnel and other voters living abroad.

At the same time, implementation of new voting or counting technologies should not exclude any group of voters or inhibit their participation in any way. Certain groups of voters, such as elderly, illiterate, rural or low income voters, may be unaccustomed to using computers or other electronic devices and may be initially reluctant to vote or cast their ballots electronically. Such considerations must be factored into both the design of the technology and related public outreach to ensure maximum usability of the equipment, particularly among groups that may be unfamiliar with electronic technologies.

Unintended disenfranchisement and potential erosion of trust in the election process has to be weighed against the potential for inclusion of certain groups and other possible benefits.That calculus is a matter of importance to all citizens, and is why sometimes seemingly technical considerations in this arena are actually public policy issues that require broad participation.The opinions and concerns of stakeholders (political parties, civil society and voters), must be central to decisions about whether and how to employ electronic voting or counting technologies. In addition, they should have an opportunity to monitor the processes for procuring the proposed equipment, including testing, certification, deployment and evaluation of its performance.This type of involvement will help build an understanding of the technologies, the likely benefits and a realistic assessment of the challenges.

If there is political consensus behind the decision to adopt electronic technologies, the potential for successful implementation is much higher. On the other hand, a decision to move ahead with such technologies in the face of significant opposition or lack of involvement is very risky, and could ultimately result in the failure of the project.

The accessibility and usability of proposed technologies should remain important considerations throughout the decision making process. Civil society organizations representing particular groups, such as persons with disabilities, illiterate or linguistic minorities should be consulted at regular intervals and be invited to test the equipment with these specific interests in mind. Pilot tests of equipment should also take issues of accessibility and usability into account.

Another aspect of inclusiveness is the need to provide voter information and education on new voting and counting technologies, so voters understand and feel confident using the equipment. Specific voter education campaigns should also be designed to target certain disadvantaged groups, explaining features that may facilitate their participation. As much as possible, voters should have the opportunity to try the technology before using it on Election Day.

Observer groups should give attention to issues of inclusiveness when observing a country that adopted electronic voting or counting technologies. Those groups should collect data on Election Day that demonstrates the extent to which certain populations experience difficulties when using the technology. Post-election survey data and focus groups can also provide valuable information about voter experiences using new technology for the first time.

TRANSPARENCY[7]

Transparency is a key principle for credible elections. A transparent election process is one in which each step is open to scrutiny by stakeholders (political parties, election observers and voters alike), who are able to independently verify the process is conducted according to procedures and no irregularities have occurred. Providing transparency in an election helps establish trust and public confidence in the process, as voters have a means to verify the results are an accurate reflection of the will of the people.

Electronic voting and counting technologies pose a challenge to ensuring transparency, since many visually-verifiable steps in a traditional election (such as how ballots were marked) are automated inside a machine and, therefore, cannot be seen by the voter and others. In such circumstances, particular efforts must be made to provide transparency in each step of the process.

A degree of transparency can be afforded through the design of the voting and counting technology. For instance, a VVPAT produces a paper record that can be checked by the voter to make sure the vote is accurately recorded. A paper record also provides the possibility of an auditable process. End-to-end verification systems allow a check to be conducted that all votes have been accurately recorded and tabulated.

Equally important to the transparency of Election Day is the transparency of the development of the technology itself. The procurement, development, testing and certification of voting and counting equipment should be carried out transparently, so stakeholders are confident the machines meet relevant requirements, function properly and have the necessary security features in place.

[7] For more detailed information on this topic, please refer to the following subsections in Part 2: Pilot Project, pgs. 88-93; Legal and Procedural Framework, pgs. 106-113; Procurement, Production, and Delivery, pgs. 124-133; Security Mechanisms, pgs. 134-145; Voter Education, pgs. 162-169; and Testing, Source Code Review and Certification, pgs. 173-181.

Stakeholders may have limited capacity to make use of these transparency mechanisms and may have to adapt their expertise to fully use them. The EMB can help observers in this regard by educating them on the electronic voting or counting system being used and how they can effectively observe it.

Certain mechanisms for providing transparency, such as the use of open source code, may be controversial, as vendors may be reluctant to disclose source code citing protection of intellectual property and the security of technologies. Irrespective of these interests, however, all software and hardware should be made available for independent review.

Electoral contestants and election observers have a critical role to play in ensuring the transparency of an election process. It is not possible for everyone to understand e-voting and counting systems. Thus, voters rely on others who have the capacity to understand these processes. It is therefore essential that stakeholders, including election observers and party/candidate agents, have access to the process.[8]

To carry out their role effectively, such monitors must be given sufficient access both in law and practice to make an informed assessment. This may require that additional points of observation be created in the electoral process. With traditional paper-based voting and manual counting, observers focus on the voting and counting process itself. Electronic voting and counting technologies entail a number of other activities, some critical to the integrity of the process, that can be observed, but which take place well in advance of Election Day. Such activities include the testing and certification of the systems and the installation of software on voting or counting machines. Those observing elections need to make additional efforts to monitor these processes, which take place outside of the normal window of election observation.

[8] For more detail on this point see Council of Europe (2011) Guidelines on transparency of e-enabled elections, available at www.coe.int.

Observers and party/candidate agents must also have access to relevant documentation about the procurement, development, testing and certification of equipment. It is critical they are able to observe during each stage of the process, from the initial decision making about whether to use electronic voting, to the final announcement of results. The transparency of various stages of the process should be a key consideration in the observers' overall assessment of the election.

The ability of observers and party/candidate agents to fulfill their roles is more challenging in an election that uses electronic voting and counting technologies. Observers must be properly trained to understand and report on the processes they observe. Watching voters use an electronic voting machine is unlikely to provide the information necessary to effectively assess the voting process. They should, therefore, become knowledgeable about the specific technologies that have been adopted and should be prepared to evaluate the testing and auditing of the voting and counting equipment, as well as the documentation of the process.

Since election observers and party/candidate agents may not have the expertise needed to understand certain aspects of electronic voting and counting technologies, organizations and parties may need to hire personnel specifically with an information and communications technology (ICT) background. They may also decide they are unable to assess certain aspects of the process and, if so, should disclose in their reporting which parts of the process they have and have not been able to observe effectively and take this into account in their overall assessment of electoral integrity.

The complex nature of electronic voting and counting technologies may also require ICT experts to provide independent oversight of such technologies, especially regarding the review of software and hardware. Professional ICT groups and academic communities can play a useful role in assessing electronic voting, either in partnership with election observer groups or independently. While the EMB should not exclude organizations that are skeptical about the benefits of electronic voting or counting technologies, they should be aware of any such organizational agendas.

FIGURE 3 – VERIFIABILITY[9]

System verifiability or auditability is becoming an increasingly important feature for electronic voting systems. Electronic counting systems have a natural audit trail of the (often paper) ballot, so additional verifiability mechanisms are less important for such systems. With DRE voting machines, and also with remote electronic voting, there is no obvious way for the voter to be sure their ballot choices have been recorded or counted accurately.

This lack of transparency was one of the main motivations for the development of the aforementioned VVPAT. Electronic voting machines with a VVPAT store the voter's ballot choices electronically but also on a paper record, often within the voting machine. This allows the voter to check that their ballot choices have been recorded accurately on the paper record. Electronic results produced by the electronic voting machine can then be checked against paper records,

[9] For more detailed information on verifiability, please refer to the following subsection in Part 2: Design Requirements, pgs. 116-123.

verified by the voter, to ensure the electronic result reflects the voter's choices.

However, use of VVPAT solutions is not without complications, especially with respect to the internal printer. Other schemes have been developed to provide the voter with some form of receipt so they can individually check that the vote has been received and counted accurately. This transparency has to be accomplished without violating the secrecy of the vote, which is a challenge.

End-to-end verifiable systems provide mechanisms for any oversight body to check that votes are received as cast, recorded as received and counted as recorded (i.e., all stages of the process function correctly and accurately). The voter will have some role in this verifiability, as only they know how they intended to cast their vote. Some end-to-end voting schemes provide the voter with a code they can use to check, after Election Day, that their vote has been included in the count with the correct value. Other schemes limit the role of the voter to checking the vote was received and recorded accurately, and provide other independently-verifiable proof that recorded votes are counted accurately.

INTEGRITY[10]

One of the fundamental principles elections must comply with is that they must accurately reflect the will of the voters. The integrity of the electoral process also has implications for other related issues, as discussed later in the section on trust.

The integrity of the process when using electronic voting and counting technologies is a particular challenge because of the nature of these technologies. With traditional paper balloting and hand counting, the entire process is not only clearly visible to those observing it, but it is also easily understandable to the average voter. The ballot box can be shown to be empty at the start of voting by polling staff, then sealed, observed in the polling station to ensure that only legitimate voters are putting in ballots, and at the end of voting the seal can be broken and the ballots counted in full view of observers. This overall transparency and simplicity of the process makes it relatively easy to observe the process and identify errors in the system if and when they occur. While political party and candidate agents, observers and the media perform a monitoring function, they also carry out a verification function to ascertain whether the process leads to an accurate reflection of the will of the voters.

This basic transparency is lacking for electronic voting and electronic counting, especially for electronic voting. The complexity of electronic voting tends to be beyond the understanding of the vast majority of voters. The technologies have what are known as "black box" components that take inputs from voters and produce outputs in a way that cannot be observed and verified by external observers or easily checked by election administrators. This is a potential problem from a transparency, trust and integrity perspective.

[10] For more detailed information on this topic, please refer to the following sections in Part 2: Election Day, (Set-Up, Testing, Security, Troubleshooting), pgs. 183-193; Tabulation, pgs. 194-197; Challenges and Recounts, pgs. 199-203; and Internet Voting, pgs. 218-227.

Those advocating against the use of electronic voting and counting technologies in the United States have long argued black box voting should not be accepted or trusted. They argue there is absolutely no basis on which to accept or trust these voting and counting technologies.[11] Examples of voting and counting machines making significant errors in the results they generate have been provided, and the worry is that there are many more discrepancies taking place that are not identified because they are not as egregious and obvious or are impossible to identify because the necessary audit mechanisms are not in place.

As a result, additional and varied measures are required to provide the same level of assurance that an electronic voting or counting process is actually delivering an election that reflects the will of the voters. Additional measures may include transparency mechanisms; testing and certification regimes; authentication mechanisms; and audit mechanisms:

- **Transparency** – is a crucial tool to ensure the integrity of electronic voting and counting technologies. While ensuring voting and counting technologies are transparent does not alone guarantee that technologies will generate accurate results, it does provide the space and tools to do so. Making electronic voting and counting processes transparent allows the EMB and stakeholders the opportunities to monitor critical elements of the process and ensure that errors, accidental or otherwise, are not made in these aspects of the electoral process. The previous section details steps that can be taken to improve transparency in the process of introducing and implementing electronic voting and counting technologies. Steps range from access to system documentation and source code for electoral stakeholders, to additional points of observation for observers.

[11] See Harris, B. (2004) Black Box Voting and www.verifiedvoting.org.

FIGURE 4: NEW STAGES OF OBSERVATION – EXAMPLES FOR AN ELECTRONIC VOTING MACHINE

The introduction of electronic voting or counting technologies produces a number of new points at which oversight of the process can and should take place. These points of oversight will vary depending on the technology introduced and the specific vendor system being implemented. Examples of additional observation points for an electronic voting machine system are provided here:

- **Certification** – it is unlikely certification of the electronic voting machine system would be fully open to observation; if possible, such observation would probably be impractical due to the length of time this process can take. However, documentation about the process should be available and reviewed by observers.

- **Source Code Review** – the source code should be made available for scrutiny, although this will obviously require party/candidate agents and observers with specialized IT skills.

- **Testing** – the EMB will need to conduct its own regime of testing, regardless of whether the electronic voting machines are formally certified, and observers should consider observing this testing. Party/candidate agents and observers should also review documentation on testing.

- **Storage and Distribution** – arrangements for the storage of electronic voting machines between elections may be observed and an assessment of the security arrangements made. The procedure for handover, transportation and local storage immediately prior to the election may also be monitored.

- **Machine Configuration** – prior to the election, the electronic voting machines will need to be configured for the election being conducted. This configuration process is critical and should be monitored. This may involve observing that proper procedures are followed, as well as using mechanisms to prove that the loaded version of the software is the tested and approved version.

- **Voter Education Efforts** – voters will need to be informed in advance about the use of electronic voting machines, especially if they are being used for the first time. Party/candidate agents and observers should monitor and assess the efforts made by the EMB to educate voters.

- **Training for Polling Staff** – it is important that polling staff are properly trained in the use of electronic voting machines, new administrative and security procedures and what to do if there is a problem with the machines. Party/candidate agents and observers should monitor this training process and determine whether sufficient efforts have been made to prepare polling staff for the use of electronic voting machines.

- **Electronic Voting Helpdesk** – it is likely that implementation of an electronic voting machine system will include the establishment of a help desk for reporting and resolving problems encountered while using the voting machines during voting. Oversight of this help desk function is also important.

- **Audit of VVPAT** – the manual count of paper records produced by an electronic voting machine is a vital mechanism for ensuring that the machine functions correctly, but also for building trust in the electronic voting machine. This process must be open to observation and, accordingly, should be observed.

- **Testing[12] and Certification[13]** – given the lack of transparency of electronic voting and counting processes compared to paper balloting, it is essential that election administrators make efforts to build confidence in voting or counting machines, ensuring they work properly before they are used. This testing needs to not only ensure the systems developed meet the requirements specified by the EMB, but also that they meet the requirements of the environment.

  These tests are essential so the EMB can use electronic voting and counting technologies with confidence. It is important to note that these various tests take time and money to conduct, and an

[12] For more detailed information on the topic of testing, please refer to the following sections in Part 2: Pilot Project, pgs. 88-93; Legal and Procedural Framework, pgs. 106-113; Design Requirements, pgs. 116-123; Testing, Source Code Review and Certification, pgs. 173-181; and Election Day, pgs. 183-193.

[13] For more detailed information on the topic of certification, please refer to the following sections in Part 2: Legal and Procedural Frameworks, pgs. 106-113; and Testing, Source Code Review and Certification, pgs. 173-181.

appropriate amount of time needs to be allocated for these testing processes. The testing itself and reports analyzing results of the testing should be reviewed by electoral contestants and observers to ensure public confidence.

FIGURE 5: TYPES OF TESTING

The Council of Europe's E-Voting Handbook[14] identifies six types of testing EMBs should conduct:

- **Acceptance Testing** – this method of testing software that tests the functionality of an application performed on a system (for example software, batches of manufactured mechanical parts, or batches of chemical products) prior to its delivery.

- **Performance Testing** – this testing determines the speed or effectiveness of a computer, network, software program or device. This process can involve quantitative tests done in a laboratory, such as measuring the response time or the number of millions of instructions per second (MIPS) at which system functions. Qualitative attributes such as reliability, scalability and interoperability may also be evaluated. Performance testing is often done in conjunction with stress testing.

[14] Caarls, S. (2010) E-voting Handbook: Key steps in the implementation of e-enabled elections, Strasbourg: Council of Europe

- **Stress Testing** – this testing determines the stability of a given system or entity. It involves testing beyond normal operational capacity, often to breaking point, in order to observe the results. Stress testing may have a more specific meaning in certain industries, such as fatigue testing for materials.

- **Security Testing** – this process determines if an information system protects data and maintains functionality as intended. The six basic security concepts that need to be covered by security testing are: confidentiality, integrity, authentication, authorization, availability and non-repudiation.

- **Usability Testing** – this technique evaluates a product by testing it on users. It can be seen as an irreplaceable usability practice, since it gives direct input on how real users use the system.

- **Review of Source Code** – this systematic examination of computer source code aims to find and rectify mistakes overlooked in the initial development phase, improving both the overall quality of the software and the developers' skills.[15]

[15] CoE (2010), pp.34-35.

In addition, some countries choose to have electronic voting and counting technologies certified prior to use.[16] Certification serves a similar purpose as testing, but it should be conducted by a body independent of the EMB, political parties, government and suppliers. Ideally, the certification process is conducted in an open, transparent manner builds confidence in the operation of the voting or counting technology. Certification should be done by a source that is widely accepted by stakeholders as independent and competent.

The U.S. Election Assistance Commission's *Voting System Testing and Certification Program Manual* defines certification as, "the process by which the Election Assistance Commission, through testing and evaluation conducted by an accredited Voting System Testing Laboratory, validates that a voting system meets the requirements set forth in existing voting system testing standards…and performs according to the Manufacturer's specifications for the system."[17]

The Council of Europe's *Certification of E-voting Systems* considers certification as, "a process of confirmation that an e-voting system is in compliance with prescribed requirements and standards and that it at least includes provisions to ascertain the correct functioning of the system. This can be done through measures ranging from testing and auditing through to formal certification. The end result is a report and/or a certificate."

[16] Council of Europe (2011), Certification of e-voting systems: Guidelines for developing processes that confirm compliance with prescribed requirements and standards, Strasbourg: Council of Europe, pp. 2-3.

[17] U.S. Election Assistance Commission (2011), Voting System Testing and Certification Program Manual. Washington, DC, p. 17.

The Council of Europe continues, "Certification can be applied in different ways. Solutions chosen by a member State may include certification of a single e-voting system for nationwide use, it can opt to certify multiple systems, provisionally certify an e-voting system, or only test one or several parts, i.e. component testing. Member States may choose those measures described in the present guidelines that correspond with their particular voting system, bearing in mind the need to ensure that the voting procedures respond to possible threats and risks while being in line with international commitments."

Certification has an important role to play in ensuring electronic voting and counting systems comply with requirements and standards, but it also plays a vital role in establishing trust among key stakeholders. The independence and competence of certifying institution(s) is fundamental to this trust building role.

- **Authentication**[18] – it makes little sense to spend time testing and certifying an electronic voting or counting system if there is subsequently no check that this is the actual system being used for the election. Authentication can be done through digitally signing the version of software that is tested and approved. Mechanisms can then be established so the digital signature of installed software can be checked by those observing the election.

  Likewise, when electronic data passes from one stage of the process to another, for example if voting/results data from the polling station is passed to the tabulation process (often done through portable electronic media, such as a memory stick), the validity of the data received for tabulation needs to be verified. Otherwise, it would be

[18] For more detailed information on this topic, please refer to the following sections in Part 2: Procurement, Production and Delivery, pgs. 124-133; and Internet Voting, pgs. 218-227.

easy to substitute false data into the process. This issue can also be dealt with through the use of digital signatures for data. This means only results data with an authentic digital signature would be accepted by the tabulation system. All such results transfers require verifiable safeguards that are observable by party/candidate agents and election monitors in order to maintain confidence in this highly-sensitive aspect of elections.

- **Audit**[19] – the ability to verify the operation and audit the results of an electronic voting or counting system is an emerging standard for electronic voting and counting technologies. While electronic counting solutions have a natural audit trail in the ballot that is fed into the counting machine, electronic voting solutions do not inherently have this feature. It can easily be added to electronic voting systems though. The most common way is through the use of a VVPAT, which was discussed in the section on transparency. The VVPAT is a paper record of the choices made on the voting machine, which can be checked by the voter to ensure the same electronic choices were made. The voter does not keep this paper record.

  However the audit trail is provided, it is critical that it is used to check the accuracy of the electronic voting or counting process whether or not election results are contested. A random sample of audit trails should be routinely checked against electronic results produced by electronic voting or counting machines to ensure there are no differences between the electronic and audit trail results. This is important not just for the present but for future elections that may be closely fought and where even small discrepancies may be critical. Conducting the audit in a public manner will provide an additional

[19] For more detailed information on this topic, please refer to the following sections in Part 2: Legal and Procedural Frameworks, pgs. 106-113; Testing, Source Code Review and Certification, pgs. 173-181; and Challenges and Recounts, pgs. 199-203; and Internet Voting, pgs. 218-227.

check on the integrity of the system and help build confidence and trust in the system. Such an audit provides an important check on the accuracy of the results. Without this audit of the paper trail, the value of the VVPAT is undermined.

TRUST[20]

Trust is a vital component of the democratic process, and trust in the election process is critical for acceptance of electoral outcomes by the public, political actors and other electoral stakeholders. It is not only important for the integrity of the electoral process that voters and other electoral stakeholders trust the process to accurately reflect votes cast, but also for these actors to trust EMBs have executed their responsibilities in a manner that safeguards the integrity of the process. While delivering elections that reflect the will of the voters is of critical importance for EMBs to generate trust, it is also important for EMBs to engage electoral stakeholders throughout the process and be responsive to their concerns and needs so trust is maintained over time.

This is especially important when electronic voting and counting technologies are being introduced into the electoral process. The inherent opaqueness of these technologies when compared to paper-based ballots, as well as the relative lack of familiarity with these technologies among most stakeholders should compel EMBs to ensure the design and implementation process is open and generates confidence. Failure to do so may lead to experiences where strong electoral systems with foundations of trust are forced to backtrack on electronic voting because electoral authorities did not engage stakeholders throughout the process and lost the support needed to move forward with electronic voting. Where there is not a tradition of strong, trusted electoral

[20] For more detailed information on this topic, please refer to the following sections in Part 2: Decision in Principle, pgs. 77-81; Procurement, Production and Delivery, pgs. 124-133; Project and Risk Management, pgs. 153-161; Voter Education/ Information, pgs. 162-169; Post-Election Audits, pgs. 205-209; and Internet Voting, pgs. 218-227.

administration, the consequences of failing to establish confidence in electronic voting and counting technologies could be even more severe. Trust in the electoral process is a hard-won commodity that can quickly dissipate if errors are found. It is essential that EMBs take the steps necessary to further and maintain trust with the introduction of electronic voting and counting technologies.

As discussed, transparency is a key factor in generating public and stakeholder trust in the electoral process, but it is a difficult measure to provide for electronic voting systems where the casting and counting of ballots is not visible. EMBs can use a number of concrete steps to foster transparency in the process of design and implementation of electronic voting and counting systems, but the basic underlying stance for EMBs should be to have a process that is open and engages electoral stakeholders every step of the way. Given the complexity of electronic voting and counting systems, it is important that EMBs provide stakeholders with information about the technologies and the process through which these technologies will be implemented. Some steps EMBs can take to elicit trust through transparency have already been discussed above.

In addition to providing access to independent experts and stakeholders to test the technology to be used in a particular election, EMBs can also embrace transparency by making stakeholders a key part of the evaluation process while the choice of technology is being evaluated for adoption, as well as after an election. EMBs should engage informed stakeholders in these evaluations where the performance of electronic voting and counting systems is tested against either standards established for traditional, paper-based systems or emerging standards (e.g. the Council of Europe’s e-voting recommendations) for electronic voting systems.

Voters are the end client for any voting system. Prudent EMBs should ensure voters are informed about changes in the way they cast their vote, and that at least some voters have a chance to try the technology out so that any usability issues can be identified early and addressed. Voter education programs that communicate the essential characteristics of the electronic voting system should be disseminated far and wide before the first use of these technologies so voters are not caught off-guard when voting. Demonstrations of voting technology through mock and pilot elections should be deployed so electoral authorities can ascertain whether voter education or other voter sensitization programs need to address specific issues in preparing voters for the introduction of the electronic voting technology.

SECRECY[21]

The secrecy of the vote is seen as one of the fundamental principles required in the conduct of democratic elections. Failure to secure the secrecy of the vote opens the possibility for voters to prove how they have voted, facilitating voter coercion and vote buying. Both of these practices undermine the free expression of the will of the voter and the possibility for election results to reflect the will of the voters.

If implemented properly, the paper-based system of voting effectively protects the secrecy of the vote. In the case of electronic counting, the same protections that currently exist for the hand counting of paper ballots should be applied. Electronic voting, however, introduces a number of additional ways secrecy can be violated. Voting machines record the choices cast on them by voters, and these votes may be recorded in the order in which they are cast with a timestamp. This means if someone knows the order in which voters cast their ballots on a voting machine or the time at which a voter cast their ballot and has access to the record of voting on the machine, they could determine the choices made by each voter.

[21] For more detailed information on this topic, please refer to the following sections in Part 2: Legal and Procedural Frameworks, pgs. 106-113; Procurement, Production, and Delivery, pgs. 124-133; Security Mechanisms, pgs. 134-145; Election Day (Set-Up, Testing, Security, Troubleshooting) pgs: 183-193; and Internet Voting, pgs: 218-227.

Appropriate procedures restricting access to logged transactions on the voting machine would reduce this threat to the secrecy of the vote. In countries that have experienced authoritarian trends, these issues are likely to generate suspicions among citizens concerning breaches of ballot secrecy, and extra steps may be required to establish public confidence.

Other developments with electronic voting machines are increasing the threat to the secrecy of the vote. While the VVPAT is a vital tool in building confidence in the use of electronic voting machines and in providing an audit mechanism, it can also be implemented in such a way as to undermine the secrecy of the vote. Some VVPAT systems have a roll of paper on which the voter's choices are printed. As the choices are printed sequentially, this can be used with the order in which voters cast their ballots on the voting machine to determine the content of each person's vote. Access to the paper audit trail cannot be restricted in the same way as with electronic records on voting machines, since the audit trail is meant to be taken out and checked against the electronic record of the voting machine.

However, not all VVPAT systems function in this way. Some voting machine paper audit trails operate a cut-and-drop system where the printed vote is cut from the roll of paper and drops into an internal ballot box within the voting machine. This ensures that audit records are randomized in the same way as placing a paper ballot into a physical ballot box.

A potential, final challenge to the secrecy of the vote from electronic voting machines comes from the most recent developments with voting machines, whereby the machines also conduct voter identification. Most voting machines still rely on a physical process for voter identification and authentication, with polling staff checking voter names against a voter list separate from the voting machine. This means voter identification data and vote data are held in completely separate processes (the former through a manual process and the latter through an electronic process), which are never linked in any way, making it impossible to link voting data to the voter.

More recent voting machines are also fulfilling the function of voter identification and authentication. This identification can be by simply entering an ID number or passcode for the voter, or it can be through the voting machine scanning a biometric attribute of the voter and identifying them from a list of approved voters. Clearly, when the voting machine identifies the voter, it possesses both pieces of information required to break the secrecy of the vote and could retain the link between the two.

Technical solutions are readily available to ensure it is not possible to link voter data with the value of their vote. However, EMBs will need to adequately address concerns by stakeholders that this link is still maintained and that the secrecy of the vote is not violated.

While challenges related to the secrecy of the vote with electronic voting machines can be resolved, it is important that electoral stakeholders are cognizant of them and take all necessary steps to ensure the secrecy of the vote when considering the use of voting machines. At the same time, observers should evaluate whether any aspect of the process might challenge this fundamental principle.

ACCOUNTABILITY[22]

Elections are the primary means by which voters hold those elected to office accountable. While elections create an accountability mechanism, there must also

[22] For more detailed information on this topic, please refer to the following sections in Part 2: Design Requirements, pgs 116-123; Procurement, Production and Delivery (EMB-Vendor Relations), pgs. 124-133; Recruitment and Training of Personnel, pgs. 147-151; Project and Risk Management, pgs. 153-161; Challenges and Recounts, pgs. 199-203; Post-election Audits, pgs. 205-209; Evaluation of System, pgs. 211-217; and Internet Voting, pgs 218-227.

be accountability within an election process if it is to be genuine.[23] Accountability in an election process ensures those who conduct elections do so in compliance with the election legislation and relevant procedures, and in a manner that promotes the integrity of the process.

Generally, elections are conducted by EMBs. Within EMBs it is critical that responsibilities are clearly defined, including who has authorization to take specific actions or decisions. Officials at all levels of election administration must be responsible for their actions and decisions, and must be held accountable should they fail in their duties. Disciplinary measures and penalties must be defined for such instances, including the possibility of criminal liability for serious offenses.

The principle of accountability remains the same for elections that include electronic voting and counting, but is more complicated than traditional paper-based systems in several respects. First, because the consequences of some actions taken by officials may not be visible (since they take place within a machine), it is particularly important that each action taken is properly recorded. Second, because many aspects of implementing electronic voting and counting systems require highly-specialized skills (e.g., configuration, installation and maintenance), it may be a challenge for EMBs to identify staff that can perform such tasks. Third, because of the technical nature of the process, it is common that suppliers of the technology assist the EMB and fulfill some responsibilities of the EMB.

While it is preferable for an EMB to have in-house capacity to maintain its election equipment, it might not be possible to identify staff with needed specific, technical skills. In any case, technology vendors will inevitably be involved to a certain degree in the setup, use and maintenance of the equipment they supply.

[23] Merloe, P. (2008) Promoting Legal Frameworks for Elections: An NDI Guide for Developing Election Laws and Legal Commentaries, pp. 17-21.

However, the EMB needs to remain in control of the relationship with the vendor and ensure the relationship does not violate its own responsibility to be in charge of implementing the electoral process. Any role for the vendor must be clearly defined so the EMB remains in control of the process at all times, and remains accountable should a problem arise.

Vendors of election technology have a different set of concerns than election officials. Their primary concern is to make money by delivering their products and services according to the contract they have concluded with the EMB. Vendors may not be aware of such constraints as election deadlines or legal requirements that must be met. It is the responsibility of the election officials to ensure the process meets deadlines and legal requirements, and liaise closely with vendors to make sure these criteria are met. The procurement process also must lead to contractual requirements that include firm deadlines for delivery that correspond to the electoral calendar, including sufficient time to remedy deficiencies in vendor performance, and sufficient penalties to deter non-performance. The vendor should not be in a position to take any action affecting the functionality of the equipment without the express authorization of the EMB. Any actions taken by the vendor should be carefully monitored and recorded.

EMBs can take steps to increase their own accountability in a number of ways. They can hold regular public consultations to present information on their recent activities and answer any complaints. This is especially necessary in a situation where new technologies are implemented that may not be broadly understood by the public or electoral contestants. EMBs can also allow political parties, election observers and the media the opportunity to attend their meetings where policies are being formulated, particularly in regard to the introduction and use of new election technologies. It is also common for EMBs to publish a report following an election that considers how the election was conducted and may provide recommendations for improvements in the future.

EMBs may be held accountable by a variety of institutions. It is good practice for electronic voting and counting systems to be certified by an independent authority, before they are approved for use, to verify they meet the necessary requirements. Audits can be conducted at regular intervals to verify that the equipment in use is the same that has been certified.

In many countries, parliamentary committees play an important oversight role, holding hearings to review the effectiveness and impartiality of EMBs. In countries with electronic voting and counting, a parliament may appoint specific independent committees with technical competence to evaluate the implementation of the technologies. For example, in Belgium, Parliament appoints an independent College of Experts that has the responsibility to review the integrity of voting and counting technologies throughout the election cycle.

Accountability can also be strengthened through the conduct of audits. On Election Day, voting and counting machines should be audited in a sample of polling stations to determine whether votes have been accurately recorded by the machines. An independent body can also conduct an overall audit of the technology after Election Day to verify that each step of the election process has been properly carried out.

Political parties, the media and citizen election observers also hold EMBs accountable by monitoring their activities and bringing any violations to the attention of the public, as well as the relevant authorities through complaints and appeals procedures. In countries with electronic voting and counting, political parties and citizen observers may need to develop specific skills to detect any violations and collect the necessary evidence to file a complaint.

SECURITY[24]

The security of the electoral process is critical for all elections. There are always points at which those wishing to manipulate the system could attempt to manipulate vote data. System security is especially important for electronic voting and counting systems, which may introduce new vulnerabilities into an election process. These vulnerabilities include external security threats to the security of the system, as well as internal threats of manipulation by those with official access to the system. These technologies are inherently less transparent than paper ballots, where all steps in the voting and counting process are observable. If electronic voting and counting systems are to be trusted by electoral stakeholders, it is important that the security challenges presented by the use of the technology are understood. Mechanisms must be in place to mitigate these security challenges, and any security breaches should be easily identified.

The security of electronic voting and counting systems has become an increasingly important public issue. Early systems were implemented with very few, if any, security mechanisms or checks and balances to ensure that they accurately recorded and reported on votes cast. The 2000 U.S. presidential election can be seen as a global turning point in terms of the scrutiny that technology-based electoral systems were subjected. While technology was certainly not the only problem in that election, it clearly showed that technology, even if well-established, was fallible; checks and balances were essential if voters and contestants were to trust the results generated by technology. This lesson later manifested itself across many aspects of electronic voting and counting, including a much greater scrutiny of the physical security of electronic voting and counting machines and investigations into the possibility of infiltrating the code which runs the systems.

[24] For more detailed information on this topic, please refer to the following sections in Part 2: Procedural and Legal Frameworks, pgs. 106-113; Procurement, Production and Delivery, pgs. 124-133; Security Mechanisms, pgs. 134-145; Project and Risk Management, pgs. 153-161; Election Day (Set-Up, Testing, Security, Troubleshooting), pgs. 183-193; and Internet Voting, pgs. 218-227.

Electronic voting and counting machines and results systems did not fare well under this additional scrutiny. Despite the denial of suppliers and often election administrators, numerous security flaws were found in electronic voting and counting machines by IT security experts in several countries (such as the U.S., the Netherlands and Germany), some with well-established systems of electronic voting and counting. Such cases weaken public confidence in the integrity of electronic voting and counting machines and demonstrate the need for increased vigilance against emerging security risks.

It is clear the issue of physical and logistical security of voting and counting machines and associated communication networks are keen concerns for electoral stakeholders that are important for the integrity of elections. Voting machine suppliers and election administrators have had to increase the measures implemented to ensure this security is achieved, both in terms of voting machine design and in terms of control procedures relating to access to electronic voting machines and systems. The problem is that, as technological solutions ensure system security is improved, so are the ways in which systems can be hacked and manipulated.

As a result, one of the key ways in which these security concerns have been mitigated is through the development of effective audit mechanisms for electronic voting machines, such as the VVPAT. This ensures that, when audit trails are routinely checked, even when a security breach occurs, it can be detected.

EMERGING ELECTRONIC VOTING STANDARDS

Electoral standards based on public international law are well-elaborated in documents issued by intergovernmental organizations such as the United Nations; the African Union; the Commonwealth; the Council of Europe; including its European Commission for Democracy through Law (the Venice Commission); the European Union; the Organization of American States (OAS);

the Organization for Security and Cooperation in Europe (OSCE); and other bodies. These sources illustrate a common understanding of the content of international electoral standards, drawing directly from the wording of Article 21 of the Universal Declaration of Human Rights, Article 25 of the International Covenant on Civil and Political Rights (ICCPR), other articles in those documents related to the exercise of rights that are essential to democratic elections, and other human rights treaties, declarations and instruments. A number of rulings by international tribunals concerning genuine elections and writings of highly-qualified legal experts advance electoral standards in harmony with those sources of law, and the generally-accepted practices of states conducting elections reflect them as well.

The core of these international electoral standards can be defined as the right of citizens, without discrimination, to take part in government and public affairs, directly or indirectly through freely chosen representatives, by exercising their right to vote and to be elected at genuine periodic elections, which shall be by universal and equal suffrage, held by secret ballot and guaranteeing the free expression of the will of the electors. This combines with the right to seek, receive and impart information (i.e., the freedom of expression) about the nature of electoral processes, forming the basis for electoral transparency.[25]

These international electoral standards frame the conditions for using any tools to secure genuine elections, including electronic voting and counting. Because these new technologies for voting and counting fundamentally change the way many components of the electoral process are conducted, the standards demand corresponding new techniques to safeguard electoral integrity and earn public trust in their use. As a result, there have been initiatives in recent years to evolve these international electoral standards in order to cope with the challenges of using voting and counting technologies. The Council of Europe's

[25] P. Merloe, "Human Rights – The Basis for Inclusiveness, Transparency, Accountability and Public Confidence in Elections," in International Election Principles: Democracy & the Rule of Law (JH Young, ed., ABA 2009), pp. 3, 18-20.

2004 *Recommendation on Legal, Operational and Technical Standards for E-voting* did much to set the agenda for this adoption of existing standards for electronic voting and counting technologies. The Council of Europe followed up this document with several other publications, including documents on transparency and certification of e-voting systems.[26] The OSCE's Office for Democratic Institutions and Human Rights, the OAS, the Carter Center and NDI have approached the issue of standards for electronic voting and counting technologies from the perspective of observing or monitoring elections in which these technologies are used. IFES and International IDEA have also sought to provide guidelines and standards for the implementation of electronic voting and counting technologies by EMBs.

In analyzing the publications by the organizations listed above, it is clear that some trends are emerging in the recommendations about the conduct of elections using electronic voting and counting technologies. Common themes can be seen in the following areas:

- **Transparency** – as much of the process as possible should be transparent and verifiable. Effective access should be provided for party/candidate agents and observers in a manner that does not obstruct the electoral process.

- **Public Confidence** – closely related to and relying heavily upon transparency is the requirement that voters understand and have confidence in the electronic voting or counting technology being used. Public confidence requires that stakeholders are: involved in the processes of deciding whether to introduce electronic voting and counting technologies and considering the type of system to be introduced; provided information so they understand the technologies

[26] "E-voting Handbook: Key steps in the implementation of e-enabled elections", "Guidelines on certification of e-voting processes" and "Guidelines on transparency of e-enabled elections", www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Default_en.asp

being used; given the opportunity to take part in simulations of the systems that take place; allowed to monitor testing, certification and auditing and review findings; and informed well in advance about the introduction, timeline and how to participate.

- **Usability** – electronic voting and counting technologies must be easy to understand and use. Stakeholders should be involved in the design of electronic voting and counting technologies and in public testing. Further, electronic voting and counting technologies should endeavor to maximize the accessibility of the voting system for persons with disabilities and minority language groups, and must not disenfranchise others. They must also afford voters the possibility to review and amend their vote before confirmation of their choice.

- **System Certification** – electronic voting and counting technologies must be certified by a qualified, independent body before their use and periodically thereafter. This ensures the use of such electronic technologies continues to meet the requirements of the electoral jurisdiction as well as the technical specifications for the system. Further, the certification process should be conducted in a transparent manner providing electoral stakeholders access to information on the process and earning public confidence.

- **System Testing** – any electronic voting or counting system should be subjected to a comprehensive range of testing before it is approved for use by an EMB. This testing should take place transparently and with access for electoral competitors and observers.

- **System Security** – the opportunities for systematic manipulation of the results mean that system security needs to be taken seriously. Security measures need to ensure that data cannot be lost in the event of a breakdown; only authorized voters can use an electronic voting or counting system; system configuration and results generated can be authenticated; and, only authorized persons are allowed to access electronic voting, counting and results management functionality, although party/candidate agents and observers should be able to monitor the integrity of that functionality. Any intervention that affects the system while electronic voting and/or counting is taking place should be carried out in teams of two, be reported on and be monitored by the electoral authority, party/candidate agents and observers. Attempts to hack into electronic voting and counting machines or the election management system into which results are received need to be detected, reported and protected against.

- **Auditability and Recounts** – electronic voting and counting technologies must be auditable so it is possible to determine whether they operated correctly. It must be possible to conduct a recount. Such recounts must involve accurate and monitored manual recounts of votes cast electronically (e.g., with the paper record representing the basis for legal determination of the vote cast) and not merely be a repetition of the electronic result already provided.

- **Verifiability** – it must also be possible to assure voters their votes are being counted as cast while also ensuring that secrecy of the vote is not compromised. This requires that electronic voting systems create an audit trail which is verifiable. It should provide the voter with a token or code with which to perform the verification. However, the token or code must not allow the voter to prove to others how they have cast their vote. The most common solution to this for in-person electronic voting machines is through the production of a VVPAT, and this solution is emerging as a standard in this regard. It should be noted that a VVPAT is not appropriate for unsupervised remote electronic voting (e.g. Internet voting, text message voting etc.) as there would be nothing to stop a voter from removing the paper record of the vote, and making vote buying and voter coercion possible.

- **Mandatory Audit of Results** – the existence of an audit trail for electronic voting and counting systems achieves little if it is not used to verify that electronic results and the audit trail deliver the same result. A mandatory audit of the results generated by electronic voting or counting technologies should be required by law and take place for a statistically significant random sample of ballots whether or not results are subject to a dispute.

- **Secrecy of the Ballot** – the use of electronic voting and counting technologies must comply with the need for secrecy of the ballot. This requirement is not a new standard, but it is one that is made more difficult by electronic voting and counting technologies. This is especially the case for remote electronic voting systems, where voters have to first identify themselves and vote electronically using the same interface.

- **Accountability in Vendor Relations** – the EMB needs to remain in control of the relationship with the vendor and ensure the relationship does not violate its own responsibility to be in charge of implementing the electoral process. Any role for the vendor must be clearly defined so the EMB remains in control of the process at all times and remains accountable, should a problem arise.

- **Incremental Implementation** – whenever electronic voting and counting technologies are introduced, they should be done so in an incremental manner and should start with less important elections. This will allow public understanding and trust to develop in the new system, and provide time to deal with problems and resistance.

It is too early to say international standards are fully evolved concerning the use of electronic voting and counting technologies. Nevertheless, trends can be seen in emerging electoral standards concerning their adoption. As a means to maintain electoral integrity, these trends in emerging standards should be carefully considered when the adoption of any new technology is deliberated and employed.