INTERNATIONAL IDEA INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

Introducing Electronic Voting:

Essential Considerations

PolicyPaper

December 2011

Electronic voting is often seen as a tool for making the electoral process more efficient and for increasing trust in its management. Properly implemented, e-voting solutions can increase the security of the ballot, speed up the processing of results and make voting easier. However, the challenges are considerable. If not carefully planned and designed, e-voting can undermine the confidence in the whole electoral process. This policy paper outlines contextual factors that can influence the success of e-voting solutions and highlights the importance of taking these fully into account before choosing to introduce new voting technologies.

International IDEA at a glance

What is International IDEA?

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization that supports sustainable democracy worldwide. International IDEA's mission is to support sustainable democratic change by providing comparative knowledge, and assisting in democratic reform, and influencing policies and politics.

What does International IDEA do?

In the field of elections, constitution building, political parties, gender in democracy and women's political empowerment, democracy self-assessments, and democracy and development, IDEA undertakes its work through three activity areas:

- providing comparative knowledge derived from practical experience on democracy-building processes from diverse contexts around the world;
- assisting political actors in reforming democratic institutions and processes, and engaging in political processes when invited to do so; and
- influencing democracy-building policies through the provision of our comparative knowledge resources and assistance to political actors.

Where does International IDEA work?

International IDEA works worldwide. Based in Stockholm, Sweden, it has offices in Africa, Asia and Latin America.

International IDEA resources on Electoral Processes

International IDEA
Publications Office
SE -103 34 Stockholm
Sweden

Graphic design by: Glad grafisk form

Printed by: Bulls Graphics, Sweden

ISBN: 978-91-86565-21-3

Contents

Key Recommendations

1 Define the goals clearly. Make sure electronic voting is the most appropriate solution.

2 Be aware of the challenges. None of the systems currently available is perfect, nor is there agreement on what a perfect e-voting system would look like. Learn from previous, international experience.

3 Get key stakeholders to buy in. Opponents of the system can and will come up with objections and weaknesses and create distrust in the system and potentially in the entire electoral process.

4 Provide for auditing and certification. These are important confidence-building measures and should be transparent, allowing stakeholders access to procedures and documentation.

5 Allow enough time for project implementation. Usually the technical implementation of e-voting systems takes at least one year after awarding the tender and it takes a much longer time for an e-voting system to be socially accepted.

6 Plan for training, professional development, and civic and voter education. Well-informed stakeholders will find it easier to trust a new system.

7 Consider sustainability issues and plan for the future. Consider the total cost of ownership, including review, upgrades and replacement as well as adjustments to new requirements over time, rather than the one-time purchase costs.

Executive Summary

Technology upgrades in elections are always challenging projects that require careful deliberation and planning. Introducing electronic voting (also called e-voting) is probably the most difficult upgrade as this technology touches the core of the entire electoral process—the casting and counting of the votes. E-voting greatly reduces direct human control and influence in this process. This provides an opportunity for solving some old electoral problems, but also introduces a whole range of new concerns. As a consequence, e-voting usually triggers more criticism and opposition and is more disputed than any other information technology (IT) application in elections.

This paper does not provide a safe recipe for the successful introduction of e-voting; rather, it presents some of the recurring challenges and concerns that surround this technology and should be taken into account in an implementation strategy.

The introductory chapter provides the background and discusses typical features provided by e-voting solutions and the various technical options that are often at the root of controversies, and also provides an overview of the strengths and weaknesses of this technology.

Based on this background, the paper introduces guiding principles and overall goals for the implementation of e-voting. Emphasis is put on building trust in this new technology. Various factors contributing to this trust-building exercise are visualized as a three-layered pyramid of trust, describing the context in which e-voting projects are implemented. All three layers of this pyramid are closely interrelated. Trust needs to be built on all layers of the pyramid in parallel which commonly takes several years and several electoral cycles to achieve. Weaknesses in just one layer can be enough to undermine all the others and may quickly lead to a loss of trust in the entire system.

Finally, the paper offers some key recommendations for those implementing e-voting systems.

Background and Introduction

Electronic voting in polling stations is in place in some of the world's largest democracies, and Internet voting is used in some, initially mainly small and historically conflict-free, countries. Many countries are currently considering introducing e-voting systems with the aim of improving various aspects of the electoral process. E-voting is often seen as a tool for advancing democracy, building trust in electoral management, adding credibility to election results and increasing the overall efficiency of the electoral process. The technology is evolving fast and election managers, observers, international organizations, vendors and standardization bodies are continuously updating their methodologies and approaches.

Properly implemented, e-voting solutions can eliminate certain common avenues of fraud, speed up the processing of results, increase accessibility and make voting more convenient for citizens—in some cases, when used over a series of electoral events, possibly even reducing the cost of elections or referendums in the long term.

Unfortunately not all e-voting projects succeed in delivering on such high promises. The current e-voting technology is not problem-free. Legislative and technical challenges have arisen in some cases; in others, there has been scepticism about or opposition to the introduction of new voting technologies.

The inherent challenges of e-voting are considerable and linked to the complexities of electronic systems and procedures. Many e-voting solutions lack transparency for voters and even for election administrators. Most e-voting solutions are only fully understood by a small number of experts and the integrity of the electoral process relies largely on a small group of system operators instead of thousands of poll workers. If not carefully planned and designed, the introduction of e-voting can undermine confidence in the whole electoral process. It is therefore important to devote adequate time and resources to considering its introduction and looking at previous experiences of electronic voting.

A definition of electronic voting

Some definitions of electronic voting are very broad. This paper focuses on systems where the recording, casting or counting of votes in political elections and referendums involves information and communication technologies.

E-voting: not comparable to any other ICT application?

Virtually every information and communication technology (ICT) application is built in a way that allows verification of its proper functioning by observing the application's outputs. If a customer does not trust a bank's electronic banking system, he or she can check their account overview and confirm that all transactions are reflected properly. If the owner of a car does not trust the electronics in the car, every starting of the engine gives an opportunity to test that system.

E-voting systems are fundamentally different. Due to the requirement to protect the secrecy of the vote, they have to avoid any connection between the voter's identity and the vote cast. This is in itself a challenge as standard ICT systems are inherently built for tracking and monitoring transactions that happen on them. More importantly, breaking the link between voter and vote means that the examination of an e-voting system after an election cannot prove directly that every vote was indeed counted and tallied as cast.[1] This is why indirect proofs of the validity of the electronic results, such as paper trails or system certification, in combination with stringent quality control and security procedures, are exceptionally important. Without such mechanisms, manipulated or incorrect results produced by an e-voting system could remain undetected for a long time.

Typical features and functionalities of e-voting systems

Internally, electronic voting systems have many functions, including encryption, randomization, communication and security systems. A specific analysis of these functionalities goes beyond the immediate scope of this paper. For a basic understanding of what e-voting systems can do, however, it is useful to consider the following list of some of the end-user functionalities that such systems can provide to both voters and election officials.

- *Electronic voter lists and voter authentication.* Part of an electronic voting system can be an electronic voter list, covering either a single polling station or the entire country. This list can be used to authenticate eligible voters and to record that they have cast their vote.
- *Poll worker interfaces.* Special functionalities that are only available to poll workers, for example, resetting the vote count at the opening of the polling station, closing polling, printing and transmission of results.
- *Interfaces for casting votes.* These include touch screens, optical mark recognition (OMR) ballot papers that are fed into a scanner, touch-sensitive tablets, push buttons, web pages or special client software for Internet voting.
- *Special interfaces for handicapped voters.* These include Braille or audio input devices for the blind, easier access for voters with physical disabilities, and simpler interfaces for illiterate voters.

[1] **End-to-end verifiable e-voting systems like Scantegrity or Prêt à Voter aim at achieving such functionality. However, at the time of writing such systems are not widely used in real life. See the list of References and Further Reading.**

Strengths associated with e-voting

- Faster vote count and tabulation.
- More accurate results as human error is excluded.
- Efficient handling of complicated electoral systems formulae that require laborious counting procedures.
- Improved presentation of complicated ballot papers.
- Increased convenience for voters.
- Potentially increased participation and turnout, particularly with the use of Internet voting.
- More attuned to the needs of an increasingly mobile society.
- Prevention of fraud in polling stations and during the transmission and tabulation of results by reducing human intervention.
- Increased accessibility, for example by audio ballot papers for blind voters, with Internet voting as well for housebound voters and voters from abroad.
- Possibility of multilingual user interfaces that can serve a multilingual electorate better than paper ballots.
- Reduction of spoilt ballot papers as voting systems can warn voters about any invalid votes (although consideration should be given to ensuring that voters are able to cast a blank vote should they so choose).
- Potential long-term cost savings through savings in poll worker time, and reduced costs for the production and distribution of ballot papers.
- Cost savings by using Internet voting: global reach with very little logistical overhead. No shipment costs, no delays in sending out material and receiving it back.
- Compared to postal voting, Internet voting can reduce the incidence of vote-selling and family voting by allowing multiple voting where only the last vote counts and prevent manipulation with mail-in deadlines through direct control of voting times.

Weaknesses associated with e-voting

- Lack of transparency.
- Limited openness and understanding of the system for non-experts.
- Lack of agreed standards for e-voting systems.
- System certification required, but no widely agreed standards for certification.
- Potential violation of the secrecy of the vote, especially in systems that perform both voter authentication and vote casting.
- Risk of manipulation by insiders with privileged access to the system or by hackers from outside.
- Possibility of fraud through large-scale manipulation by a small group of insiders.
- Increased costs for both purchasing and maintaining e-voting systems.
- Increased infrastructure and environmental requirements, for example, with regard to power supply, communication technology, temperature, humidity.
- Increased security requirements for protecting the voting system during and between elections including during transport, storage and maintenance.
- Reduced level of control by the election administration because of high vendor- and/or technology-dependence.
- Limited recount possibilities.
- Need for additional voter education campaigns.
- Possible conflict with the existing legal framework.
- Possible lack of public trust in e-voting-based elections as a result of the weaknesses above.

- *Interfaces for the results output.* For voting machines (see the definition below) this is often a printer. However, some machines only use digital displays. Once voting is closed this interface can be used to display or print the results that were recorded by the voting machine. If results are printed the printouts can be used as physical evidence of the results produced by the voting machine, and copies can be distributed to stakeholders present at the polling station and can also be posted for public display.
- *Printers for printing a voter-verifiable receipt for each vote* (see below on the voter-verified audit paper trail, VVPAT).
- *Result transmission system.* Many voting machines can transmit results to central counting systems, for example via the Internet, telephone, mobile phone or satellite connection. In the absence of communication links, the results can also be transported physically, using electronic storage media such as memory cards.
- *Result tabulation systems, usually located at result processing centres.* At the end of election day, they receive electronic results from polling stations and automatically tabulate the results for the various competitions and districts.
- *Result publication systems.* Preliminary and final results can be published in many different ways including on websites, CDs, and geographic visualization systems, and if required on all levels of detail down to single polling stations. The more detailed the published results are, the more transparent the election.
- *Confirmation code systems.* Some e-voting solutions allow for control codes that are intended to allow individual verification of each vote by the relevant voter.

Typologies of e-voting systems

In discussing the advantages and disadvantages of the various e-voting systems it is useful to distinguish several overlapping typologies of systems.

All typologies have various strengths and weaknesses, both when compared with each other and when compared to traditional paper-based voting. There is no such thing as a perfect electronic voting system and available systems continue to evolve with ongoing technological advances. It is therefore important to choose the right system for the right context by carefully weighing the advantages and disadvantages of all options.

The types of e-voting systems

Technically, most e-voting systems fall into one of the following four types.

- *Direct recording electronic (DRE) voting machines.* 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.
- *OMR systems* which are 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 (where scanning and counting happens in the polling station, directly as voters feed their ballot paper into the voting machine).

- *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.
- *Internet voting systems* where votes are transferred via the Internet to a central counting server. Votes can be cast either from public computers or from voting kiosks in polling stations or—more commonly—from any Internet-connected computer accessible to a voter.

The general term voting machine (VM) is often used to refer to DRE and PCOS systems as well as to voting kiosks for Internet voting.

E-voting in controlled and uncontrolled environments

E-voting can be conducted either 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, embassies and so on.

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. Current forms of Internet voting have not yet been able to provide a definitive solution to such concerns.

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

E-voting as only or alternative channel

E-voting can be introduced as the only voting channel available to voters or it can be offered as an additional option for voting and the voter can choose the preferred channel.

Internet voting is commonly introduced as an alternative channel while voting machines are mostly introduced as the only voting channel available to voters in a polling station.

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.[2] 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.

Proprietary code vs open source

Any expert who wants to analyse and understand an electronic voting system needs to have access to its programming source code.

[2] End-to-end verifiable e-voting systems with cryptographic receipts allow direct verification. However, such systems are not widely used in real life, not least because they are not very user-friendly. See the list of References and Further Reading.

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.[3]

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.

[3] **One body working to develop open source e-voting systems is the US Open Source Digital Voting Foundation.**

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.

Guiding Principles and Overall Goal

The advantages of e-voting listed in the previous chapter may only be among the reasons why an EMB considers the introduction of this technology. Considerations such as the faster processing of results, the prevention of fraud and the provision of a better service to voters are often high priorities.

One common motivation for the introduction of e-voting is to demonstrate the technical abilities of a country or stakeholders. Very often, it is believed that such a choice might show the external world the level of internal development achieved in a country. To avoid falling into the trap of technological determinism,[4] this should not be the main reason for pursuing an electronic voting strategy.

Whatever the exact expectations, the EMB should always aim to achieve several overall goals:

- The benefits of the chosen e-voting solution should outweigh the drawbacks, not only when compared to other electronic voting systems but also when compared to paper voting.
- Any additional cost incurred by e-voting should be justified by the benefits that can be expected from the solution.
- Even if heavy vendor involvement is required, the EMB should have or build the capacity to retain overall control of the e-voting system, and sufficient resources must be available to the EMB, not only during the initial introduction but also for the long-term operation of e-voting systems in order to avoid complete dependence on an external entity.
- A new e-voting system should not only help the election administration; it should also be a service to citizens. It should make it easier for voters to cast their vote, or at the very least not create more difficulties compared to previous procedures.
- Finally, the general public, as well as other key stakeholders in the electoral process, should trust the voting solution and be confident in it. Their trust in the e-voting system should be built on a well-understood and reliably implemented solution rather than on the ignorance of key stakeholders.

Building trust may be the most critical and all-encompassing goal. The pyramid of trust outlined in the next chapter can be useful to help understand how many distinct factors contribute to building that trust.

[4] **The presumption that a society's technology is the primary driver of social change.**

The E-Voting Pyramid of Trust

'A voting system is only as good as the public believes it to be.'

McGaley and Gibson, 2003

A credible electoral process through public trust and confidence

The top of the pyramid—and the ultimate goal of electoral reform by implementing an e-voting solution—is a credible electoral process that enjoys a high level of public trust and confidence in the new system.

Public trust is initially mainly built on the socio-political context in which e-voting is introduced. Some factors in this context can be directly addressed by a comprehensive e-voting implementation strategy, while others, such as a general lack of trust in the EMB or fundamental political or technical opposition, will be more difficult to change.

A supportive socio-political context significantly helps the introduction of e-voting and can temporarily even cover up problems that may occur in the detailed technical implementation. Trust in a solution that is technically weak can, however, be misleading. Weaknesses in the operational, technical or legal foundations will eventually surface and may then discredit not only e-voting, but possibly the entire electoral process, especially when the political stakes of an election are high. The complete cancellation of electronic voting from a country's electoral framework may be the consequence, as has happened in Germany, Ireland and the Netherlands.

'People will use insecure systems if they feel or think they are secure.'

Oostveen and van den Besselar, 2004

A negative socio-political context creates serious risks, even if the technical and operational foundations of the e-voting solution are sound. It is very difficult to make e-voting systems transparent and their operations understood in the short and even medium term by a non-expert audience. Weak social and political support will hinder the implementation of a trusted e-voting solution as opponents will find it much easier to undermine trust in this voting technology by pointing to some of its inherent weaknesses.

The socio-political environment

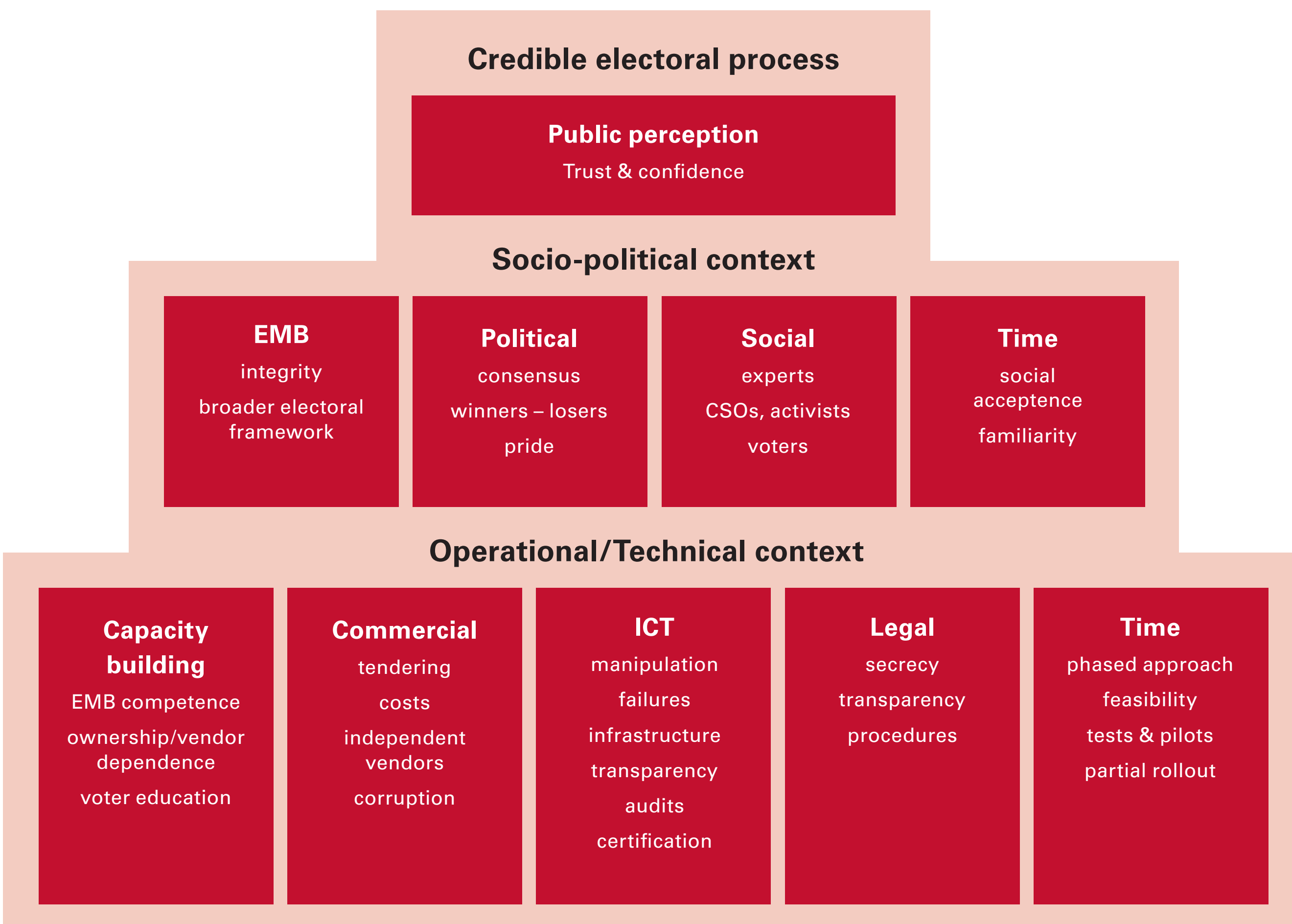
Trust in election administration and confidence with the broader electoral framework

E-voting tends to take a good deal of the responsibility for the electoral process away from thousands of polling station officials and place this responsibility in the central election administration and the implementers of the e-voting system. In doing so, the implementation of e-voting reduces the risk of widespread fraud and manipulation at polling station level, but concentrates the risk of manipulation at the central level.

This is beneficial in an environment where there is little public confidence in polling station officials, but where the central election administration is trusted. However, in an electoral environment where there is little trust in the central EMB structure, the introduction of electronic voting systems can easily become subject to rumour-mongering about potential central manipulation. Some of these rumours may be hard to refute.

International IDEA's *Handbook on Electoral Management Design* lists independence, impartiality, integrity, transparency, efficiency, professionalism and service-mindedness as guiding principles for trusted EMBs. If there are problems with the EMB's track record in these areas, such problems and related doubts will probably be aggravated through electronic voting.

Figure 1. The pyramid of trust



Estonia

Internet voting was introduced as an additional voting channel in 2005 and enjoyed widespread trust from the very beginning.

Estonia is a conflict-free country that enjoys a high level of trust in its institutions, and e-voting accompanied a wider programme of digitalization of its institutions. Not even massive hacking attacks against Estonia's e-government infrastructure ahead of the 2007 elections undermined this confidence.

In 2011 almost 24 per cent of votes were cast online.

As with any other form of technology upgrade, electronic voting systems could increase the existing capacity; however, if the initial capacity level is low, the opposite is likely to happen: the positive effects are bound to fade and, if trust is already low, distrust is likely to increase.

Together with the question of trust in the EMB itself, it is also important to consider trust in the broader electoral framework. In an environment where many stakeholders are not confident with the electoral system design, mechanisms to deal with electoral disputes and complaints, officials or the government, the EMB will find it difficult to win the level of trust required to implement a widely accepted e-voting solution.

Finally, to facilitate widespread social acceptance, the new voting technology needs to show clear benefits for voters. If voting gets easier, more accessible and more convenient for citizens they will accept and support the new system more easily.

Venezuela

When DRE-based e-voting was introduced in Venezuela in 2004, trust in the impartiality of the EMB was very low. The potential benefits of curbing widespread fraud throughout the country through e-voting were offset by the lack of trust at the central level and there were fears that the new e-voting system would be used to manipulate results.

This, in combination with technical weaknesses of the system, which did not eliminate the theoretical possibility of cross-checking voters and votes, created a critical situation just a few days before the 2005 election.

An effective remedy to restore credibility included massive paper trail recounts in 45 per cent of the polling stations—far more than the small statistical samples that are normally deemed sufficient—and the elimination of the automated identification process. This made the process very expensive and no longer cost-effective compared to paper-based solutions. But it was the only way to remedy the lack of trust that the technology choice itself could not make up for.

Bahrain

In 2006, only weeks before the first e-voting was supposed to take place, the government decided to return to paper voting due to pressures from the opposition, which suspected vote-rigging.

Political consensus

E-voting systems can be most easily introduced when there is political consensus about the benefits of the new voting system. Political actors may, however, oppose electronic voting for many reasons, either in principle, because they have real technical concerns, or because they fear the new voting channel is an advantage for their opponents; or because they believe that other parties may receive more credit for modernizing this part of elections; or just because they do not trust in the independence of those implementing the system. Facing such opposition, successful confidence building may be difficult or impossible.

It is therefore always a very wise approach to seek multiparty support in the approval of the legislative changes needed to introduce electronic voting systems. The same is true even when it is not a statutory requirement for changing the legislation.

A related risk factor in this context is e-voting systems that are introduced as projects of political, or more commonly national, pride—with the intent of demonstrating technology savvy and modernity. Sustainability and a meaningful cost-benefit ratio can be the first victims of such an approach. In these types of contexts, even obviously unsuitable or inadequate solutions may be pushed through and perceived as necessary to avoid the embarrassment of a failed prestige project.

An approach whereby e-voting is considered an option that can be withdrawn without important stakeholders losing face helps to minimize this risk.

Social context

Key social actors, such as non-governmental organizations (NGOs) and experts, often have strong opinions or concerns about e-voting. Ideally these actors should be included early on when planning the introduction of e-voting, both by providing them with ample information about the system envisaged and by allowing them to raise their concerns in the early phases, when there is still time to address them.

ICT security expert groups are often strong opponents of e-voting. Some of this opposition is quite fundamental, and many currently available systems do not address the concerns of such opponents. It is important to hear and address their concerns by clarifying any misunderstandings, correcting weaknesses or accepting certain risks as a trade-off for the benefits of introducing the new system.

Non-technical concerns also need to be seriously considered. E-voting projects can receive criticism from stakeholders who mourn the loss of the ritual of voting and

Brazil

The introduction of e-voting in Brazil was motivated by economic and fraud-prevention factors. A multi-year approach for the gradual introduction of e-voting was adopted and included the following steps:

1. Voter and civic information including usability and feasibility studies starting in 1986
2. Capacity building within the EMB, and digitalization of the result aggregation
3. Development of hard- and software, involving local technical expertise
4. Testing of equipment in the Brazilian environment
5. EMB's final decision on the type of machine fitting the Brazilian context best
6. Quality control and testing in various environments
7. Authorization of e-voting in 1996 local and municipal elections
8. Post-election review and subsequent quality overhaul
9. Full e-voting roll-out in the 2002 general elections

A hacking competition was organized in 2009 to create additional confidence in the technology.

Over the years citizens and stakeholders gained enough trust in the system for the paper trail that was initially included to be deemed redundant and scrapped after technical problems associated with the printers.

While systems without paper trails are often disputed, the Brazilian case exemplifies what can be achieved with successful trust, capacity and consensus building over many years and several electoral cycles.

its social importance in an electoral process, for example, who argue that e-voting reinforces the digital divide as it appeals more to the affluent and literate groups. Others argue that any spending on electronic voting is a luxury in contexts where many citizens see their basic day-to-day needs as not being catered for. The results of a clear analysis of benefits and drawbacks are essential in order to address such criticism.

Time

Time is a critical factor on various levels. Operationally, e-voting cannot be introduced overnight, but social acceptance of it should realistically be expected to take much longer than pure technical implementation. Commonly it will take several electoral cycles without major technical glitches or political controversy, and with trusted results and long-term civic education campaigns, before citizens and stakeholders are fully confident with electronic voting, based on their own experience and knowledge. Ideally, information and sensitization campaigns on the possible introduction of e-voting systems should start well in advance of technical implementation, with the possibility to shape the technical requirements of the system on the basis of the social context's response and concerns.

Operational and technical foundations

Preparing or ensuring a supportive socio-political environment is a very important factor for the successful implementation of e-voting. Sometimes a poorly designed or unsuitable voting system can be successfully used for some time if this environment is largely supportive. Still, when underlying technical problems grow too big, they will sooner or later complicate the process. When placed against a backdrop of tight deadlines, and a weak or inadequate civic education and information campaign, a defensive protective attitude can easily develop within the EMB as the natural reaction to criticism. As issues become more and more visible, doubts about the electoral process will build up, the election administration and the e-voting system will lose credibility and at some point e-voting may need to be scrapped altogether to restore trust in the electoral process.

Therefore it is important that the trust in an e-voting system is well deserved in the sense that the e-voting solution selected is built on solid technical foundations. Such technical foundations have legal, ICT, project management, commercial and timing aspects.

Capacity building

Electronic voting should not be seen as a technical solution to a problem of lack of capacity or of competence within the election administration. On the contrary, it will require more expertise and more capacity building at all levels of the EMB as well as with other key external stakeholders.

One of the most difficult tasks for EMBs is to retain oversight, control and ownership of the e-voting solution, thus avoiding dependence on the vendor and a vendor-driven approach. Outsourcing and relying largely on outside companies for logistics and technology in other aspects of organizing an election may be acceptable, but when it comes to the casting and counting of the votes the EMB is always expected to be fully aware of how this is conducted and to be able to intervene in a transparent

The Netherlands

In 2008 e-voting was suspended after 20 years of use when activists showed that the systems in use could, under certain circumstances, endanger the secrecy of the vote.

An official commission found that the Ministry of the Interior and Kingdom Relations, which was responsible for organizing elections, was lacking in-house expertise, causing too much dependence on vendors and certification agencies. Voters had to switch back to pen and paper.

In spite of the problems, many stakeholders, especially mayors and voters, still trust e-voting. On the basis of positive experiences from the past they are asking for a reintroduction of voting computers.

and efficient manner in the event of any problem. This requires significant technical and managerial competence and the EMB needs to be in a position to build and retain such competence.

Moreover, the security of an electronic voting system depends on strict adherence to prescribed procedures by all officials involved in their operation, from the EMB commissioners to poll workers. This makes comprehensive training at all levels and stages of the electoral process absolutely critical for the success and credibility of an electronic election.

Finally a comprehensive civic and voter registration campaign is important. Citizens need to learn more than simply how to cast their votes electronically. They also need to understand the rationale for the specific technology choice adopted and the trustworthiness of the solution selected. Specific voter information exercises need to be set up by the EMBs well in advance of election day, and possibly connected to other public events where the exercises are likely to involve large strata of the population. This type of approach requires adequate budgetary provision, which is often overlooked. Eventual public opinion about the entire e-voting effort might depend entirely on the public's degree of familiarity with the selected solution on election day.

The Philippines

Following regional pilots in 2008, PCOS-based e-voting was introduced throughout the country in 2010.

After delays in the early project phases, only less than one year was available for system implementation.

About one week before the election the system came close to breakdown when it was discovered that all 75,000 PCOS machines were wrongly configured. The problem was solved at the very last moment by physically reconfiguring all voting machines in a massive logistical operation.

After an eventually successful election, one concern was the great extent to which the EMB depended on the system vendor.

Commercial aspects, procurement and costs

Before embarking on an e-voting project, a full cost-benefit analysis as part of a wider feasibility study should be conducted.

All ICT equipment has replacement and upgrade cycles of only a few years. This is especially true for the rapidly evolving electronic voting technology. Special attention should be paid to a realistic calculation of the total cost of ownership (TCO), including all costs of storage, maintenance, upgrading and operating of the system over several electoral cycles. If electoral cycles are long and voting machines may only be used once every few years, leasing may be more cost-effective and transparent than purchasing e-voting systems.

Ireland

Between 2005 and 2009, Ireland invested over 60 million euros in an e-voting solution without VVPAT, before deciding that the system was unreliable and would need further, costly modifications before it could be used.

High costs in combination with a lack of trust led to the scrapping of e-voting in 2009. In the absence of a solution for the destruction of the unused machines, Ireland is still having to cover the storage costs in the foreseeable future.

Detailed and clear specifications, developed solely under EMB control and without vendor influence, but properly understood by vendors and those who evaluate the tenders, are of crucial importance. Spending more time detailing and explaining the specifications, while often considered a luxury, will greatly improve the chances of the most suitable bid being identified and selected in the procurement process.

The costs of e-voting, especially in the initial implementation phases, tend to be substantial. A procurement process with transparent and open procedures is essential to avoid any perception of the process being hijacked by vendors. Additionally, the process needs to defuse any concerns about corruption or political bias on the part of the vendor that might weaken trust in the solution eventually selected.

Procurement should not be initiated at the last possible moment. With a fixed election day as the ultimate deadline, it is not uncommon for procurement time lines to be underestimated at the cost of technical implementation time lines. This creates the risk of systems being immature and poorly implemented. Careful consideration of procurement against the electoral cycle is a key part of satisfactory implementation.

The contract award process should never be carried out without effective pilot and validation tests over a restricted number of shortlisted proposals before the winning one is identified. This type of exercise can reveal critical system failures in some segments of the process that have not been properly addressed by the vendor, potentially causing additional expense or changes in the approach that might be difficult to explain and support later on.

ICT, security and transparency

Choosing the right voting technology for a given context is essential. The technology needs to address the requirements identified and to operate reliably within the available infrastructure, taking into account the prevailing environmental conditions.

The ICT component should be implemented with a high level of transparency that generates broad stakeholder confidence. This needs to include credible and widely publicized mechanisms for preventing manipulation by outsiders as well as by insiders operating the system.

India

Following pilots since 1982, the biggest democracy in the world has successfully used voting machines throughout the entire country since 2002. Two distinct features of the Indian VMs are the low price, significantly lower than that of most other systems, and a relatively simple technology.

The Indian system provides no paper trail, a fact that is widely accepted, given the absolute trust institutionally granted to the EMB. However, the simplicity of the system created controversy around alleged security problems in 2010 and led to the Indian EMB considering the introduction of paper trails in 2011.

Alternative arrangements in case of unexpected inadequacies of the infrastructure, breakdowns and system failures should be prepared in order to ensure continuity in the project, especially in cases of time-limited or early implementation.

A significant factor to enhance the transparency and security of the e-voting solution is a stringent certification and/or audit procedure, allowing for independent confirmation of the correctness of the results produced.

In the case of voting machines in controlled environments, this is ideally complemented with a VVPAT system.

VVPAT systems, in connection with properly conducted manual recounts of randomly selected polling stations, provide an efficient method of transparently verifying the accuracy of the results produced by voting machines. Meaningful use of VVPAT systems requires the determination of a statistically sound random sample size and a selection procedure for the recount, as well as mechanisms for resolving potential discrepancies between the manual and the electronic count.

In the absence of a VVPAT, the credibility of an e-voting system depends entirely on stringent certification of the system before it is used, accompanied by audits throughout and after the electoral process that confirm that the systems in use are the ones that have been certified and that all necessary procedures have been adhered to as prescribed.

An important requirement for meaningful certification is the availability of a certification agency that is trusted by all stakeholders. This agency should be clearly independent of political, vendor and EMB influence. The certification methodology and results should be available to all stakeholders, including domestic and international observers.

Any system certification has to be conducted against an agreed set of requirements and standards. Currently there are no globally agreed standards and requirements for e-voting systems, so they will have to be defined by each country that moves in this direction, possibly based on international examples, as an integral part of the e-voting implementation project. A public comment exercise may be a good opportunity to give a wide range of stakeholders and experts a say, allowing them to participate in the process and offer early critiques that could strengthen the process.

Certification and audits are important confidence-building measures and should be conducted transparently with public access to related documents and procedures. Any requirements for accessing information—such as non-disclosure agreements—hinder transparency and are potentially a sign of weakness, and should be avoided wherever possible.

The United States

Following the 2002 Help America Vote Act, the United States saw a massive investment in voting machines, many without a paper trail.

In 2005 and 2007 the US Voluntary Voting System Guidelines (VVSG), currently the most comprehensive guidelines with specifications and requirements for certifying voting machines, were published.

By 2008 many states required paper trails, making voting machines without a paper trail obsolete.

As of 2010, 40 states have moved towards requiring paper trails.

The legal framework

Electronic voting often significantly changes the way in which elections are conducted in a country. These changes often touch upon interactions between different institutions that might be very sensitive for the EMB to handle, or even be outside the EMB's remit or mandate. Accordingly all adjustments that are required between the technology and the legal framework must be identified.

The legal framework needs to be reviewed to identify direct and indirect references to fundamental obligations for democratic elections that the state has subscribed to at the international and regional level. These references might be interpreted differently in an e-voting context and require harmonization with the technology choice that the country wants to implement. Having first ascertained that the choice of technology is compatible with the overall requirements for democratic elections, the selected e-voting solution then needs to be reviewed in the light of any reference in the national legislation to election terminology, such as references to ballot boxes, paper ballots, the paper balloting and counting process, the value of spoilt and blank votes, fraud and so on, in order to ensure that the specific implementation solution is consistent with their meaning.

There are also new types of concerns that require specific attention, such as the relation between electronic voter registration systems and e-voting choice, or the timely addressing of e-voting-related complaints in a system that produces results more speedily. Possible inter-institutional arrangements between the EMBs and the different authorities that might be in charge of these other aspects need to be considered and eventually addressed. In the first case, the data exchange arrangements

Germany

In 2009 e-voting was declared unconstitutional. According to the constitution all elections must be public. The Constitutional Court ruled that this principle requires that the key steps of an election—including vote casting and counting—be subject to public scrutiny which should not require any specialized knowledge.

An independent method for detecting any computer mistakes was also deemed to be of key importance.

for the automated identification of voters might require special attention; in the second case, the body adjudicating over electoral disputes will have to be informed about the different meaning that notions such as the secrecy of the vote, recounts, the handling of mistakes and voter coercion may take on in an electronic context.

However, legal implications can even go much further than that: a legal review should probably go beyond the electoral law and the fundamental obligations for democratic elections, and cover layers of parallel or subsequent legislation.

Issues such as digital identity, digital identification, digital signatures, data protection, data retention, and certification and audit regulations can all be relevant. The German case shows that the constitution also needs to be taken into account.

It is not uncommon for technology to render some old manual procedures redundant. A practical approach may be to choose or modify technology to reflect old procedures, thereby reducing the need for major legal change. Decisions on such an approach should be carefully evaluated as an unnecessarily complex and error-prone solution may be the consequence.

This wide range of legal change, which can take several electoral cycles to achieve (covering the progress from test to pilot to full-scale electronic elections), highlights how important a strong political consensus on the introduction of e-voting is.

Ideally, a legal reform/review process should accompany the technical experimentation with electronic voting and be influenced by its experimentation. For the best possible technical solution to be achieved (and rooted in solid legal foundations), no rigid predefined legal framework should drive and shape the technical development, nor should technology alone drive laws and regulations. Adjustments of the two need to take place in tandem, always bearing in mind that electoral and democratic principles should never be jeopardized or weakened. Without a strong and multiparty political consensus on the process, such an approach is not achievable.

Time and phased implementation

What all other operational aspects have in common is that they take time:

- time to identify, define and specify requirements;
- time to build capacity in the EMB;
- time to understand and evaluate trade-offs;
- time to update the legal framework;
- time to procure and implement the technology; and
- time to educate the citizenry.

All these activities can be expected to take several electoral cycles and require a phased implementation approach.

Such a phased approach should start with feasibility studies and testing of the different available options, followed by pilot implementations in mock elections or local or regional pilots that are gradually expanded before covering the entire electorate.

A phased approach will not only provide the time to build a technically mature system based on hands-on experience; it will also give the citizens and stakeholders time to acquaint themselves with this new technology.

While it takes time to implement a reliable system, technology—once implemented—also becomes obsolete over time. Periodic technical reviews of the system are required to keep the system up to date and secure.

United Kingdom

In 2005, after various local pilots, it was concluded that e-voting systems were expensive, brought about no increase in turnout, and lacked an adequate audit trail. Paper voting was more trusted.

Recommendations

1. Define the goals clearly.
The reason for introducing electronic voting should be clearly defined. Clear goals make it easier to evaluate the advantages of possible e-voting solutions between alternative systems as well as against the existing or an improved paper voting system.

2. Be aware of the challenges.
E-voting is still work in progress. Currently none of the available systems are perfect, nor is there agreement on what such a perfect e-voting system would look like. One can only decide to implement a solution that best fits the local context in terms of needs, urgency, costs and timing.

3. Learn from previous, international experience.
Many pitfalls can be avoided by studying what kinds of systems are available and used internationally. Get international experience on board and avoid taking the first steps in isolation.

4. Make sure electronic voting is the most appropriate solution.
Electronic voting is only one option for resolving challenges in the electoral process. Make sure you have evaluated alternative solutions and that e-voting is the best solution in your context.

5. Get key stakeholders to buy in.
As introducing electronic voting is a trade-off of advantages and disadvantages, make sure that there is wide agreement among stakeholders, including political parties, that this technology is overall advantageous.

Be aware that significant opponents of the system can and will come up with objections and weaknesses of the system and create distrust in the system and potentially in the entire electoral process. Even in the absence of genuine opposition to e-voting, the system can become disputed for purely political reasons.

6. Provide for transparent auditing and certification.
E-voting systems should be certified by an independent agency and audits should be conducted throughout the process to allow independent confirmation of the results produced.

Certification and audits are important confidence-building measures and should be transparent, allowing stakeholders access to related procedures and documentation.

7. Allow enough time for project implementation.
Usually the technical implementation of e-voting systems takes at least one year after awarding the tender. Quality, reliability and transparency will be affected by lack of time for project implementation.

This has particular relevance to negotiated transitions, where political negotiations always take all the time available and a technical rush to deliver a first transitional election is almost inevitable. E-voting is unlikely to be appropriate in such circumstances.

Social acceptance of e-voting usually takes several electoral cycles to achieve and is best won by gradually expanding pilot projects.

8. Plan for training, professional development, and civic and voter education.

Well-trained staff are important not only for the successful conduct of an election, but also for allowing the EMB to retain overall control of the e-voting solution, thus taking full ownership of the technology.

Well-informed voters will not only find it easier to use e-voting on election day; they will also find it easier to trust a new system if they understand why it is being introduced, what benefits it brings and how the various security measures that are built in support the integrity of the election.

9. In the event of problems remain transparent, but stay the course.

When problems occur, an overly protective attitude will probably be counterproductive and fuel and exaggerate rumours and allegations which can be more damaging than the actual difficulties encountered.

If the project is well planned on solid foundations, remaining fully transparent and staying the course will be the best strategy.

10. Consider sustainability issues and plan for the future, not only for today.

The cost of introducing e-voting can already be very high, but to remain secure and trustworthy e-voting systems need continuous reviews, upgrades and replacement as well as adjustments to new requirements.

When considering the costs of e-voting it is important to consider the total cost of ownership over time rather than the one-time purchase costs.

11. Be aware that trust can take years to build but be lost in a day.

While it can take a long time for an e-voting system to be socially accepted, but loss of trust can happen fast if there are serious technical problems or political disagreements. A badly implemented or failed e-voting solution can halt further development of this technology for years.

Annex A

The strengths and weaknesses of e-voting: a matrix

The following matrix gives an overview of the typical strengths and weaknesses that different e-voting solutions tend to have compared to paper-based equivalents (Internet voting vs postal voting; voting machine vs paper voting in controlled environments). The classification into 'strengths' and 'weaknesses' is for the purpose of a rough overview only. Details vary depending on specifics of context and systems. Cases where these details are very important are classified as 'mixed'; cases where e-voting has little or no impact are classified as 'neutral'.

Electoral issues, compared to paper voting	Internet voting	DRE without VVPAT	DRE with VVPAT	PCOS	Electronic ballot printers
Faster count and tabulation	Strength	Strength	Strength	Strength	Strength
More accurate results	Strength	Strength	Strength	Strength	Strength
Management of complicated electoral systems	Strength	Strength	Strength	Strength	Strength
Improved presentation of complicated ballot papers	Mixed	Mixed	Mixed	Weakness	Mixed
Increased convenience for voters	Strength	Mixed	Mixed	Weakness	Mixed
Increased participation and turnout	Strength	Neutral	Neutral	Neutral	Neutral
Addressing needs of a mobile society	Strength	Mixed	Mixed	Neutral	Mixed
Cost savings	Mixed	Weakness	Weakness	Weakness	Weakness
Prevention of fraud in polling station	Neutral	Strength	Strength	Strength	Strength
Greater accessibility	Mixed	Mixed	Mixed	Weakness	Mixed
Multi-language support	Strength	Strength	Strength	Weakness	Strength
Avoidance of spoilt ballot papers	Strength	Strength	Strength	Strength	Strength
Flexibility for changes, handling of deadlines	Strength	Strength	Strength	Weakness	Strength
Prevention of family voting	Strength	Neutral	Neutral	Neutral	Neutral
Lack of transparency	Weakness	Weakness	Mixed	Mixed	Mixed
Only experts can fully understand the voting technology	Weakness	Weakness	Mixed	Mixed	Mixed
Secrecy of the vote	Weakness	Mixed	Mixed	Mixed	Mixed
Risk of manipulation by outsiders	Weakness	Mixed	Mixed	Mixed	Mixed
Risk of manipulation by insiders	Weakness	Weakness	Weakness	Weakness	Weakness
Costs of introduction and maintenance	Strength	Weakness	Weakness	Weakness	Weakness
Infrastructure/environmental requirements	Mixed	Weakness	Weakness	Weakness	Weakness
Lack of e-voting standards	Weakness	Weakness	Weakness	Weakness	Weakness
Meaningful recount	Weakness	Weakness	Strength	Strength	Strength
Vendor-dependence	Weakness	Weakness	Weakness	Weakness	Weakness
Increased IT security requirements	Weakness	Weakness	Weakness	Weakness	Weakness

Annex B

The costs of e-voting: some examples

Below are some examples of the cost of e-voting systems. Note that the figures are calculated very differently between countries. Additionally, technology choice and context (number of voters, number of elections) have an enormous impact on the cost per voter. Note also that these are the capital costs of introduction; the costs of maintenance and depreciation need to be considered additionally.

Austria (Internet voting, student council elections)

3.8 euros (EUR)/registrant (403 EUR/voter)

870,000 EUR for 230,000 registrants, 2161 voters[5]

Brazil (voting machine)

3–5 US dollars (USD)/voter

1 billion USD initial costs plus 500 million USD per election for 100 million voters.[6] Over time, costs decreased to 3 USD/voter.[7]

Estonia (Internet voting)

1–5 EUR/voter or 0.1-0.5 EUR/registrant

500,000 EUR for establishing the system (without need for a voter authentication system); running costs around 100,000 EUR for 100,000 voters or 1 million registrants.

India (voting machine)

0.6 USD/voter

Around 300 USD/machine for up to 3800 voters; around 1.4 million machines were purchased for 700 million voters.[8]

Ireland (voting machine)

21 EUR/voter

53 million EUR spent for a system for 2.5 million voters (21 EUR/voter) plus 800,000 EUR annual storage costs.[9]

---

5 See <http://www.parlament.gv.at/PAKT/VHG/XXIV/AB/AB_02562/fnameorig_166607.html>.

6 See <http://www.observatorioelectoral.org/biblioteca/?bookID=26&page=8>.

7 Information provided by the Brazilian Superior Elections Tribunal.

8 See <http://eci.nic.in/eci_main/faq/evm.asp>.

9 See <http://evoting.cs.may.ie/Documents/CostofElectronicvotingAsOfMay.pdf>.

Philippines (voting machine)

3 USD/voter

120 million EUR for 50 million voters (2010).[10]

Switzerland (Internet voting)

0.3 EUR/voter (assuming three elections per year)

Estimation: 10 million EUR in 10 years for 1 million voters.[11]

United States (voting machines)

3 USD/voter, example Maryland[12]

Venezuela (voting machine)

4 USD/voter

120 million USD for three elections and 10 million voters.

---

[10] See <http://www.comelec.gov.ph/modernization/2010_natl_local/SBAC/winning_bidder/notice_of_award.html>.

[11] See <http://www.e-voting.cc/static/evoting/files/Swiss_Experiences.pdf>.

[12] See <http://www.saveourvotes.org/legislation/packet/08-costs-mdvotingsystem.pdf>.

References

and Further Reading

Recommendations and guidelines

Caarls, Susanne, 'E-voting Handbook: Key Steps for Introducing E-voting', Council of Europe, 2010, available at <http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Biennial_Nov_meeting/ID10322%20GBR%206948%20Evoting%20handbook%20A5%20HD.pdf>

Council of Europe, 'Certification of E-Voting Systems', 2011, available at <http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf>

Council of Europe, 'Guidelines on Transparency of E-enabled Elections', 2011, available at <http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf>

Council of Europe, 'Legal, Operational and Technical Standards for E-Voting', 2004, available at <http://www.coe.int/t/dgap/democracy/activities/key-texts/recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf>

Goldsmith, Ben, 'Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies', International Foundation for Electoral Systems, 2011, available at <http://www.ifes.org/Content/Publications/Books/2011/~/media/Files/Publications/Books/2011/Electronic_Voting_and_Counting_Tech_Goldsmith.pdf>

Norden, Lawrence D. and Lazarus, Eric, 'The Machinery of Democracy: Protecting Elections in an Electronic World', Brennan Center for Justice, 2007, available at <http://www.brennancenter.org/content/resource/the_machinery_of_democracy_protecting_elections_in_an_electronic_world/>

Norwegian Ministry of Local Government and Regional Development, 'Electronic Voting: Challenges and Opportunities', 2006

US Election Assistance Commission, 'Voluntary Voting System Guidelines', 2005, available at <http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx>

Observing electronic voting

Carter Center, 'Developing a Methodology for Observing Electronic Voting', 2007, available at <http://www.cartercenter.org/documents/elec_voting_oct11_07.pdf>

Organization of American States, 'Observing the Use of Electoral Technologies', 2010, available at <http://www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf>

Organization for Security and Co-operation in Europe, Office for Democratic Institutions and Human Rights, 'In Preparation of Guidelines for the Observation of Electronic Voting', October 2008, available at <http://www.osce.org/odihr/elections/34725>

Pran, Vladimir and Merloe, Patrick, 'Monitoring Electronic Technologies in Electoral Processes', National Democratic Institute, 2007, available at <http://www.ndi.org/files/2267_elections_manuals_monitoringtech_0.pdf>

Vollan, Kåre, 'Observing Electronic Voting', Norwegian Centre for Human Rights, 2005, available at <http://www.jus.uio.no/smr/english/about/programmes/nordem/publications/nordem-report/2005/1505.pdf

Voting from Abroad: The International IDEA Handbook on External Voting (Stockholm: International IDEA, 2007), Chapter 9, 'Observation of External Voting', available at <http://www.idea.int/publications/voting_from_abroad/upload/chap9.pdf>

Trust and confidence

International IDEA, *Electoral Management Design: The International IDEA Handbook* (Stockholm: International IDEA, 2006), available at <http://www.idea.int/publications/emd >

McGaley, M. and Gibson, J.P., 'Electronic Voting: A Safety Critical System', National University of Ireland, Maynooth, 2003

Oostveen, A.-M. and van den Besselaar, P., 'Security as Belief: User's Perceptions on the Security of Electronic Voting Systems' , Royal Netherlands Academy of Arts and Sciences, available at <http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-8.pdf>

E-voting and turnout, voting from abroad

International IDEA, *Voting from Abroad: The International IDEA Handbook on External Voting* (Stockholm: International IDEA, 2007), Chapter 10, 'E-voting and External Voting', available at <http://www.idea.int/publications/voting_from_abroad/upload/chap10.pdf>

Trechsel, Alexander and Vassil, Kristjan, 'Internet Voting in Estonia: A Comparative Analysis of Four Elections since 2005', European University Institute, 2010, available at <http://www.vvk.ee/public/dok/Report_-_E-voting_in_Estonia_2005-2009.pdf>

Vassil, Kristjan and Weber, Till, 'A Bottleneck of E-Voting: Why Technology Fails to Boost Turnout', European University Institute, 2009

End-to-end auditable systems

Jones, Douglas W., 'Some Problems with End-to-End Voting', University of Iowa, 2009, available at <http://www.cs.uiowa.edu/~jones/voting/E2E2009.pdf>

Prêt à Voter, <http://www.pretavoter.com>

Scantegrity, <http://www.scantegrity.org>

Open source e-voting

Open Voting Consortium, <http://www.openvotingconsortium.org>

US Open Source Digital Voting Foundation, <http://www.osdv.org>

ICT procurement, replacement cycles, cost of ownership

'The Cost of E-Voting', *Wired Magazine* (2008), available at <http://www.wired.com/threatlevel/2008/04/the-cost-of-e-v>

Joint Taskforce on Electoral Assistance, 'Procurement Aspects of Introducing ICTs Solutions in Electoral Processes', 2010, available at <http://www.ec-undp-electoralassistance.org/images/operational%20paper.pdf>

Yard, Michael, 'Direct Democracy: Progress and Pitfalls of Election Technology', International Foundation for Electoral System, 2010, available at <http://www.ifes.org/Content/Publications/Books/2010/Direct-Democracy-Progress-and-Pitfalls-of-Election-Technology.aspx>

Abbreviations

DRE	direct recording electronic voting (systems)
EBP	electronic ballot printer
EMB	electoral management body
EUR	euro
ICT	information and communication technology
IDEA	International Institute for Democracy and Electoral Assistance
IT	information technology
OMR	optical mark recognition
PCOS	precinct count optical scanners
TCO	total cost of ownership
USD	US dollar
VM	voting machine
VVPAT	voter-verified paper audit trail
VVSG	Voluntary Voting System Guidelines

Acknowledgements

Special acknowledgement goes to the lead author, Peter Wolf, and the two supporting authors of this paper, Rushdi Nackerdien and Domenico Tuccinardi. Additionally a number of individuals and organizations have provided invaluable feedback, corrections and additions to a first draft of this paper: Fabio Bargiacchi, Jordi Barrat i Esteve, Ingo Boltz, Susanne Caarls, Andrew Ellis, Manuel Kripp, Niall McCann, Betilde Muñoz-Pogossian and technical experts of the Organization of American States as well as the Brazilian Superior Elections Tribunal.

Thanks are also due to Eve Johansson for her professional input in editing this policy paper and to Lisa Hagman, International IDEA's Publications Officer, for ensuring the smooth production on behalf of the Communications Team.

INTERNATIONAL IDEA
International Institute for Democracy and Electoral Assistance
SE -103 34 Stockholm
Sweden
Tel +46 8 698 37 00
Fax +46 8 20 24 22
E-mail info@idea.int

ISBN 978-91-86565-21-3