Implementing and Overseeing
Electronic Voting and Counting Technologies

Chapter 2.3: Implementing Electronic Voting or Electronic Counting in an Election

Lead Authors

Ben Goldsmith
Holly Ruthrauff

NDI NATIONAL DEMOCRATIC INSTITUTE

IFES International Foundation for Electoral Systems

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.

2.3 IMPLEMENTING ELECTRONIC VOTING OR ELECTRONIC COUNTING IN AN ELECTION

PROJECT AND RISK MANAGEMENT

The successful implementation of electronic voting or counting in an election should have as a first step a comprehensive project management plan. The management plan should detail the steps necessary for effective implementation, the schedule for these steps, as well as the personnel responsible for carrying them out, and should identify risks associated with the implementation and how these risks can be addressed. The management plan is a key resource for managers to gauge progress on the implementation of electronic voting or counting technologies and to respond to delays or obstacles. Observers should use the management plan to provide oversight of the implementation process and make recommendations in cases where deadlines are not being met according to schedule or where risks are not being effectively addressed.

Elections are a complex logistical exercise. The introduction of electronic voting and counting systems makes them even more complex. As has been discussed previously in this manual, the successful implementation of electronic voting and counting technologies depends on a broad number of variables working together properly. For this to happen, the project needs – first and foremost – effective planning and management.

Although this manual attempts to present the implementation of electronic voting and counting in as straightforward a manner as possible, discussing it as a coherent process, implementation is much more likely to involve a diverse range of processes conducted by official and unofficial actors, dispersed across institutions and over a lengthy period of time. The EMB must establish mechanisms for overall project management and coordination, including the establishment of a project management group. Such a group can include members from a diverse range of relevant institutions to ensure the smooth coordination and timely progress of the project. It is important that a broad set of skills be represented among members (e.g., project management, field operations, training, logistics, voter education, legal and IT) so that all aspects of various issues are considered.

Two important questions for the election authorities and other relevant institutions are whether to devote dedicated staff to the project and whether project staff should have additional responsibilities. While it may be preferable to have staff dedicated to the project, this might not be possible – particularly if there is a long time period between the project's conception and its actual implementation. In a situation where there are few or no dedicated project staff, the role and importance of a project management group is further increased.

From the outset, it is important that the EMB and other relevant institutions (or the project management group) conduct a planning process that lays out step-by-step how the project will be implemented, who (or which institution) has responsibility for each aspect and how long it is expected to take. The

project management group should draft a detailed plan and timeline that set out each stage of the project as well as the deadlines to be met. This plan and timeline should be publicly available and reviewed by EMBs on a regular basis to ensure that targets are being met.

As has been stressed elsewhere in this document, the amount of time necessary to implement electronic voting and counting systems should not be underestimated, and the schedule should include adequate time for public consultation, drafting of the necessary legal framework, feasibility studies, pilot testing, design of appropriate technology, security testing, expert review, personnel recruitment and training and voter education. The timeline should also include some flexibility in case some of the activities take longer than anticipated.

In Norway, for example, the Parliament decided in 2008 to pilot Internet voting during the September 2011 local elections. This timeframe provided several years for development of the system and pre-testing, with the 2011 pilot taking place in only 10 out of 429 municipalities. Despite this extended timeframe, the project team still had to work very hard to get the Internet voting system ready in time for the pilot.

FIGURE 15 – UK ELECTORAL COMMISSION REPORT CRITIQUES THE 2007 ELECTRONIC VOTING PILOTS

The UK Electoral Commission conducted comprehensive assessments of all of the voting pilots that it conducted between 2002 and 2007. After the 2007 pilots, it identi-

fied several project management issues that had not been properly addressed:

"It is important to realise that these remote e-voting pilots are complex IT projects and therefore require effective planning, testing and quality management. The lack of these elements in the 2007 pilots resulted in significantly higher implementation risks than necessary. The relative success of the delivery of the pilots, notwithstanding some issues at individual pilots, was due to the efforts of individual local authorities and their suppliers, combined with good luck."

The report also went on to emphasize the need to allow adequate time for testing prior to polling so that identified issues can be properly resolved and retesting can take place.

The project management group should meet on a regular basis to review the project's progress. Periodic progress reports can refer back to the original plan and timeline in order to assess progress made to date; these reports should also be publicly available. The project management group can further promote transparency by allowing political actors and independent observers to attend some of its meetings and by regularly briefing them on project progress.

It may be advisable to establish a broader consultation group in addition to the formal project management group. This group could be kept informed of project progress and consulted periodically and at key stages during the project implementation process. This consultation group should have a wide range of interests and organizations represented, such as members from academia, civil society and

professional communities. The inclusion of those who advocate against the use of electronic voting or counting in this consultation group will also be important, as those critical of the use of such technologies often raise important issues and perspectives that may need to be addressed to some extent.

A critical aspect of project management is developing a risk assessment tool that realistically identifies possible sources of risk, considers any mitigating factors and provides appropriate responses. This will involve a full assessment of potential security risks, as these are among the most critical for an electronic voting and counting system and should be carefully considered; but other types of risk related to logistical or even legal issues should be considered as well.

Although each project will have its own risks, a risk plan should address:

- Late or failed delivery of equipment and services
- Failure of security mechanisms (e.g., breach of electronic voting machine security)
- Missing, malfunctioning or late delivery of equipment, software or supplies (e.g., thermal paper, backup batteries, and other consumables)
- Communications failure (e.g., nonfunctioning Internet connection)
- Power failure
- Problems with staff recruitment
- Legal challenges to the use of the technology
- Public (mis)perception and resistance
- Attempts to discredit the system by those with competing commercial or political interests

A risk management plan should be developed early in the project and should be made publicly available so as to increase public confidence in the election authorities' ability to face the challenges of implementing electronic voting or counting.

Election observers should review the project management documents on an ongoing basis and highlight any gaps that they identify in a timely manner so that recommendations can be made to improve the project. Using the project documents, observers can also provide oversight to ensure that deadlines are being met and the project remains on track in terms of its timeline. Observers should also review the risk management plan to determine whether risks have been realistically anticipated and countermeasures devised. Observers are in a key position to provide this assessment of project progress to citizens on an ongoing basis through periodic statements. Such reporting can enhance public confidence in the election administration and also highlight any areas of concern in a timely manner so that action can be taken.

FIGURE 16 – ELECTRONIC VOTING PROJECT MANAGEMENT IN THE NETHERLANDS

Despite using electronic voting for many years in the Netherlands, the Ministry of Interior, which is in charge of the overall framework for elections, did not have the technical capacity to properly manage and regulate the electronic voting process. This allowed vendors too much control over the implementation of electronic voting technologies and the setting of standards for these technologies. Consequently, vendors and the ministry failed to update voting technology in line with modern security requirements, posing severe security risks to the electronic voting process.

In the late 1960s, the government of the Netherlands commissioned the Dutch Organization for Applied Scientific

Research (Toegepast Natuurwetenschappelijk Onderzoek, TNO) and the Dutch Apparatus Factory (Nederlandse Apparatenfabriek NV, NEDAP) to design and build a voting machine. At this time, the Ministry of the Interior was responsible for developing the overall legal framework for elections, including ensuring proper standards and regulation of voting machines. During the initial design process, the ministry chose not to set any legal requirements for TNO and NEDAP. The decision to award TNO and NEDAP creative control over the voting machines set a precedent that gave Dutch suppliers control over the ministry on electronic voting project management and regulation.

Voting machines became more widespread in Dutch elections during the late 1980s and 90s, yet the ministry's regulation of these technologies remained limited. Vendor influence over electronic voting continued in part because of the ministry's lack of knowledge of electronic voting technologies. The ministry was unable to determine clear requirements regarding functionality, integrity and security of voting machines. One paragraph of the Electoral Code (Article J33, paragraph 2) did specify some requirements for voting machines (such as secrecy of the vote and a clear candidate list; however, legislation was largely process-oriented and did not delve into standards or technical requirements.

The ministry also relied heavily on vendor knowledge when revising standards on electronic voting, which created a conflict of interest. TNO, for example, was included in a

ministry working group in 1990 and tasked with drafting technical regulations for voting machines. Their suggestions did not require any security features or a voter-verified paper audit trail (VVPAT), nor did it address the possibility of manipulation. Consistent with TNO's recommendations, no such regulations were ever issued by the ministry.
In the absence of a strong regulatory framework, vendors did not update technology in line with modern security requirements, making the voting machines vulnerable to internal and external security threats. The ministry also overlooked several warning signs with the voting machines, including problems that were discovered with similar machines in Ireland as well as concerns raised by the Electoral Council. For example, the Electoral Council advised the ministry on several occasions to introduce a certification procedure for the tabulation software. The ministry did not enact regulations in response to these concerns.

KEY CONSIDERATIONS: PROJECT AND RISK MANAGEMENT

FOR IMPLEMENTING BODIES

- ☑ Has a project management body been established?
- ☑ Are measures in place to ensure that project staff time can be sufficiently devoted to the project in the presence of other responsibilities?

- ☑ Has a detailed plan and timeline that sets out each stage of the project as well as the deadlines to be met been drafted? Is there some flexibility built into the plan in case some activities take longer than anticipated?
- ☑ Has a full management plan been developed?
- ☑ Will the plan be reviewed on a regular basis by the project management body to ensure that targets are being met?
- ☑ Is a broader consultation group with a wide range of interests and organizations represented also involved in the process of implementing the project?

FOR OVERSIGHT ACTORS

- ☑ Is the project management body inclusive and diverse so as to involve a broad set of skills in implementing electronic voting and counting?
- ☑ Has the project management body made its detailed plan and timeline available to the public so that stakeholders can hold management bodies accountable to targets and deadlines?
- ☑ Does the project management body produce periodic progress reports for the public, and/or are stakeholders invited to attend certain meetings to be briefed on progress?
- ☑ Has the EMB conducted a full security risk assessment, taking into account technical, logistical and legal issues that could arise?
- ☑ Has the risk management plan been made public so that stakeholders may provide input?

VOTER EDUCATION AND INFORMATION

Voter education and information are critical elements in building voters' confidence in newly introduced technologies. EMBs should be strategic and proactive in providing information on how to vote, how the overall system works, why the new technology has been adopted and methods to ensure the system's integrity. Voter education strategies should consider the target audiences and use different types of outreach methods based on how different segments of voters commonly access information. Particular consideration should be given to targeting groups, such as voters with disabilities, and rural and elderly voters, that may be less comfortable with technology. It is also important to provide opportunities for voters to try out the new voting equipment in person. Election observers have a responsibility to assess the adequacy and effectiveness of voter education efforts and make recommendations on how any identified gaps can be filled.

Experience has demonstrated that due consideration of voters' level of awareness about and confidence in the new technologies is key to the success of any electronic voting or counting system. It is not enough for voters to know how to vote using this new technology; they must also have confidence in the integrity of the technology that is being used. Providing voters with the information necessary to cast their votes using a new system efficiently and with confidence requires a comprehensive approach to voter education and public outreach. Such efforts should therefore start as early as possible and continue until results are certified.

The main responsibility for informing and educating voters rests with the EMB. As part of its overall strategy for introducing electronic voting and counting, the EMB should have an accompanying plan for educating and informing voters including the allocation of sufficient resources to meet these requirements. A public outreach strategy should include detailed information about how to

vote, as well as how the overall system works. The strategy should consider the target audiences and use different types of media (TV, radio, press, Internet) based on the country context and, in particular, the mediums through which different segments of voters most commonly consume information. Voters should also have an understanding of the reasons why the new technology is being adopted, how it will be implemented and what mechanisms have been included to ensure its integrity. EMBs should be proactive in providing such information, in order to demonstrate transparency and build public trust in the system.

The EMB's public outreach plan should also include strategies for how to react to stakeholder comments or media stories about the voting and counting technology that might not be accurate or that might cast doubt over the technology in some way. Particularly in the age of 24-hour news and viral social media, media officers have to be ready to provide any necessary clarifications at short notice. By responding quickly to critical stories about the voting or counting system, the EMB may be able to avoid a story gaining momentum disproportionate to its accuracy or relevance. It will be useful for EMBs to prepare a comprehensive booklet containing frequently asked questions (FAQ) and talking points regarding e-voting or counting, for use by election commissioners, senior managers and public relations personnel, which includes responses to common and often-repeated criticisms of electronic voting machines. Responses to questions from journalists or stakeholders should always aim to inform and educate, rather than to dismiss concerns.

In addition to a media campaign, the EMB should identify as many opportunities as possible for voters to try out the new voting equipment in person. Information transmitted by media cannot replace the experience of trying the equipment in real life. As mentioned above, usability tests as well as pre-pilot and mock elections are good initial opportunities for voters to try out and become comfortable with the equipment, as well as to receive assistance on how to use it. Election officials should be creative and take advantage of all possible opportu-

nities to share information on the electronic systems throughout the pre-election period. Voters are likely to be curious about the new technology and interested in trying it for themselves. In Geneva, authorities installed test machines using the new Internet voting interface in the waiting room of the passport service office so that citizens could test the voting system while they waited.

Since increased accessibility of elections is a frequently cited goal of electronic voting and counting projects, particular consideration should be given to reaching out to target groups with special voter education messages and campaigns. Voters with disabilities and elderly voters should be informed about any new functionality that may facilitate their ability to vote unassisted, and should be provided with relevant information about any further steps they need to take prior to voting. Elderly voters may be particularly hesitant to use new technology, and special efforts should be made so that they feel comfortable with the equipment. Voters from minority language groups should receive voter information in their own languages to inform them about new opportunities to use ballot interfaces in alternative languages. Specific TV and radio campaigns should also provide information for illiterate and low-literacy voters, to explain how they will be able to vote using the new system (e.g., by displaying candidate photos or party symbols on the ballot) and to encourage their participation, given that they may be unfamiliar or uncomfortable with electronic technologies.

The adoption of new election technologies may offer opportunities for election officials to reach out to young voters and encourage their participation. In addition to voter education campaigns in the traditional media, voter education efforts aimed at young voters should take full advantage of social media.

While the primary responsibility for voter education rests with the EMB, civil society groups may also be usefully engaged in educating voters about electronic voting and counting systems. To play this role, civil society groups must have access to accurate and timely information from the EMB about how the

new system will work and what voter education messages should be disseminated. Voter education messages should be carefully formulated to transmit the most necessary information in a user-friendly format.

Voter information should also be available at polling stations – including leaflets or posters that explain to voters how to cast a ballot using the new equipment. Polling officials should be well prepared to answer any questions about the voting machines – such as how to use the machines, how the vote is counted and transmitted and how the security and secrecy of the vote are protected. Providing this kind of information will help to increase voter confidence and trust in electronic voting and counting.

As representatives of citizens, domestic election observer groups have a particular responsibility to ensure that the public is adequately informed about elections. Election observers should assess the provision of voter education by election officials throughout the election process and should determine whether adequate information has been provided. Such information can be collected by long-term observers, and data may also be available in public opinion surveys. If any gaps in knowledge or among particular target groups or regions are identified, election observer groups should make recommendations to election officials about how such gaps can be filled so that voters have the information they need to vote and have confidence that their votes will be accurately reflected in the election result.

FIGURE 17 – MEDIA ENGAGEMENT IN THE PHILIPPINES

When the Philippines began to implement its new optical-scan ballot-counting system, the Commission on Elections's (COMELEC) Project Management Office embarked on a widespread public acceptance program with three objectives: first, to educate the electorate on how the automated electoral system worked; second, to promote acceptance of the system as a guarantee of speedy and credible results; and third, to manage expectations. Dissemination of messages for the campaign through private TV networks was critical for its success, as was ongoing engagement with the media on Election Day. While the COMELEC's policy of open and transparent engagement with the media was challenging at times, the Commission believed that it was a considerable asset to engage and inform the media in such an open manner.

The three major TV networks considered it part of their corporate social responsibility to spread information about the new ballot-counting machines, and as a result, developed and aired information clips in the run-up to the election at no cost to the government. The core content of these information clips was approved by COMELEC to ensure accuracy and consistency. One network released a music video that featured a well-known

dance troupe singing a catchy tune about the automated election system. This tune became so pervasive that it was one of the most recognizable tunes in the country at the time. Even children knew the lyrics to the song, and voters waiting in line on Election Day were observed singing it together.

On Election Day COMELEC deployed over 40,000 technical staff to monitor how the new technology was working. All issues were reported to a situation room in the capital. COMELEC adopted a policy of transparency about these incidents. A press center was placed in the situation room, and COMELEC kept the press fully informed about any reported problems, even those that did not reflect well on COMELEC. The result of this was that the media were well informed throughout Election Day about issues that had arisen as well as COMELEC's response to these issues, and the coverage that this provided meant that COMELEC was easily able to get airtime to explain what was being done about reported problems.[36]

36 Taken from a presentation by Gregorio Larrazabal, former COMELEC commissioner.

KEY CONSIDERATIONS: VOTER EDUCATION AND INFORMATION

FOR IMPLEMENTING BODIES

- ☑ Has a comprehensive plan for educating and informing voters about the new technologies been developed and have sufficient resources been allocated to conduct voter education and information activities?
- ☑ Does the public outreach strategy include detailed information about how to vote as well as how the overall system works?
- ☑ Have strategies been developed for how to react to stakeholder comments or media stories about the voting and counting technology?
- ☑ Is a set of Frequently Asked Questions (FAQ) available for reference to election commissioners, senior managers and public relations personnel that include responses to common and often-repeated criticisms of electronic voting machines?
- ☑ Are opportunities available for the public to engage with the new voting equipment in person in the pre-election period?
- ☑ Are targeted efforts in place to address voter education for specific populations such as the elderly, minority ethnic/language groups, and youth?
- ☑ Is voter information available at polling stations?
- ☑ Are polling officials sufficiently prepared to answer any questions about the voting machines?

FOR OVERSIGHT ACTORS

- ☑ Has the EMB developed a comprehensive plan for voter education, including sufficient time and resource allocation?
- ☑ Does the EMB strategy for voter education identify target audiences and incorporate a variety of media sources and other mediums through which those target audiences commonly consume information?
- ☑ Has the EMB provided opportunities for citizens to engage with the new voting equipment in person?
- ☑ Has the EMB made extra efforts to engage target groups, such as the elderly and disabled, via specialized voter education messages and campaigns? Have voters from minority language groups received voter information in their language?
- ☑ Have civil society groups actively engaged in voter education efforts themselves, and have they received the necessary technical information on the new technologies from the EMB to produce effective voter education materials?
- ☑ Have civil society assessed the adequacy and effectiveness of EMB public outreach efforts? Has any public opinion polling been conducted to gauge the readiness of voters?

SOFTWARE AND HARDWARE MAINTENANCE, STORAGE AND UPDATE

Vital functions such as secure storage of electronic voting and counting equipment, maintenance, upgrades, and reconfiguration need to be performed in the period between elections. Care should be taken to ensure that these processes are planned for and that appropriate procedures are put in place to undertake these functions securely and with as much transparency as possible. EMBs should also focus on identifying staffing and training needs to address maintenance and storage as much as possible without the support of vendors.

Equipment used for electronic voting or counting will remain unused between elections, possibly for long periods of time. In the case of electronic voting or counting machines, these machines will need to be placed in storage between elections. EMBs may choose to store this equipment centrally or in regional storage facilities, depending on the logistics involved in moving the equipment and the availability of suitable storage locations.

The EMB will need to be aware of any environmental conditions that are required when storing the electronic voting or counting equipment, as the equipment may be sensitive to extremes of temperature and humidity or may require dust-free environments. Finding suitable storage locations may be especially challenging in very hot countries, where extreme heat may degrade the reliability of the equipment.

Even where a relatively small amount of equipment is used, such as for Internet voting systems, it will be important that this equipment is placed in a secure location between elections so that the perception and reality that the equipment could be tampered with can be countered. The storage location(s) should be guarded and should have appropriate and clearly identified access

control systems. All access to the storage location should be logged, with the reasons for the access clearly identified in the log. It is good practice for party representatives and observers to be invited to supervise any routine access to stored electronic voting or counting equipment; this may also take place in the storage locations due to the space requirements of maintaining or configuring a large number of machines.

Electronic voting and counting machines need to be maintained and checked, especially when left for long periods of time between elections. Machines may also need to be upgraded through their life cycle, which may be fifteen to twenty years. Electronic voting and counting machines will need to be configured before elections so that they are programmed for the types of elections being conducted and the political entities on the ballots. Observers and party representatives should be provided access to these configuration processes.

The conduct of this checking, maintenance, upgrade and configuration may be covered by the supply contract for the electronic voting or counting equipment, or it may be the responsibility of the EMB. In order to avoid dependence on suppliers, it is preferable that the election management body handle these functions. The development of the capacity within the EMB to conduct these tasks may require significant staff training. Thus, it may decide to build this independent capacity over the course of several elections, with reduced dependence on the supplier as time progresses.

KEY CONSIDERATIONS: SOFTWARE/HARDWARE MAINTENANCE, STORAGE AND UPDATE

FOR IMPLEMENTING BODIES

- ☑ Is the EMB aware of the environmental conditions that should be addressed when storing the electronic voting or counting equipment?
- ☑ Are suitable storage locations available, and are these storage locations guarded and do they have appropriate and clearly identified access control systems?
- ☑ Is a maintenance schedule for the equipment established and implemented?
- ☑ Is all access to the storage location logged and explained?
- ☑ Are the electronic voting and counting machines configured before the elections so that they are programmed for the type of elections being conducted and the political entities on the ballots?

FOR OVERSIGHT ACTORS

- ☑ Has the electronic equipment been stored in a secure location between elections in a manner that prevents unauthorized tampering?
- ☑ Are party representatives and observers allowed to monitor routine access to stored electronic equipment?

- ☑ Do observers and party observers have access to monitor the process of configuring and upgrading machines before elections?
- ☑ Are the checking, maintenance, upgrade and configuration of equipment conducted by the EMB or the vendor? If by the vendor, does the EMB have the capacity to properly oversee these processes?

TESTING, SOURCE CODE REVIEW AND CERTIFICATION

EMBs must ensure that there is appropriate and systematic testing of electronic voting and counting systems in the period before an election so that problems can be highlighted and addressed in a timely fashion before Election Day. EMBs should also provide access to independent experts to review the source code in order to engender transparency and build confidence in the electronic systems. EMBs may also require independent bodies to certify the electronic voting and counting systems prior to their use. Both testing and certification are time-consuming processes, and EMBs should ensure sufficient time before Election Day for these steps in the process to take place. Observers and parties should ensure they have the expertise and capacity to comprehensively inspect the source code and assess the testing and certification processes.

Testing and Source Code Review

Ensuring that electronic voting or counting systems function correctly and generate accurate results based on the votes cast is critically important. Not only must election management bodies ensure this, but they also must convince key electoral stakeholders that this is the case so that they will trust and accept the results. Unlike other electronic transactions, one cannot check afterward that

his or her vote was recorded correctly.[37] For example, with electronic banking, people can check their statements to see if any incorrect transactions were made and can have mistakes corrected. The need for a secret vote denies the possibility for this level of transparency.

As a result, the EMB needs to make additional efforts to test the electronic voting or counting system before it is used to ensure that it works correctly. Figure 5 in the Overview section shows the different kinds of tests that the Council of Europe recommends for electronic voting and counting systems; these include acceptance testing, performance testing, stress testing, security testing, usability testing and source code review.

All of these tests will be conducted by, or on behalf of, the EMB. The more these tests can be conducted by the EMB, the better, as long as it has the competency to do so. If any aspect of testing is outsourced, EMB personnel must remain engaged and provide oversight of the testing process. From a transparency and confidence-building perspective, it is also useful to have an external, independent body conduct some level of testing. In the US, local EMBs carry out testing before each election. In Maryland, this testing consists of preparing and configuring the machines, casting hundreds of votes on each voting machine, and producing and checking results on the voting machine as well as through the central tabulation system, before clearing the voting machines of voting data, sealing them and securing them so they are ready for use in the election.

While different EMBs will take varying approaches to the testing regime that is used, it is vital that the EMB does some level of testing and that testing is done

37 It should be noted that there are electronic voting and counting schemes designed to provide this level of verifiability for voters (such as Scantegrity, Prêt à Voter and Punchscan voting systems). However, these systems can be seen as quite complex for voters and have challenges in terms of scalability when it comes to larger elections. The crux of the challenge for such end-to-end verifiable voting schemes is to provide verifiability without violating the secrecy of the vote. This is a particular challenge in countries where employers or others could demand that a voter use such mechanisms after the election to prove she or he voted as instructed or where vote-buying schemes could easily be adapted to take advantage of such mechanisms.

before each election. Testing before each election is necessary to check the election-specific configuration and also to deal with any technology changes, which is especially important for Internet voting where new browsers as well as updated versions of existing browsers may need to be accommodated.

Full system testing also needs to take place sufficiently in advance of elections to enable the remedy of any problems encountered. It is also prudent to do a final check of equipment closer to Election Day. In the 2010 Philippine election, during which electronic counting machines were being used for the first time, the machines were scheduled for final testing and sealing one day before the election. The COMELEC IT Department decided to test some machines earlier and discovered less than a week before the election that a bug in the configuration of the scanning software would cause the machines to register votes incorrectly. The decision to do early testing and sealing detected the problem in time, so that new compact flash cards could be distributed nationwide, rescuing the election from disaster.

Access to the source code for electronic voting and counting applications may also be made available so that independent experts can check that no errors exist in the source code (see the previous discussion of open source code in the "Security Mechanisms" section). Additional scrutiny of the source code may help to identify the existence of any errors, oversights or malicious code, but will also importantly help to build confidence in the electronic voting or counting systems by increasing transparency.

Fully open source code is not necessary to provide these confidence-building mechanisms, but it is the more preferable option. Should open source code not be used, experts representing key electoral stakeholders (political actors and civil society) should be allowed sufficient access to review the source code and should not be restricted in reporting their analysis of its content by the use of any nondisclosure agreements. The EMB may also decide to engage

an external body to conduct an independent review of the source code as a confidence-building measure.

All of the reports on the testing of electronic voting or counting systems should be made available for review by political actors and observers. Again, this transparency will help to build confidence in the system.

It is important to recognize that conducting these different kinds of tests takes a significant amount of time and resources. Electronic voting and counting systems are complex; and especially when new systems are developed, they will often contain errors that need to be corrected. Each time an error is identified and corrected, it may be necessary to conduct the full test process again, as even a small change may lead to unforeseen consequences. Therefore, sufficient time and resources must be allocated for this testing to take place, as well as for any corrections and retesting to be implemented.

FIGURE 18 – SOURCE CODE REVIEW MECHANISMS IN BRAZIL

Brazil's electoral commission (Tribunal Superior Eleitoral, TSE) is credited for making the source code to its electronic voting system available for review by electoral stakeholders. In addition to providing access to the source code, the TSE invites computer scientists and interested parties to find system vulnerabilities. Despite these efforts, electoral stakeholders believe that the TSE can take further steps to ensure greater transparency in this process. Among the steps

suggested are providing more time for experts to analyze the system and source code, and placing fewer restrictions on public comments resulting from the expert analysis.

The Tribunal Superior Eleitoral (TSE) takes steps to provide transparency for electoral stakeholders by offering access to the source code for the electronic voting system as well as opening the system for hacking competitions. However, the TSE has come under some criticism in recent years because of the manner in which these initiatives have been implemented, which has led to calls for greater transparency with regard to technical aspects of the electronic voting system.

Brazilian electoral law stipulates that the source code should be made available for review by political parties and the Brazilian bar association (Ordem dos Advogados do Brasil, OAM). Electoral stakeholders in Brazil believe that the TSE failed to meet this requirement for the 1996, 1998, and 2000 elections. The TSE did start to make the source code available for review after the 2000 elections, but the manner in which the source code is provided has also come under some criticism. Computer scientists criticize the fact that auditors must sign a nondisclosure agreement and, consequently, any problems found during the audit are not made public. Auditors also point out that only a few days are given for auditing and the examination of the code occurs in very controlled conditions on the TSE's computers, which are insufficient to comprehensively examine the code. In some cases, the code was modified after it had been given to the parties for review.

To its credit, the TSE has gone beyond its legally mandated requirements to make the source code available for review to independent computer scientists. These computer scientists have generally found the system to be robust, but have made several recommendations to improve the system, including instituting a voter-verified paper audit trail (VVPAT) to enhance the auditability of the system. The TSE has thus far resisted instituting VVPAT in the electronic voting system. Since 2009, the TSE has also organized hacking competitions, inviting computer scientists and other interested parties to find external vulnerabilities in the electronic voting system, but there have been complaints that the TSE does not allow enough time (three days are provided) to thoroughly test the system and that those participating in the competitions do not have enough time to analyze the code.

Certification

In addition to comprehensive testing of electronic voting and counting technologies prior to use, it is good practice to have these systems certified prior to use.[38] The purpose of certification is similar to testing in that it determines whether the electronic voting or counting technology operates effectively. The difference is that an authority independent of the EMB, political parties,

38 The Council of Europe (2004) recommendation on e-voting requires that, before any e-voting system is introduced, it be certified by an independent body to verify that it is working correctly and meets all necessary security measures (Recommendations 25 and 111).

the government and suppliers conducts certification. The certification process should be carried out in an open and transparent manner and is intended to build confidence in the operation of the electronic technology.

This certification process will provide independent assurance that the electronic voting or counting solutions meet a certain set of standards. If any changes are subsequently made to the hardware or software, the certification process will need to be completed again, although it may be possible to conduct an abbreviated recertification if changes are minimal and can be categorically identified. Time is again an issue, and the process of certification may take between six and 12 months, depending on how many issues are found that require fixing and how complex the system is. While certification can be a strong mechanism for ensuring the integrity of the electronic voting or counting system and in building trust in the system, it does limit the flexibility of the EMB in making last-minute improvements to the system, as any such improvements would require recertification.

A number of institutions, such as university information technology departments or technology institutes, could play a role as certifying bodies. It is important that the process of certification is well defined. In some countries the certifying institutions themselves have to be preauthorized and must meet a series of standards for the work they will conduct certifying electronic voting and counting technologies. Clear guidance will need to be developed for certifying institutions on the certification requirements (which should be publicly available), the records they should make of their findings, the consequences of a product failing to comply in some way, the mechanisms for a vendor to resubmit after failing certification and the openness of the certification process and certification reports.

FIGURE 19 – E-VOTING CERTIFICATION PROCEDURES IN THE UNITED STATES

In 2005 the U.S. Election Assistance Commission (EAC) established Voluntary Voting System Guidelines (VVSG) to accredit the functional capabilities, accessibility and security requirements of electronic voting and counting systems. These requirements have to be met for systems to gain EAC certification, and the EAC has accredited several testing labs to conduct the certification process. Individual states, however, may decide whether or not to use VVSG for the electronic voting and counting systems employed in their elections.

Electronic voting systems, both direct-recording electronic and optical-scan ballot counting, are used extensively throughout the U.S. Under the Help America Vote Act (HAVA) of 2002, the Election Assistance Commission (EAC) was established and empowered with adopting voluntary voting system guidelines, accrediting voting system test laboratories and certifying electronic voting and counting systems. In 2005 the EAC adopted the Voluntary Voting System Guidelines (VVSG), thereby establishing standards relating to the functional capabilities, accessibility and security requirements of electronic voting and counting systems. These are the standards that the EAC's certification process applies to systems. The VVSG contains approximately 1,200 requirements that systems are required to comply with in order to obtain certification by the EAC.

The EAC does not test electronic voting and counting systems itself, but provides accreditation to a number of testing labs which conduct the certification process. Suppliers of electronic voting and counting systems must apply to one of the approved testing laboratories in order to obtain accreditation for their system. Certification requirements under the VVSG are quite rigorous, and systems may initially fail to meet the requirements. In such cases the system must be modified and resubmitted through the certification process. Typically it will take between six and 18 months to obtain certification for a system, although there is no guarantee that a system will ever be certified.

It is important to note that this EAC certification process is voluntary in the U.S., with each state deciding if it will make certification by the EAC a requirement for the voting and counting systems used in the state's elections. Each state may also apply state-level certification requirements. This state-level certification process will typically be used to ensure that electronic voting and counting systems comply with state-specific electoral legislation. It may also be used to complement the EAC certification process or as an alternative to certification by the EAC.

KEY CONSIDERATIONS: TESTING, SOURCE CODE REVIEW AND CERTIFICATION

FOR IMPLEMENTING BODIES

- ☑ Are necessary levels of testing of the electronic voting and counting systems going to take place, including, as recommended, acceptance testing, performance testing, stress testing, security testing, usability testing and source code review?
- ☑ Are any external independent actors involved in the review process?
- ☑ Is there a plan in place to conduct full system testing sufficiently in advance of the elections?
- ☑ Is access to the source code also made available to independent experts and stakeholders to check for errors or malicious code?
- ☑ Will a certification process be conducted by an authority independent of the EMB to provide independent assurance that the electronic voting or counting solutions meet a certain set of standards?
- ☑ Have sufficient time and resources been allocated for the testing and certification process to address any issues that are identified during these processes?

FOR OVERSIGHT ACTORS

- ☑ Which tests are conducted?

- ☑ Does the EMB conduct the tests or does the vendor? If the vendor, does the EMB remain engaged and provide oversight of the process?
- ☑ Are tests conducted sufficiently in advance of elections so that any problems encountered can be addressed?
- ☑ Is the source code for the electronic technologies open source? If not fully open source, do observers and party representatives have sufficient access to inspect the source code, including not being restricted in reporting their analysis of its content by the use of any non-disclosure agreements? For their part, election observers and parties should ensure they have the capacity and/or expertise to comprehensively inspect the source code.
- ☑ Are all test reports available for review by political actors and observers?
- ☑ Is an independent certification process conducted, and, if so, are the processes and results publicly available?

ELECTION DAY (SETUP, TESTING, SECURITY, TROUBLESHOOTING)

Election officials should ensure that sufficient resources are in place at every polling station to receive and properly operate electronic voting equipment on Election Day. These resources should include sufficient personnel (including technicians) and processes to address any issues that may arise with the proper operation of the electronic equipment on Election Day. Observers should assess whether all procedures are appropriately followed in the setup, operation and closing of electronic voting equipment at the polling station, whether the technologies are usable and accessible for all voters and whether sufficient measures are taken to ensure election security.

Electronic voting and counting equipment should be delivered to polling stations just prior to Election Day and issued to a designated person (usually the head of the polling station committee) using appropriate handover procedures and documentation. As electronic voting and counting equipment is considered to be sensitive balloting material, all access to the equipment must be controlled and recorded, and proper security precautions must be in place to secure the machines until voting starts. Party representatives and accredited observers should be permitted to witness the delivery and setup of voting and counting equipment.

On Election Day, polling officials follow procedures to initialize the voting and/or counting machines. Typically there is a demonstration in front of any party representatives and/or observers present to show that there are "zero votes" recorded in the machine during the initialization process prior to the start of voting. Test elections are also sometimes conducted for party representatives and observers to show that ballot choices are accurately recorded.

A sufficient number of technicians should be available to provide assistance, either on the premises, on call or via telephone hotlines should officials have any problems with the setup, initialization or functioning of voting and counting equipment. Specific procedures and contingency plans must also be in place for the possibility that a voting or counting machine does not work and cannot be fixed. These could include the rapid replacement of nonfunctioning or malfunctioning machines from a store of spare machines kept under the same security protocols, postponement of elections in that polling location or the use of alternative means of voting, such as paper balloting.

During the voting period, party representatives and observers should assess whether polling officials are adhering to proper procedures for processing voters, providing assistance when necessary and respecting all security safeguards. It is particularly important for observers to consider whether the secrecy of

the vote is being respected – both through the arrangement of the polling station and the way that assistance is offered to voters. Observers should also pay particular attention to any technical problems that arise with the equipment during the voting and how such problems are resolved. The introduction of technology into the voting process is likely to increase the possibility of technical problems, but they should be dealt with efficiently and according to procedures, in a manner that does not interrupt the voting process if possible.

Security safeguards during voting should include procedures for controlling access to electronic voting and counting equipment. It should be clear who is allowed access to machines in any given situation (for instance if repairs are needed), and any access should be properly documented in the polling station protocol. Safeguards such as authentication codes and tamper-proof seals on any external ports should also be used.

While electronic voting and counting equipment should have been already submitted to several rounds of usability testing during its development and in any pilots, Election Day is the real test for how well voters interact with the technology. Observers should pay close attention to the accessibility of electronic voting and counting machines, including the experiences of special groups of voters such as those with disabilities, and elderly, illiterate or minority-language voters.

At the close of voting, officials should carry out closing procedures for the electronic voting and counting equipment. Polling officials should carry out the relevant command to close voting on each voting (or counting) machine. Depending on the type of equipment, individual machines may produce a tally sheet of results for that machine. Should each machine produce its own tally, these figures should be aggregated into a polling station results protocol.

The printouts for each voting or counting machine should be posted outside the polling station, together with the overall results protocol for the polling

station. Party representatives and observers should be given copies of results printouts or should be permitted to copy the figures. As in traditional voting, results protocols should be signed by members of the polling station commission. Electronic voting and counting machines may also produce an activity log, detailing all actions taken on the machine during Election Day. These should also be available for observers.

FIGURE 20 – ELECTION DAY PLANNING IN THE PHILIPPINES

In the Philippines, the nationwide shift to electronic counting machines led to several logistical challenges during the 2010 national election. Due in part to budgetary constraints, the Commission on Elections (COMELEC) was unable to procure enough precinct count optical scan (PCOS) machines to accommodate as many polling locations as under the manual election system. On Election Day the reduction in polling locations led to long lines, shortages of poll workers and poorly managed technical support for PCOS machines. There were also challenges in providing Election Day support for the electronic counting machines and in transmitting the results at the close of polling.

The transition to nationwide use of electronic counting machines during the 2010 Philippines elections presented a number of logistical challenges for election officials in preparation for Election Day. Due in part to budgetary constraints,

the Commission on Elections (COMELEC) was only able to lease enough precinct count optical scan (PCOS) machines to accommodate approximately 80,000 precincts. As a result, precincts had to be clustered, significantly reducing the number of precincts, down from approximately 250,000 in 2007. Instead of 200 voters per precinct, there were up to 1,000 voters per precinct. On Election Day, voters across the country had to wait for hours in line. Although precincts were clustered, the number of polling station workers per precinct was not increased accordingly, which compounded the already lengthy wait times. International and domestic observers noted that this may have led to disenfranchisement of voters who could not wait or decided against waiting in long lines.

The use of PCOS machines also required significant preparations for providing real-time technical support on Election Day. A number of issues arose on Election Day, including missing or drained batteries, paper jams and precincts running out of thermal paper. Some incidents resulted in PCOS machines not being used at all on Election Day. Although the vendor, Smartmatic, claimed to have recruited and trained over 48,000 technical assistance providers to be deployed on Election Day, many election officials complained that most PCOS technicians did not have the proper skills to assist them with mechanical problems that occurred during Election Day processes.

Data transmission and results tabulation also presented enormous challenges on Election Day. Although the transmission was in general fast and efficient, there were reports of transmission failures, delays or the inability of the consolidation centers to receive data. Problems emerged, in part, due to the fact that the reporting hierarchy required for electronically transmitting election results was the same as that used in manual elections. This system stipulated that data be reported from precinct to municipality to province to central server. According to several post-election assessments, this reporting hierarchy should have been adjusted to allow for direct transmission to a central server, which would have been much more timely and cost-effective.

FIGURE 21 – NONPARTISAN CITIZEN OVERSIGHT OF ELECTIONS IN THE PHILIPPINES

The experience of citizen observer groups during the 2010 Philippine elections points to a number of challenges oversight groups face as they transition from observing paper-based elections to observing elections that utilize electronic voting and counting technologies. In the 2010 national election, these groups observed several aspects of the electoral process, especially during the pre-election stage and on Election Day. However, they faced significant internal and external challenges in effectively observing the mechanics of the new process. The foremost lesson learned was that bet-

ter coordination and cooperation among civil society actors could have helped pair IT expertise with election-monitoring experience and methodologies to more effectively observe the new election system.

Just as the transition from manual to electronic technologies in the Philippines triggered significant adaptations among EMBs, it also necessitated major changes in the organizational structures and methodologies of civil society actors. By 2010, some groups had accumulated decades of experience monitoring manual elections, such as the country's first observation group, the National Citizens' Movements for Free Elections (NAMFREL), but they had to quickly attempt to acquire and apply IT knowledge to their efforts. Other groups, including the Center for People Empowerment in Governance (CenPEG), brought their IT expertise to the new electoral environment, but they lacked election observation experience. In addition to the challenge of acquiring IT knowledge, several groups faced challenges observing the election due to a lack of accreditation by the COMELEC, which only provided official accreditation status to one group, the Parish Pastoral Council for Responsible Voting (PPCRV). While many organizations still monitored without accreditation, this greatly restricted observer groups' access to a number of critical parts of the electoral process.

Despite these internal and external challenges, civil society groups were proactive in promoting transparency and accountability from the early phases, including during legal

reforms, system design, and procurement, through Election Day processes and the post-election period.

In the years leading up to the 2010 elections, as the Philippines adapted its legislative framework and standards to accommodate electronic technologies, civil society organizations such as NAMFREL provided input on reforms. In the pre-election period, IT-focused groups such as CenPEG, through its "Project 30-30", advocated for measures to improve the integrity of the new automated system. For example, CenPEG attempted to review the source code used for the new automated system. The COMELEC, however, regulated access to the source code and did not agree to have the source code taken out of its headquarters, citing intellectual property rights and security concerns. CenPEG subsequently filed a legal complaint against the COMELEC. The Supreme Court eventually issued a ruling after the elections directing the COMELEC to provide source code access to CenPEG. After years of court battles and negotiations between the COMELEC and Dominion Voting Systems, which owns the source code, the COMELEC offered the source code for public review on May 9, 2013, just four days before the May 13 general elections. Watchdog groups and some political parties commented that the source code release had come too late for a meaningful review.

To monitor the transmission and tabulation processes, several election observation groups had planned to collect the results at the precinct level and compare them to the

precinct-level results published on the COMELEC's website. However, the comparison of results for a sizeable portion of precincts was not possible, in part because observers were not able to collect election results in many locations. In a number of cases, poll workers refused to provide PPCRV's accredited observers with a copy of the election results. Unaccredited observers from NAMFREL; Bantay Eleksyon, a coalition of 47 organizations formed by the Consortium on Electoral Reforms; and other groups had an even more difficult time entering polling stations and obtaining copies of election results. Another major obstacle was that, on election night, the COMELEC stopped posting precinct-level results to its website after approximately 90 percent of the results had been posted. Then the COMELEC took the data down. Before it was taken down, a group of IT experts created a mirror image of the site and, upon later analysis, found a number of anomalies and missing data. COMELEC has never explained why the full precinct-level results were not released publicly, nor why the website had a number of data errors. This raised serious concerns among some political contestants and citizen observation groups.

Following the 2010 elections, civil society groups reported a number of lessons learned from their observation efforts. In particular, they emphasized the need for better coordination between traditional election observers and IT experts so that they could take advantage of each other's comparative strengths, knowledge and networks. Citizen observation groups, particularly those which lacked IT capacity prior to

2009, did not sufficiently refine their monitoring methodologies and tools to take into account the new technologies of the 2010 elections. In many cases, they did not have the specific expertise to anticipate where problems or vulnerabilities could occur, or to develop the tools and observer training necessary to collect evidence of these problems. Similarly, IT experts and groups with higher IT capacity did not have the experience or organizational structures of the more experienced observation groups, which limited their ability to effectively observe processes during the days immediately surrounding Election Day.

KEY CONSIDERATIONS: ELECTION DAY (SET-UP, TESTING, SECURITY, TROUBLESHOOTING)

FOR IMPLEMENTING BODIES

- ☑ Are a sufficient number of technicians available to provide assistance, either on the premises, on call or via telephone hotlines should officials have any problems with the set-up, initialization and function of voting and counting equipment?
- ☑ Are specific procedures and contingency plans in place for the possibility that a voting or counting machine does not work and cannot be fixed?
- ☑ Is it clear who has access to machines in any given situation, and is there a process for properly documenting any access in the polling station protocol?

- ☑ Will safeguards such as authentication codes and tamper proof seals be used on any external ports?
- ☑ Are closing procedures to be carried out by polling officials clearly defined with the relevant command to close voting or counting on each machine?
- ☑ If individual tally sheets are produced, will the results be aggregated into a polling station results protocol?

FOR OVERSIGHT ACTORS

- ☑ How have observer groups and political parties had to change their election day strategies to effectively monitor new technologies on election day? Do they have the necessary technical expertise?
- ☑ Are machines secure during and after the transfer from storage to the polling location until voting starts? Are observers permitted to observe the delivery of equipment?
- ☑ Is there a demonstration to show that no votes have been recorded in the machine prior to the start of voting?
- ☑ Do polling officials follow procedures for set-up, processing of voters and closing the polling station, and do observers have access to all of these processes?
- ☑ Is secrecy of the vote ensured, both through the polling station arrangement and the way that assistance is offered to voters?
- ☑ If problems with equipment arise, are polling officials or authorized technicians capable of resolving them efficiently, according to procedures, and without interrupting the voting process?

- ☑ Is access to the equipment and sensitive materials sufficiently secure, controlled and recorded?
- ☑ How accessible and usable are electronic machines for voters? In particular, what are the experiences of special groups, such as disabled, elderly, illiterate or minority language voters?
- ☑ Are printouts for each voting or counting machine posted outside the polling station, together with the overall results protocol for the polling station? Are party representatives and observers given copies of results printouts or at least permitted to copy the figures?
- ☑ Are electronic voting and counting machines activity logs available for observers?
- ☑ How has the implementation of new technologies affected the conduct of voting? Have any new problems been introduced that were unforeseen, and if so, how did the EMB respond?

TABULATION

Electronic voting and counting technologies allow for quicker tabulation and transmission of results when compared to paper-based systems, but election authorities must ensure that these processes are undertaken with as much transparency as possible and with a strict focus on the security of results data. Results can be transmitted either through secure communication channels or by encrypted data. And as these security measures are taken to safeguard the data, election authorities must ensure that observers and oversight groups are able to observe the data being uploaded. Results data from the polling station to central level should be made publicly available online.

Once votes from electronic voting or counting machines have been aggregated at the polling station level and recorded in a polling station protocol, they must be delivered in a secure and efficient manner either to the next level of the election administration or to the central election authorities for tabulation, depending on the election legislation.

Results transmission is likely to be simultaneously conducted through more than one channel. Often unofficial results are transmitted first, and then official results follow. Results may be transmitted electronically through the Internet (using a modem or satellite device) or by mobile phone. Security measures should be in place to prevent any interference with the electronic transmission process. For instance, data may be encrypted, and secure communication channels may be used, along with digital signatures to verify the integrity of the data that is received. At the same time, hardware devices such as memory cards or memory sticks may also be transported to the next-level election commission, with encrypted and signed data. Paper results protocols may be sent through an additional channel.

At the next stage in the tabulation process, for instance at a district-level tabulation center, election officials will feed results from polling stations into the system. If results have been submitted electronically or using electronic hardware, then results may be automatically uploaded without the need for any data input, saving time and avoiding errors.

The tabulation process at all levels should be fully transparent for party representatives and observers. Observers should be able to witness the data being uploaded or entered into the tabulation computers. If observers have collected results protocols from polling stations, they should be able to verify that these figures have been properly recorded at each higher level of the tabulation process. The full tabulation from the central level down to the polling station should be publicly available on the Internet in an easily verifiable format.

Depending on the technology adopted, the tabulation process when using electronic voting and counting systems has the potential to be extremely quick – even instantaneous. In such cases, consideration must be given to how results will be presented. One criticism of the Ireland pilot of electronic voting was that the tabulation and announcement of results happened too suddenly, before the losing candidates could prepare for defeat. Traditionally in Ireland the tabulation process takes one or even several days,[39] and is conducted in front of party representatives, who are able to make an early calculation of the results. There have been similar objections to rapid reporting of results in the United States, where multiple time zones create the possibility that the outcome of a presidential election may be known even before the polls close on the West Coast.

FIGURE 22 – OBSERVATION IN LONDON CRITIQUES ELECTRONIC COUNTING

In the 2008 London mayoral and assembly elections, electronic ballot scanners were used in three centralized counting centers. However, after observing the process, the British NGO Open Rights Group cited a lack of transparency in several areas that did not allow for observers to confirm that the results were an accurate reflection of voters' intentions. In its report, Open Rights Group made a number of recommendations for the use of electronic counting systems in future elections.

In 2008, the British digital rights NGO Open Rights Group deployed 27 observers to follow voting and counting during the London mayoral and London Assembly elections. The group focused in particular

39 The length of vote counting in Ireland is due to the country's use of the STV (single transferable vote) proportional representation electoral system.

on assessing the counting process, as the vote count was conducted using electronic ballot scanners at three centralized counting centers. The final report released by Open Rights Group concluded that "there is insufficient evidence available to allow independent observers to state reliably whether the results are an accurate reflection of voters' intentions."

In particular the group criticized inadequate transparency of the process, including the inability of observers to witness the recording of valid votes and the lack of a random manual audit on a sample of ballot scanning machines to assess the overall accuracy of the counting process. The group also criticized the lack of observer access to the control desk of the equipment supplier, despite the fact that its computers were connected to the counting server.

In its report, Open Rights Group offered five key recommendations to authorities for improving the system in the future. The group also provided recommendations for the future consideration of using e-counting technologies more broadly, which included conducting a thorough cost-benefit analysis of the use of e-counting machines; allowing sufficient time for formal consultations with key stakeholders before deciding whether to use e-counting technologies in the future; and building in sufficient time for procurement and implementation of any new technologies.[40]

40 The full report can be found here: www.openrightsgroup.org/wp-content/uploads/orglondonelectionsreport.pdf.

KEY CONSIDERATIONS: TABULATION

FOR IMPLEMENTING BODIES

- ☑ Is results transmission simultaneously conducted through more than one channel?
- ☑ Is the path of results transmission clearly defined?
- ☑ Is the tabulation process designed to be transparent for party representatives and observers, and is the tabulation publicly available in a verifiable format?

FOR OVERSIGHT ACTORS

- ☑ Are sufficient security measures in place to prevent interference with the electronic transmission process?
- ☑ Are polling station level results published on the Internet in an easily-verifiable format?
- ☑ Is the tabulation process at all levels fully transparent for party representatives and observers? For example, can observers witness the data being uploaded or entered into the tabulation computers?
- ☑ How has the announcement of results changed with the implementation of new technologies (i.e., are results announced more quickly?), and how does this affect the post-election political dynamic and overall public confidence?

CHALLENGES AND RECOUNTS

Electoral authorities generally follow the same procedures for challenges and recounts for an election with electronic voting or counting as they do for paper-based elections. However, in the case of electronic voting, some form of audit trail must exist so that the results can be verified and electoral authorities should consider this requirement during the planning stages for electronic voting systems. In the case of electronic counting systems, clear guidelines and rules should be established regarding the counting of ballots that are not read by scanners.

A key part of ensuring the integrity of the results is the ability of political competitors to lodge challenges to the results and receive effective redress. This is first of all a question of the legal framework. It must clearly define who can lodge a challenge against the results, which body the challenge should be lodged with, what circumstances an investigation will be conducted in and what situation a recount of the results will occur in. As the counting and tabulation processes are likely to be much faster using electronic voting and counting equipment, the deadlines for responding to challenges will need to reflect this.

Generally complaints and appeals procedures should remain the same as in traditional elections. However, the additional question of whether the equipment functioned properly may account for a greater number of challenges, and mechanisms must be in place to demonstrate that the count reflects the votes as cast through the conduct of recounts.

In order to determine whether votes have been accurately counted by a voting or counting machine, some kind of voter-verified audit trail – either paper or electronic – must exist that can serve as the basis for a recount. Without this audit trail, it is not possible to conduct a recount. While some

voting machines do not produce a voter-verified audit trail, having such a trail is increasingly viewed as an emerging standard in the field. Simply recalculating the votes using the same machine is not sufficient to independently verify the accuracy of the results. In the case of electronic counting machines, the ballots that have been counted serve as the audit trail and can be manually recounted.

When electronic counting machines are used, blank ballots or ballots that cannot be read by scanners (e.g., damaged ballots or ballots with unclear or stray marks) must be set aside for adjudication, typically in the presence of candidate representatives and observers. In such cases officials must manually determine whether a vote is valid and, if so, for which candidate or party it has been marked. If candidate representatives disagree with the determination, the disputed ballots may be reviewed with a more senior-level election official who will determine if and how to count the ballot.

Manual recounts may be also called in the case of a very narrow margin of victory. Some election laws may require a manual recount should the results fall within a prescribed margin of victory. Clear and unambiguous legal guidelines must be in place for what steps should be taken if the results do not match or are not within a certain margin of error, especially whether the paper or electronic results should take precedence. Observers should closely follow the process of challenges and recounts, and audit reports should be publicly available.

FIGURE 23 – CHALLENGES AND RECOUNTS: POLITICAL PARTIES AND THE COMPLAINTS PROCESS IN THE PHILIPPINES

The electoral complaints and protests filed by political parties after the 2010 Philippines elections point to several issues that are important for political contestants in countries with electronic voting and counting systems: the need for specialized technical expertise, effective training of party observers to collect appropriate documentary evidence, and IT capacity in courts making decisions on electoral complaints.

In 2010, political parties in the Philippines observed the country's first nationwide use of electronic technology for elections. The introduction of e-counting technology was expected to reduce fraud and errors during counting and tabulation (canvassing). Thus, it was hoped that the number of electoral complaints and protests filed by parties and candidates would decrease. However, due to several factors, electoral protests increased in 2010. The House of Representatives Electoral Tribunal received a record number of cases (65) in 2010. The COMELEC also received more cases filed by losing candidates in 2010 (98) than in the 2007 elections (73).[41]

41 Libertas. Issues and Challenges to Dispute Resolution under the PSCOS AES.

Some of the protests were related to the electronic technology used in the elections, including complaints about: erroneous counting of votes or misreading of ballots by the optical-scan machines; errors in the initialization of optical-scan machines; errors in transmission and consolidation of results; erroneous rejection of ballots; nonimplementation of security measures; and manipulation of optical-scan machines and/or compact flash cards. Ultimately, many cases were dismissed due to insufficient evidence or on procedural grounds.

Reflecting upon their experiences with monitoring and filing complaints, the major political parties cited a number of lessons learned. A lack of IT training and tools for observing the new technologies made it difficult for party agents to collect the necessary evidence to support their candidates' claims. Parties also pointed to the importance of making sure the courts have the IT capacity to effectively rule on technology-related cases. They also noted that the cost of filing complaints has increased, since parties have to hire more specialized legal and IT expertise, significantly adapt party pollwatcher trainings and tools, and educate themselves in more detail about the new technologies.

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?
- ☑ Do deadlines for responding to challenges reflect the fact that counting and tabulation processes are likely to be much faster using electronic voting and counting equipment?
- ☑ Does a voter verified audit trail exist as the basis for a recount?
- ☑ Is there a process in place for adjudicating blank ballots or ballots that cannot be read by scanners?
- ☑ Are clear legal guidelines in place for what steps should be taken if the original and recounted results do not match or are not within a certain margin of error?

FOR OVERSIGHT ACTORS

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

- ☑ Is there a voter verified paper audit trail in place that can serve as the basis for a recount?
- ☑ If relevant, is there a clear process for adjudicating ballots that cannot be read by scanners, and are stakeholders allowed and encouraged to oversee this process?
- ☑ Do the legal guidelines clearly establish what must take place in instances where recounted and original results do not match sufficiently?
- ☑ Are audit reports made publicly available?
- ☑ Does the court or adjudicating body have sufficient IT capacity to effectively rule on election technology-related cases?

POST-ELECTION AUDITS

Trust in electronic voting and counting systems can be strengthened through mandatory auditing of these systems as soon as possible after an election to verify that the system was able to accurately capture results from the election. The legal framework for elections should specify the process through which a post-election audit should be implemented as well as the consequences of any difference found between electronic and paper records. The audit should take place as soon as possible after an election and should be open for observation by oversight groups.

Comprehensive testing and source code reviews, as well as possible certification mechanisms, will do much to ensure that electronic voting and counting systems deliver accurate results. However, to ensure trust in these systems, it is crucial that they be auditable and audited after use so that the results can be verified as accurate, ideally by an independent organization.

The way in which this auditability is provided varies depending on the type of electronic voting or counting system in question (e.g., it is different for electronic voting systems, electronic counting systems and especially for remote electronic voting systems). The most common way in which auditability is achieved for electronic voting machines[42] is through the use of a voter-verified paper audit trail, which can be manually counted as a check against the electronic result generated by the electronic voting machine.

Regardless, an audit mechanism is a way both of checking that the technologies worked properly and of verifying the results, by comparing the electronic and auditable versions of the results. In addition to checking the operation of the

42 Auditability is mainly a challenge for electronic voting systems, as electronic counting systems normally use a paper ballot completed by the voter, which naturally provides a paper audit mechanism.

system, this also helps build confidence in the system, more so if the audit is done under the full observation of stakeholders in the process.

In order to build and maintain confidence, conducting audits of the results generated by electronic voting or counting systems should be mandatory.[43] The (paper) audit trail should be manually counted and the results compared to the electronic results generated. Because it is unlikely that such an audit will be possible in every location, audits should be conducted in a randomly selected sample of locations that are only informed of the impending audit after the close of polling or counting. In contentious elections it may be appropriate to allow candidates to select a predetermined number of polling stations for manual audit in addition to the randomly selected samples. This allows the candidate to focus on areas where fraud may be suspected.

The legal framework should make clear how this audit process takes places, the number of locations, the ways in which the locations are selected and informed, when the audit takes place, the people who may be present during the audit, how the results of the audit are reported, and the consequences of any difference between electronic and paper records.

The audit process should be conducted as soon as possible after the election. An audit right after the close of voting and counting avoids the possibility or perception of tampering or manipulation before the audit takes place. If an immediate audit is not possible, then the sample to be audited should be sealed in a tamper evident way until the audit can take place. The audit should be fully observable by election observers as well as the media and political party and candidate agents.

43 This is supported by the Council of Europe (2010) in its E-voting Handbook in which it recommends that a paper audit trail should be combined with a mandatory count of paper votes in a small but statistically meaningful number of randomly selected polling stations, p. 12.

The results of the audit process will need to be interpreted differently depending on the kind of technology being used. With electronic voting technologies there should be no differences at all between the result generated from the audit trail and the electronically generated result. If a difference is found, then it will be prudent to conduct a recount of the audit trail to make sure that the manual process has not generated a mistake. Should a difference between the manual count of the audit trail and electronic count of votes still persist, even if only by one vote, this will be seen as an indication of some flaw in the operation of the electronic voting machine or the audit trail. Even a small deviation would be a critical concern. Without an understanding of why a difference is possible, it also cannot be known if this flaw could lead to much larger deviations between the electronic result and audit trail in other locations that are not being audited or in future elections.

With electronic counting technologies, the interpretation of differences between the manual recount of the audit trail and electronically generated results is more difficult. Different voters mark paper ballots in different ways, and sometimes these voter marks are interpreted differently by electoral officials. The advantage of electronic voting technologies is that they interpret ballot marking in a consistent manner, according to the instructions provided to them. A difference in vote totals through a manual count of the ballots may be due to the counting machine reading voter marks in a different way than the election official. It may be the election official has made a mistake, or it could be a simple difference in the ability of individuals to discern small differences in shading that may clearly indicate the intent of a voter, but which the machine is incapable of detecting. In extreme cases, it could be that the difference represents an error in the ballot-counting rules provided to the counting machine. This requires an amendment to the counting machine software. Depending on the severity of any error in the ballot-counting rules provided to the counting machine, this may have implications, even serious implications, for the results generated by counting machines across the election.

FIGURE 24 – E-VOTING AUDITS IN VENEZUELA

Electronic voting is a heavily audited process in Venezuela. Upon casting a vote electronically, a voter can verify that his or her vote was cast as intended through a paper receipt, which the voter then places into the ballot box. After the close of polling in randomly selected polling stations, officials conduct an audit to ensure that the count from the paper ballots matches the electronic records.

Venezuela is one of only four countries that uses electronic voting machines for its entire electorate (India, Brazil and Bhutan are the others). The voting machines used in Venezuela are touch-screen direct-recording electronic voting machines (DREs) that produce a paper receipt for the ballot once the ballot choices have been made. In the 2012 presidential election, voters were also authenticated using a biometric authentication device. After casting their ballots, voters are able to check that the paper receipt matched the selections they had made on the electronic voting machine. The voter then placed this paper receipt into a ballot box in the polling station.

While the voting machine itself tallies the votes and produces the results for the polling station, the paper record in the ballot box enables verification that this electronic record is accurate. This verification method is used extensively in Venezuela, with over 50 percent of randomly selected polling stations counting the paper records to ensure that they match the electronic results. This "hot audit" is conducted immediately after the close of polling and in the presence of observers and party representatives. No significant anomalies between the paper and electronic records have ever been found.

Prior to this, a number of other audits and oversight mechanisms are implemented. The source code for the electronic voting machines is audited before each election. Technical teams assembled by government institutions, independent institutions and political parties review the source code line by line in a "clean room," where code can be viewed in its entirety but not modified or taken away. As part of this audit process, the source code is compiled and hash functions of the final versions are registered. These hash functions can then be used to verify that the audited version of the software is being used on Election Day.

KEY CONSIDERATIONS: POST-ELECTION AUDITS

FOR IMPLEMENTING BODIES

- ☑ Does the legal framework make clear how the audit process takes place, the number of locations, the ways in which the locations are selected and informed, when the audit takes place, the people who may be present during the audit, how the results of the audit are reported, and the consequences of any difference between electronic and paper records?
- ☑ Is a randomly selected sample of locations chosen for audits, and only informed after the close of polling or counting?
- ☑ Will audits take place as soon as possible after the election?

FOR OVERSIGHT ACTORS

- ☑ Is there a way to compare the electronic and auditable versions of the results to confirm whether the technologies worked properly and to verify the results, such as through the use of a voter verified paper audit trail?
- ☑ Is a random manual audit conducted, during which the audit trail is manually counted and the results compared to the electronic results generated in a random selection of polling stations? Is it conducted as soon as possible after the election, and is it fully observable by election observers, the media and political party and candidate agents? Are the results made publicly available?

☑ If a difference is found during the audit, is there a robust process to determine the cause of the difference and to address the cause(s) to the extent possible?

EVALUATION OF SYSTEM

Comprehensive evaluations of electronic voting and counting systems after an election can be critical for the long-term viability of these systems. The evaluation should take place not too long after an election and should involve a variety of data sources and electoral stakeholders so that a well-rounded assessment of the electronic voting and counting systems can be conducted. The EMB should have a mechanism for tracking and implementing evaluation recommendations in advance of the next electoral cycle.

A comprehensive evaluation of an electronic voting or counting system is critical to its success, particularly in the longer term. Only through an honest evaluation can the positive and negative lessons learned from the use of electronic voting or counting be captured to improve the process in the future.

An evaluation may be carried out by the project management committee or by another oversight body, or it may be contracted out to independent consultants. The evaluation should focus on the original objectives of the project and the extent to which those objectives have been achieved with the adoption of the electronic voting or counting system. Issues such as efficiency, usability, accessibility, accuracy, security and cost, among others, should be considered.

An evaluation may include several components, carried out by different bodies. Post-election surveys and focus groups can be a useful way to collect valuable information about voters' experiences using the technology, if the jurisdiction

has the resources to commission such an exercise. Partnering with a university may be a useful way to conduct such activities. The number of complaints received about the electronic voting or counting system and the nature of these complaints should also be evaluated.

Evaluators should seek to involve a broad range of stakeholders in the assessment of electronic voting and counting systems. Interviews should be conducted with voters as well as with election officials at various levels, candidate and party representatives, election observers and journalists to learn about their experiences with the electronic voting and counting and whether they have recommendations to offer for the future implementation of the system.

Evaluation reports should be made available to the public and can serve as the basis for post-election roundtable discussions about the project among stakeholders, with an eye to offering recommendations for future improvement. Facilitating broad post-election dialogue about the electronic voting and counting systems can help to promote transparency and public confidence in the process as a whole, and offer valuable lessons as well.

Once the evaluation process is complete, it is important that the findings are used to improve the process in the future. A mechanism should be designed to ensure that recommendations and lessons learned are considered and implemented promptly, in time for the next election cycle.

FIGURE 25 – EVALUATION OF E-VOTING IN NORWAY

Following the 2011 trials of Internet voting in 10 of Norway's 429 municipalities, authorities contracted two research centers and IFES to carry out a thorough evaluation of the system. The evaluation used both qualitative and quantitative research methods, including questionnaire surveys in the trial municipalities, in-depth interviews with selected groups, focus groups for young people and observation studies of user-friendliness for voters with disabilities.

The evaluation sought to assess the project in the following seven areas:

- Availability and accessibility
- Trust and credibility
- Secrecy of voting (e.g., family voting, undue influence)
- Efficient counting of votes/fast electoral results
- Participation and turnout
- International experience with e-voting
- Compliance with international standards

The evaluation reports are available on the website of the Ministry of Local Government and Regional Development at: www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201.html?id=684642

FIGURE 26 – RE-EVALUATION OF THE USE OF ELECTRONIC VOTING IN THE NETHERLANDS

The Netherlands in 2006 decided to re-evaluate the use of electronic voting technologies after the system in use came under criticism for security and other reasons. To facilitate this process, the nation's parliament created commissions to investigate how past decisions on the approval of voting machines had been made and to review the organization of the election process. The findings of both commissions strongly criticized the government's management of voter technologies, and subsequently the government abandoned electronic voting, returning to paper-based voting.

Following decades of using electronic technologies in elections in the Netherlands, such technologies came under heavy criticism in 2006. In response to the publicizing of concerns about the lack of security and auditability mechanisms in the country's electronic voting machines by a group of computer experts called "We Do Not Trust Voting Computers" (described in more detail in Figure 14 above), the parliament requested that the government establish two independent commissions to consider the past and future of electronic voting.

The Voting Machines Decision-making Commission was tasked with reviewing how decisions on the approval of voting machines had been made in the past and what lessons could be learned. In its April 2007 report "Voting Machines: An Orphaned File," the commission was critical of the government's past role in electronic voting, concluding that (1) voting machines did not receive enough attention; (2) the Ministry of Interior lacked technical knowledge, resulting in officials becoming overly dependent on external actors, including technology vendors; and (3) the government did not react to signs that should have raised concern. The report also concluded that certification and testing of the voting machines was based on outdated standards and that reports from these tests should have been made public. The report noted that the legal framework did not adequately address the specifics of electronic voting, particularly the security requirements.

A second commission, the Election Process Advisory Commission, was set up to evaluate the organization of the election process and to make recommendations for future elections. In its September 2007 report "Voting with Confidence," the commission noted that requirements for election-related equipment had not been adequately established and that the security and management of the equipment were not properly regulated. It also noted that the electronic voting machines in use were not sufficiently transparent and verifiable. The commission concluded that all municipalities should have the same method of voting and that voting by paper ballot would be the most appropriate method.

The government acted quickly in the wake of the release of the commissions' reports. Within a year of release of the Election Process Advisory Commission's report, the government had decided that voting and counting in the Netherlands would fully return to paper-based, manual processes.

KEY CONSIDERATIONS: EVALUATION OF SYSTEM

FOR IMPLEMENTING BODIES

- ☑ Is a comprehensive post-election system of evaluation in place, and are the responsibilities for this evaluation clearly defined (for example, between project management committee, another oversight body, or independent consultants)?
- ☑ Are resources available to commission post-election surveys and focus groups to collect information about voters' experiences using the technology?
- ☑ Does the evaluation focus on the original objectives of the project, and to what extent they have been achieved with the adoption of the electronic voting or counting system?
- ☑ Are issues such as efficiency, usability, accessibility, accuracy, security, and cost among others considered in the evaluation?
- ☑ Are the number of complaints received about the electronic voting or counting system and the nature of these complaints also evaluated?

- ☑ Will interviews be conducted with voters, election officials at various levels, candidate and party representatives, election observers and journalists?
- ☑ Will post election evaluation reports serve as the basis for post-election roundtable discussions among stakeholders about the project?
- ☑ How will the findings from the evaluation be used to improve the process in the future, in time for the next election cycle?

FOR OVERSIGHT ACTORS

- ☑ Does the evaluation of the electronic technologies involve a broad range of stakeholders, including election officials, party representatives, observers, and voters?
- ☑ Are evaluation reports made available to the public?
- ☑ Have election officials facilitated any post-election dialogues or other mechanisms to provide stakeholders an opportunity to offer recommendations for future improvements?
- ☑ Is there an EMB mechanism in place for tracking the implementation of stakeholder and evaluator recommendations ahead of the next election cycle?
- ☑ Have oversight actors evaluated their own efforts to monitor the new technologies and have they shared their findings with the EMB and the public?
- ☑ Are oversight actors preparing to assess and adapt their own methodologies in relation to future electronic voting and counting implementation plans?

INTERNET VOTING

While Internet voting has been utilized for national-level elections in only a few countries, it is a voting mechanism that is increasingly being explored as a means to allow access to the election process for voters who may otherwise find it difficult to go to their polling location on Election Day. Internet voting, however, presents a number of technological challenges focused on security, privacy, and secrecy issues, as well as challenges for stakeholder involvement in and observation of the process. All of these must be comprehensively addressed for election authorities to consider moving forward with Internet voting.

The first use of Internet voting for a binding political election took place in the US in 2000, with more countries subsequently beginning to conduct trials of and/or use Internet voting. A total of 14 countries have now used remote Internet voting for binding political elections or referenda. Within the group of Internet voting system users, four core countries have been using Internet voting over the course of several elections/referenda: Canada, Estonia, France and Switzerland. Estonia is the only country to offer Internet voting to the entire electorate. The remaining ten countries have either just adopted it, are currently piloting Internet voting, have piloted it and not pursued its further use, or have discontinued its use.

Examples of Internet voting in other countries around the world vary widely in scope and functionality. The early cases of Internet voting were less technically advanced than those being developed more recently. Many of the changes seen in Internet voting systems have been aimed at improving the quality of elections delivered by these systems and meeting emerging standards for electronic voting.

It is fair to say that Internet voting is not a commonly used means of voting. Of the 14 countries that have so far used it in any form, only ten currently have expressed any intention of using it in the future. However, Internet voting is a relatively new voting technology and has been developing significantly over the previous ten years. Internet voting seems to fit, for many countries, a niche corner of the electoral process. It is largely targeted at those who cannot attend their polling station in person on Election Day. In fact many more countries have expressed or shown an interest in the use of Internet voting, especially when they have large numbers of expatriate voters. However, the implementation of Internet voting, according to emerging standards, is a very technical exercise. It can also pose some difficult political questions if the aim is to facilitate the inclusion of large numbers of expatriate citizens in the political process.

The technicalities of implementing Internet voting systems are largely a result of attempts to reconcile the use of Internet voting with emerging and existing standards to which elections and electronic elections should adhere. These standards include the need for secure online voter authentication, protection of the secrecy of the vote, appropriate transparency mechanisms, testing and certification regimes. The need for secure online voter authentication mechanisms may be one of the biggest hurdles in implementing Internet voting. It presents a challenge for many established democracies, which often do not have ID card systems with secure online authentication mechanisms.

FIGURE 27 – INTERNET VOTING IN ESTONIA

Estonia has implemented Internet voting in national elections since 2005 and the percentage of voters voting via Internet has trended up in each successive election. Estonia has taken several measures to ensure the secrecy of the vote, primarily through allowing multiple votes to be cast over the Internet by a voter (only the last one is counted) and also prioritizing any paper ballot cast by a voter over Internet votes cast.

Estonia became the first country to offer Internet voting to the entire electorate for nationwide, binding elections. Internet voting has now been provided in local (2005, 2009), parliamentary (2007, 2011), presidential (2011) and European (2009) elections. The first three elections were carried out without major criticisms and with a growing percentage of Internet voters. The 2011 parliamentary elections saw a significant increase in the usage of Internet voting (over 24 percent of all votes were cast using the Internet).

Internet voting is only available before Election Day during an early voting period that normally lasts for one week. Voters may cast their Internet ballots multiple times during this period, and only the last Internet ballot cast is considered valid for the official tally. Various paper ballot options are also available. Voters can cast early paper ballots. Estonians living

abroad may cast their ballots by post or vote at an embassy. Voting from ships is also offered.

The names of those voting by Internet are removed from the electoral register used on Election day in the polling station. Any paper ballot cast in the early voting period will be counted, canceling any Internet ballot cast by the voter. The strategy of allowing multiple votes and the primacy of the paper ballot is intended to protect the secrecy of the vote by allowing any voter who may have been coerced or intimidated to vote a certain way the opportunity to vote again in secrecy and overwrite their previous, tainted vote.

Internet voters identify themselves with a smart national ID card or a "mobile ID" (a new authentication channel using mobile phones with specific SIM cards that was introduced in 2011). Once authenticated, the voter casts the ballot through a platform that sends the vote to a central database. The vote is digitally signed (inner "envelope") and inserted in another virtual and signed "envelope" (outer one) that contains the identification of the voter and the session log.

In reviewing the use of Internet voting since 2000, a number of important themes emerge:

Trust in Internet Voting – As already discussed, trust in the electoral process is essential for successful democracy. However, trust is a complex concept, which requires that individuals make rational decisions based on the facts to accept the integrity of Internet voting. The problem is that Internet voting is

so complex that few voters have the technical expertise necessary to make the informed decision to place their trust in it. In order to compensate for the inherent complexity of Internet voting, extra measures need to be taken to ensure that voters have a sound basis on which to give their trust to Internet voting systems. Technical institutions and experts can play an important role in this process, with voters trusting the procedural role played by independent institutions and experts in ensuring the overall integrity of the system, rather than their own limited understanding of how Internet voting works and the verification mechanisms used.

A number of mechanisms can be used to enable the development and maintenance of trust in Internet voting systems. One of the fundamental ways to enable trust is to ensure that information about the Internet voting system is made publicly available. The system must also be trustworthy, and measures to ensure the integrity of the system are important. A vital aspect of integrity is ensured through testing, certification and audit mechanisms. These mechanisms will need to demonstrate that the security concerns presented by Internet voting have been adequately dealt with, and will need to recognize that there are some aspects of security that are outside of the control of the Internet voting system – such as the devices (i.e., the computers) that voters use to cast their ballots.

Due to the inherent lack of transparency with Internet voting, it is important to separate the responsibilities for different stages of the Internet voting process. Such a separation of duties will make it more difficult to manipulate the system. Allowing the repeated casting of Internet votes, with only the last vote being counted, also helps generate trust amongst voters. Making the Internet voting system verifiable, so that the results can be independently verified against the votes cast, is an increasingly important trust mechanism, although this needs to be done in a way that does not violate the secrecy of the ballot. Finally, Internet voting systems should be subjected to various evaluation mechanisms.

The Secrecy and Freedom of the Vote – Ensuring the secrecy of the ballot is a significant concern in every voting situation. In the case of Internet voting from unsupervised environments, this principle may easily become the main challenge. Given that an Internet voting system cannot ensure that voters are casting their ballots alone, the validity of Internet voting must be demonstrated on other grounds. One relevant argument is the similarity of Internet voting with postal voting, a method of voting considered to meet standards of secrecy by the Venice Commission. The chance to repeat and cancel an Internet vote is a common argument for the acceptance of Internet voting, as it means that a vote buyer or coercer will not know for sure which ballot will be counted for a voter. Finally, Estonia has argued that the principle of secrecy entails an obligation to provide the opportunity for a secret vote, but that voters are free to choose less secret voting options if they desire.

Accessibility of Internet Voting – Improving accessibility to the voting process is often cited as a reason for introducing Internet voting. The accessibility of voting systems, closely linked to usability, is an international standard for elections, and is relevant not only for voters with disabilities and linguistic minorities, but also for the average voter. Internet voting can have a significant impact on the accessibility of the voting process. It is important that voters, especially those who may have special accessibility issues, are involved in the development of any Internet voting system. The way in which voters are identified and authenticated can have a significant impact on the usability of the system, but a balance needs to be found between accessibility and integrity.

The voting process itself, and vote-verification mechanisms, can also be difficult to design in ways that are accessible to all. Voters will often demand that Internet voting be made available through the end of normal voting, but the duration of voting will need to be determined while considering other factors, such as any requirements for Internet voters to be able to cast a paper ballot. The proliferation of computer operating systems and web browsers presents

Internet voting system developers with increasing challenges in making their systems functional on all or most of these operating systems and browsers.

A counterargument can be made related to the "digital divide" in terms of the accessibility of Internet voting. Different groups in society have different levels of access to the Internet. Therefore, the provision of Internet voting in societies where there is very unequal access to the Internet will have a different impact on accessibility for various communities. Of course, these communities may have very different voting preferences, which could have implications for the results of the election.

Even in well-developed democracies, more affluent voters may be able to vote from the comfort of their own homes, while others may have to take time off work to wait in line to vote. The possible unequal impact on accessibility created by the provision of Internet voting would be far more severe if Internet voting were the only means of casting a ballot. However, as can be seen even where traditional voting mechanisms are also in place, Internet voting can create accessibility concerns, although the accessibility of these other voting mechanisms could be improved in order to compensate.

Electoral Stakeholders and Their Roles – The introduction of Internet voting significantly changes the role that stakeholders play in the electoral process. Not only do new stakeholders, such as voting technology suppliers, assume prominence in the Internet voting process, but existing stakeholders must adapt their roles in order to fulfill their existing functions. While electronic voting in general requires changes in the roles of these stakeholders, the introduction of Internet voting, in particular, changes the roles in a much more fundamental manner as the act of voting is taken outside of the polling station.

This new network of stakeholder roles and relationships may be difficult to manage well, and some of the various stakeholder demands may be contra-

dictory (for example, they may take different positions on the disclosure of information on the Internet voting system). Central to this new network of stakeholder relationships is public administration, especially the role of the EMB. Public administration and the EMB will establish the legal and regulatory framework for the implementation of Internet voting; and this framework will define the roles and rights of the various stakeholders in the Internet voting process. The EMB will also need to manage the implementation of the Internet voting technology, ensure control is maintained over the supplier and facilitate the open involvement of all relevant stakeholders during implementation. An open information policy will be essential to the EMB's interactions with stakeholders to develop trusted relations while implementing Internet voting.

Internet voting presents obvious challenges for party poll watchers and observers. While the role of observers in the pre-election period will be similar to their role with other forms of electronic voting as discussed above (e.g., legal framework, design requirements, testing and certification, security, etc.), observers will be unable to make a systematic assessment of the voting and counting process. Observer groups and political parties must therefore design observation strategies with this in mind and must be candid with the public about any limitations of their assessments. At the same time, Internet voting introduces several new elements and points of inquiry for election observers. These include evaluating the security of voting servers, assessing the EMB's monitoring of voting server security and threat response plans, and the functioning of Internet Service Providers (ISPs).[44] As with other forms of electronic voting, IT expertise will be critical to such efforts. Observers may also use survey techniques to gauge voters' experience with Internet voting, including their level of trust in the system.

44 Pran, V. and Merloe, P. (2007) NDI Handbook: Monitoring Electronic Technologies in Electoral Processes, pp. 85–88.

EMBs need to be sensitive and responsive to opposition and concern about the introduction and use of Internet voting systems. There will likely always be some opposition to such systems; however, to ignore opposition and concern is very risky. Even small groups opposing voting technology can have a significant impact by raising concerns that resonate with the public. EMBs that fail to respond to concerns about Internet voting may lose control of any public debate in a way that could be fatal for implementation. Proactive engagement with opponents of Internet voting by the EMB and attempts to mitigate these concerns will serve to diffuse potentially damaging public debates on Internet voting. It will also help ensure that Internet voting does not become a, or the, divisive issue in a country's political discourse.

KEY CONSIDERATIONS: INTERNET VOTING

FOR IMPLEMENTING BODIES

- ☑ What measures have been taken to build trust among stakeholders and especially voters in the development of the internet voting system?
- ☑ What technical solutions have been put in place to respect the secrecy of the vote?
- ☑ As an important goal of electronic voting technology, what efforts were made to ensure and enhance accessibility across all voter groups?
- ☑ How have traditional and new stakeholders been included throughout the design and implementation process of internet voting?
- ☑ Is there proactive engagement with those opposed to internet voting in order to address their concerns?

FOR OVERSIGHT ACTORS

- ☑ What limitations do observers and parties face in assessing the integrity of internet voting? Are there alternative strategies they can adopt to monitor the process?
- ☑ What measures have been taken to ensure voters have a solid basis to trust internet voting systems? What level of trust do voters have in the system as a result?
- ☑ Do all stakeholders support the adoption of internet voting, and if not, how have concerns been addressed by the authorities?
- ☑ How does internet voting affect accessibility for different communities, who may have highly unequal internet access? If inequities are created, are there alternative (i.e., traditional) means by which voters disadvantaged by internet voting can cast their ballots? Has the accessibility of traditional voting methods been improved to compensate for the improved accessibility for internet voters?
- ☑ To address the reduced transparency associated with internet voting, are responsibilities separated among those administering elections for different stages of the internet voting process?
- ☑ To what extent is the secrecy of the vote protected? For example, do voters have the opportunity to repeat and cancel their votes? Is the online voter authentication secure? Are the voting servers secure? How has this security been demonstrated to the public?