Information Technology and Elections Management Thematic Workshop, Nairobi, March 5-9, 2012

Electronic Voting: Theories and Typologies, Peter Wolf International IDEA

When I mention that I am working on electronic voting people sometimes ask "So why do countries actually want to use this technology?" And I think this question is a good starting point for discussing theories and typologies of electronic voting.

After all the introduction of e-voting is usually a complex and costly exercise and in many cases triggers a debate about the desirability of this technology as a whole.

In the context of the Arab Spring last year I heard some activists argue "Technology in the form of Social Media brought our democratic revolution, so technology in the form of electronic voting should fix our broken electoral process."

This is a good example of expectations towards e-voting that are often quite high and sometimes not very realistic. While e-voting certainly has its advantages it can of course not be expected to be the sole solution to an otherwise broken electoral process, a disenchantment of voters with democracy or a lack of trust in a country's election administration.

What are common expectations that e-voting can actually deliver on?

Two important benefits are directly related to the elimination of human intervention in the counting and in some cases also the tabulation phase.

1. Faster results: Automation of counting and tabulation leads to a speeding up of this process and faster availability of results. This is particularly useful if manual counting procedures are inefficient due to multiple contests and complicated electoral formulae
2. Elimination of some avenues of fraud: less human intervention also leads to less opportunities of fraud by manipulation during count and tabulation

Some e-voting systems can warn voters that are about to cast invalid votes. By giving them a chance to correct this they can

3. Reduce the number of spoilt and invalid votes

Especially e-voting in the form of Internet voting that allows voters to cast their ballot from anywhere without the time and locational constraints of voting polling stations can lead to another advantage

4. Providing better services to citizens, more convenience for voters that can potentially lead to increased participation and turnout, or simply fulfilling an expectation of the citizenry used to more and more governmental services being provided online

Internet voting is also one example of e-voting systems that can

5. Making elections more accessible for some citizens:

* home bound or institutionalized voters can be reached more easily

* some voting machines have audio interfaces for blind voters

* there may even be options for providing ballots in more languages that what is logistically feasible in paper based elections.

Of course benefits, but also disadvantages of e-voting systems depend greatly on the type of solution that is chosen.

A first important distinction is whether electronic voting is conducted in controlled or in uncontrolled environments. E-voting in controlled environments happens when the casting of votes takes place in polling stations, polling kiosks or other locations under the supervision of staff appointed by the electoral management body (EMB). By that means the election administration can to a great extent control the voting technology as well as the procedures and conditions under which voters are casting their ballots. E-voting in controlled environments can be seen as the electronic equivalent of traditional paper-based voting in polling stations or embassies. E-voting in uncontrolled environments happens without any supervision and from voting devices that cannot be controlled by the election administration. This can be from home, on

the voter's personal computer, or potentially anywhere on mobile or public devices. With voting in uncontrolled environments, concerns about the secrecy of the vote, family voting, intimidation, vote-buying, the loss of the election day ritual, the impact of the digital divide and the technical separation of voter identity and ballot paper, as well as the technical integrity of the device from which the votes are cast, all need specific consideration.

E-voting in uncontrolled environments can be seen as the electronic equivalent of postal voting or absentee voting.

Currently most systems fall into one of these four categories:

1. Direct recording electronic (DRE) voting machines. Here the voter makes the selection directly on the voting machine, usually on a touch screen, in some models also by pressing physical bottons. DREs can come with or without a paper trail (VVPAT, or voter-verified paper audit trail). VVPATs are intended to provide physical evidence of the votes cast and I will briefly explain them a little later.
2. Optical Mark Reading (OMR) systems are technically based on scanners that can recognize the voters' choice on special machine-readable ballot papers. OMR systems can be either central count systems (where ballot papers are scanned and counted in special counting centres) or precinct count optical scanning (PCOS) systems. With PCOS system scanning and counting happens in the polling station, directly as voters feed their ballot paper into the voting machine.
3. Internet voting systems allow citizens to cast their vote from computers online. In some cases such votes are cast from public voting kiosks, but more commonly from the voter's private computer. Votes are transferred via the Internet to a central counting server.
4. A final category of systems are Electronic ballot printers (EBPs), devices similar to a DRE machine that produce a machine-readable paper or electronic token containing the voter's choice. This token is fed into a separate ballot scanner which does the automatic vote count.

Even though there are more systems such as Digital Pens that read the vote as the voter writes it on the ballot paper most currently used systems fall under the four typologies mentioned.

Beyond these typologies there are also a few other important options to consider:

E-voting with or without independent physical evidence of the votes cast

Many of today's e-voting systems in controlled environments produce physical evidence of the vote cast in the form of paper receipts for the voters (often referred to as VVPAT). Voters can verify their vote on the receipt and then deposit the receipt in a ballot box. By manually re-counting the receipts, the results presented by the voting system can be independently verified. The results of an entire election can be verified by a well-designed manual recount of receipts from a random sample of polling stations. E-voting systems in uncontrolled environments commonly do not produce physical evidence as these could be used for vote-selling. Additionally, as the voter would keep the receipt, a manual recount is not possible, which renders such receipts useless. However, some Internet voting systems utilize a return code system that allows voters to verify that their vote was received unaltered by the counting server. If e-voting systems provide no physical evidence of the votes cast, direct verification of results is not possible. The results produced by such a system can only be indirectly verified. Indirect verification relies exclusively on a strict certification process against agreed standards in combination with tight security measures that prevent any violation of the voting system's integrity. In these circumstances it can be difficult to communicate the reliability and trustworthiness of the e-voting system in a transparent way to a critical or non-expert audience. This might become an insurmountable challenge in a context where the EMB does not enjoy the full trust of the electoral stakeholders.

Adding a paper trail makes e-voting systems more complex and expensive. Bearing in mind the fact that many voters do not check their receipts, as well as possible mistakes in the manual recount and the need to resolve discrepancies between the electronic count and the paper count, paper trails are not a perfect solution for guaranteeing accurate and transparent elections. Still, if implemented in conjunction with proper audit procedures and mandatory random sample recounts, they become an important tool that makes it easier to build stakeholders' trust. Paper trails allow the verification of electronic election results and make it possible to identify any faults or manipulation in an

observable and easily understandable process. The lack of a paper trail is often one of the first issues raised by opponents of electronic voting.

Access to the systems source code

Any expert who wants to analyse and understand an electronic voting system needs to have access to its programming source code. Currently, commercially available e-voting solutions are commonly based on proprietary source codes. For commercial and security reasons vendors are usually reluctant to provide access to this source code. However, vendors do increasingly recognize the need to allow source code access and several EMBs already include such access in their e-voting system requirements. The possibilities for public inspection of commercial source codes are often limited in time and scope, come at additional cost, and still only allow limited insight into the functioning of the system being examined.

Using voting systems based on proprietary code therefore often results in IT experts calling for a switch to open source systems. In contrast to proprietary systems, the source code of such systems is publicly available and fully accessible to all interested experts. Opponents of the publication of source codes argue that most currently available systems are not perfect and that publishing them will expose weaknesses to the public and to potential attackers. Advocates of the open source approach, including most computer security experts, argue that, although publishing the code can reveal problems, it also guarantees that solutions will be found quickly. For open source advocates, keeping the codes secret is viewed as 'security by obscurity' and creates a situation where only a few insiders know about the weaknesses of a system. While some efforts to develop open source e-voting systems are ongoing, such systems are currently not readily available. It should be noted that access to source codes is only one step towards full technical transparency. To fully understand an e-voting system's behaviour, the compilers which are used to translate the human-readable source codes into machine-readable code, the voting system's hardware and the operating system need to be analysed as well.

Systems with or without voter authentication

Some e-voting systems are only used for casting the vote and voter authentication remains manual; others contain an additional module for authenticating voters based on an electronic poll book or electoral register. All Internet voting systems, and some voting machines in polling stations, contain an authentication module. A voting system that performs both functions—voter identification and the casting of the ballot—is inherently open to criticism and potentially to malpractice. Even when the two functions are kept rigidly separate, there may be a possibility for inside operators to cross-check the two data sets. This possibility requires the establishment of specific technical and procedural security measures to guarantee that these two sets of information cannot be linked under any circumstances. The secrecy of the vote relies on these measures and it is important that they can be clearly communicated and demonstrated to interested stakeholders.

Internationally vs domestically developed systems

Developing reliable and secure e-voting systems according to the parameters mentioned above is a substantial effort that is often beyond the capacities of a single election administration or the domestic commercial IT sector. Therefore many EMBs purchase their e-voting solutions from international vendors.

Usually only EMBs in countries with a very large electorate will find it sustainable to develop and maintain an electronic voting solution domestically. An important advantage of this approach is that the costs of the system are invested in the local economy and local competence is built in the process. At the same time it can be difficult for locally-built systems to take on board the lessons learned from experiences in other countries. When developing a local e-voting solution it is important not to do this in a vacuum and to review and compare internationally available systems, as well as analysing the latest trends and research and connecting this analysis to an understanding of the local needs and the rationale for the introduction of the technology.

A mixed approach, between local and international sourcing options, is to have international vendors partner with local companies to produce some of the e-

voting equipment in country, and by so doing invest some of the costs of e-voting back into the local economy

Costs

Several of the options mentioned help increasing the transparency of an electronic voting solution and help to build stakeholder confidence, but they also come at an additional cost.

Most vendors will charge more for their solution if they have to provide access to the systems source code.

An e-voting system with paper trail is more expensive that one without and thorough certification can significantly increase the overall cost of electronic voting.

So one important challenge when implementing e-voting is to discuss and decide how secure and how transparent a system needs to be in a given context and match this need to a solution that comes at acceptable and sustainable cost..