CHAPTER FOUR: Monitoring Electronic Voting Technologies

INTRODUCTION

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

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

Practice shows that public confidence in electronic voting has to be built over time, usually through a phased process of introducing the technology that allows voters to use paper ballots if they prefer. A critical issue is the "comfort" of voters in using electronic technologies, which is as much a question of trust as it is the technical proficiency of voters in using the technology. Public confidence is best built through transparency concerning the technology—both toward the public and the political contestants—and through widespread civic education about the technology.

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

EVALUATING THE RATIONALE FOR INTRODUCING ELECTRONIC VOTING

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

Cost:

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

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

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

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

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

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

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

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

Service, Maintenance, Replacement. Hardware does occasionally malfunction or break down. The cost-benefit analysis should include projections of replacement costs, as well as costs of regular services and maintenance of the equipment. The lifespan of the electronic equipment is not indefinite and will depend upon the type of the equipment. Analyses should provide realistic projections of equipment lifespan. Election authorities usually keep a "strategic stock" of equipment in order to replace the equipment that malfunctions. The lifespan of software is also an important consideration, particularly in light of the rapid evolution of Information Technology.

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

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

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

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

Usability:

Usability issues are two-fold, and they relate both to the voters and election officials. The threshold questions for monitors from observer groups and political contestants to ask are: Did authorities run usability tests with voting equipment models and a variety of types of voters, and what were the results? The following questions are among those that need to be asked and answered through usability testing.

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

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

Fraud Prevention:

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

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

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

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

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

Count and Tabulation Facilitation:

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

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

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

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

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

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

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

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

LEGAL FRAMEWORK

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

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

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

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

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

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

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

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

Universal and Equal Suffrage, and Free and Secret Voting. How do basic election principles relate to changes in voting methodology? While these principles seem obvious and easy to implement, technical details of the voting system might corrupt them; for example - if the e-voting equipment records the time when a specific vote has been cast, this can corrupt secrecy of voting. The same concern relates to the paper record that is printed on continuous tape.

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

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

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

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

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

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

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

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

For these reasons, it is important that legislation requires electoral authorities to maintain their legal obligation to the citizens to organize a credible democratic election process, and therefore they must only enter contractual relationships with producers, suppliers and/or servicers of electronic technologies that ensure effective performance and give election authorities effective remedies where performance is in doubt. For example, legislation should state that contracts can only be entered with companies that have a demonstrated basis for reliable performance, such as rigorous testing of their equipment and/or use in elections, and that the producer must have enough units of equipment readily available to fulfill any contractual order on the dates specified for delivery in the contract or have a proven production record and no conflicting contracts so as to ensure timely delivery of equipment.

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

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

DEVELOPMENT OF REQUIREMENTS

Development of e-voting systems is a process that has several stages. They should all be public and transparent. The process will be fundamentally different depending on whether election authorities choose to purchase "off the shelf" products or to pursue development of a custom built voting system or a system that combines custom developed equipment with ready made products. Before that decision, election authorities should define general requirements of the electronic system, without proposing particular technical specifications. These general requirements should address secrecy, transparency, accountability, usability and security.

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

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

CERTIFICATION AND TESTING

Certification:

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

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

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

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

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

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

Testing:

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

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

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

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

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

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

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

Parallel Testing. Parallel testing is a test that is conducted on voting day (sometimes known as "hot audits"). Actual voting equipment is excluded from the voting process, isolated and monitored. Testers that register test votes on the equipment do not do so in secrecy, so that their choice can be manually counted and compared with the result of electronic "test vote."

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

PRODUCTION, DELIVERY AND MAINTENANCE

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

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

Decision to Utilize Electronic Voting. As stated above, the decision to utilize electronic voting directly affects fundamental rights of citizens and electoral contestants, and the decision therefore should be taken only after open public discussion that honors citizens' rights to participate in governmental and public affairs. Political contestants and nonpartisan election observer groups should have complete access to the process leading to the decision, and the process should allow for public input.

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

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

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

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

Subcontracting. The proposed contract should specify whether the selected producer is allowed to outsource production of certain components or certain services, and should provide transparency for any outsourcing. It also should specify clearly the relationship of the subcontractor to the producer and electoral authorities, accountability mechanisms that apply to the subcontractor, including remedies if the duties of the subcontractor are not performed on time and effectively, and include redress that the election authorities might seek.

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

HUMAN RESOURCES AND TRAININGS

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

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

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

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

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

TRANSPARENCY

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

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

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

COUNTRY NOTE:
Belgium 2006 - Reviewing E-Voting Systems

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

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

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

Even though internationally recognized technology standards are not settled, the right to access to information about essential elements of an election process is a component of internationally recognized rights to seek information, to participate in governmental and public affairs and to have genuine democratic elections. Election observation groups and political contestants therefore have a clear basis to seek transparency in electronic electoral technologies; the challenge is determining how to properly and effectively exercise those rights.[36]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SECURITY

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

Perhaps more than any other aspect of electronic voting technology, the security aspect is where the "devil is - truly - in the details." Even minor changes in security policies, access limits and the type of environment can lead to serious security breaches. Proper security analyses will require engagement of an IT security expert, who understands implications and limits of usage of technical security applications.

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

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

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

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

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

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

RECOUNTS AND CHALLENGES

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

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

In cases of discrepancy between the paper record and electronic record, the paper record should be taken as the legal representation of the voter's choice and should be determinative unless there is adequate evidence that the paper records were corrupted (for example, altered, substituted or "stuffed" as has been done with paper ballots).[42] Where it appears that the paper ballots are uncorrupted and there is a discrepancy with the electronic record, even where the paper record is legally dispositive, investigation of the cause of the failure of the electronic record is necessary.

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

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

OBSERVATION CAPACITY—STAFFING THE TEAM

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

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

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

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

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

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

Developing the capacity for evaluation of information technologies that may be introduced and used in the election system will require organizing a small team of experts. Ideally, the team would be led by an election monitoring expert, who has a good understanding of information technology. The role of the team leader will be to analyze the overall design of the system, to identify what type of expertise is required for detailed evaluation of the proposed voting system technologies and to identify the needed experts. In addition, the role of the team leader will be to design the observation strategy and serve as the main analyst of the observation findings. While the information technology team will vary depending on different technologies, one position is necessary regardless of which technologies are used — a computer security expert.

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

ELECTION DAY OBSERVATION

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

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

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

COUNTRY NOTE:

Venezuela 2006 - Electronic Voting in the Presidential Election

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

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

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

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

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

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

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

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

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

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

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

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

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

INTERNET VOTING

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

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

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

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

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

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

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

When voting via the Internet, computers that voters use do not store the votes. These computers serve only as a type of "interface" between voter and the server. The electronic record is created at the voter's computer, but these votes are immediately transferred to the server via the Internet and stored there. An observation strategy will necessarily have to be focused on security of the voting servers — systematic observation of voter's actions and ballot casting at computers on the polling day will be nearly impossible, which leave important gaps that themselves have implications for electoral integrity.

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

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

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

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

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