A Strategic Assessment of the Impacts of ICT on Electoral Technology

BY

Young J. LUKE, *Ph.D*
Department of Business Management
Faculty of Business Administration
University of Birmingham
United Kingdom

ABSTRACT

In a fully electronic electoral management system, the entire electoral process— voter, party and candidate registration; verification of candidate support signatures; ballot production; electoral logistics; voter identification; voting in polling stations or remotely; vote counting; results transmission; and presentation of preliminary and final results of data—can all be performed by electronic and digital equipment and with very limited human intervention. This can only be achieved through ICT. Key benefits of electoral technology include accuracy, speed, efficiency and effectiveness. Specialized election technology vendors offer an ever increasing range of services to EMBs, but also require EMBs to be aware of the challenges involved in dealing with these companies. Voter education, public information and EMB staff expertise are important success factors for election technology implementations. With the introduction of electronic voting, countries such as Nigeria recognizes the need for technical expertise at the commission level and put more emphasis on ICT skills when carrying out election.

KEYWORDS: **ICT, electoral technology, election technology vendors, voter education**

Introduction

In considering elections technology in recent decades, electoral administrators have adopted several types of technology into the electoral process. While these technologies can bring great benefits in accuracy, speed, efficiency and effectiveness to the process, they also pose challenges in the fields of security, costs, sustainability, transparency, and vendor dependence.

According to Binder, (2008), in a fully electronic electoral management system, the entire electoral process— voter, party and candidate registration; verification of candidate support signatures; ballot production; electoral logistics; voter identification; voting in polling stations or remotely; vote counting; results transmission; and presentation of preliminary and final results of data—can all be performed by electronic and digital equipment and with very limited human intervention. Currently, only a few countries, such as Norway, have achieved this level of automation of election administration. EMBs usually combine manual processes and electronic technology into a suitable hybrid system, which is influenced by a wide range of factors, and may arguably be considered unique in any given country.

As stated by Donno, (2006), when ICT is used in crucial steps of the electoral process, there is a growing expectation that the EMB's IT expertise is not limited to its technical departments. Election commissioners, spokespersons and other high-ranking EMB staff are increasingly expected to understand and explain technical details of the electoral process with just as much confidence as any other operational or legal aspects. With the introduction of electronic voting, countries such as the Philippines recognize the need for technical expertise at the commission level and put more emphasis on ICT skills when selecting commissioners.

Concept of Electoral Technology

Initially, electoral technology was often entirely custom built for each EMB, based on general-purpose ICT systems. In such systems, any specific electoral functionality had to be built from scratch. In recent years, however, election technology vendors have increased their range of products and provide ready-made solutions that only require relatively minor adjustments to local requirements and conditions, (Eisenstadt, 2002).

Types and Main Features of Elections Technology

EMBs can use electoral technology in virtually all aspects of managing the electoral process:

Voter registration systems for building and maintaining a voter register with personal details of all eligible voters in electronic format, in some cases also biometric information such as photographs or finger print scans. Voter registration data in electronic format can be used in many ways (e.g. data cross-checks, duplicate detection, issuing voter identification documents, targeting voter information, planning and electoral logistics, producing voter lists for polling stations and obtaining demographic information about the electorate), (Pierson, 2011).

Voter identification systems (electronic poll books) for checking the eligibility of each voter at the polling station level by comparing his or her personal details to a database of all eligible voters.

Party and candidate registration systems, for tracking the registration status of all political subjects for an election, checking any required support signatures and providing the data in appropriate formats for designing ballot papers and tally sheets, configuring voting machines, etc.

Observer registration and accreditation systems, for tracking the accreditation process for citizen and international observers and issuing their identification documents.

Districting and boundary delimitation systems, using geographical information systems to delimit political boundaries and distribute polling stations and catchment areas.

Electronic voting and vote-counting systems, various systems ranging from machine counting of paper ballots to voting machines used in polling stations and Internet voting systems; these speed up the counting process and eliminates human interference.

Result tabulation and transmission systems, for processing electronically captured turnout and results data, greatly speeding up related procedures and avoiding and detecting human error through automation and data cross-checks.

Results publishing systems, for presenting and visualizing election results in various formats including maps, charts, detailed results databases and overviews.

Voter information systems to provide voters and other electoral stakeholders with detailed data about electoral process. Such systems include polling station locators allowing voters to easily find their polling station, legal databases of regulations, information about parties and candidates running for election, databases allowing access to detailed election results and statistics, and continuously updated calendars with key events and deadlines.

E-learning systems, for the professional development of EMB staff.

All of these electoral information and communications technology (ICT) solutions employ a wide range of technology, from simple mobile phones to private satellite links, from standard productivity and collaboration systems to specialized biometric databases, and from private intranet systems to public websites and social media channels.

Selected ICT Concepts with Impact on Elections Technology

ICT Innovation Cycles and their Relation to the Electoral Cycle

According to Renwick, (2010), ICT systems evolve very quickly compared to the duration of an electoral cycle. Most ICT equipment, both hardware and software, has a useful life of about 3–5 years. After this period, equipment needs to be either replaced or significantly refurbished and upgraded. For electoral ICT applications, this can pose a significant challenge. With many electoral cycles lasting about four years, an ICT system that was successfully deployed for one election can be expected to require major upgrades or even a complete replacement for the next election.

Where the time between elections and use approaches the end of the useful life of ICT equipment, the sustainability and efficiency of purchasing, owning, storing and maintaining equipment needs to be considered. To avoid the high costs of storing unused equipment, EMBs can lease selected equipment, share it with other countries, or plan to reuse, sell or donate some of it after an election for non-electoral use, (Andrews, Boyne, & Enticott, (2006).

The 'Bathtub Curve' and Electoral Cycles

Another challenge related to long electoral cycles and the comparatively short useful life of ICT systems becomes evident when considering the bathtub curve, a concept that is widely used in engineering to describe the occurrence of failures in technical systems.

The curve starts with a 'burn-in' phase in the early stages of using a system. This phase is characterized by the high failure rate of a still-immature system. As problems are detected and addressed, the failure rate decreases and the system enters the period of its useful life with a very low failure rate. Finally, as the useful life of a system comes to an end, wear and tear lead to an increased failure rate and require the eventual upgrade or replacement of the system, (Andrews, Boyne, & Walker, 2006). While most non-election systems will be used primarily during the second phase of this curve, the sporadic nature of elections implies that electoral technology will often be used only shortly after its development and may therefore still be in the failure-prone burn-in phase. The period of useful life of election technology therefore coincides mostly with the time between elections when the system is not used. And when the next election occurs, after several years, the system may already be close to or in its wear-out phase with increasing failure rates.

The bathtub curve demonstrates that long preparation times are required for the introduction of electoral technology to make sure the burn-in phase takes place before election day, and that the time between elections must be used to identify and implement all upgrades required for the next election period.

Total Cost of Ownership of ICT Systems

One of the main claims offered in support of elections technology is cost effectiveness. However, experience suggests that the initial capital investment required to purchase an ICT system can be as low as 25 per cent of its total cost of ownership (TCO) over its expected lifetime. The TCO is the sum of all direct and indirect costs involved in purchasing, operating and eventually disposing of the equipment. It can be easy to underestimate the TCO when only looking at the initial purchase price of ICT equipment.

As stated by Ansolabehere, & Stewart, (2005), the TCO of electoral ICT systems includes the costs of:

- public dialogue about the introduction of the new system;
- purchasing or developing system hardware and software licenses;
- system certifications and auditing;
- securing the system physically and technically;
- preparing the infrastructure required to operate the system;
- Deploying, configuring and testing the system for an election;
- training staff and operators to use the system;
- operating the equipment during the election;
- retrieving the equipment after the election;
- storing and protecting the systems between elections;
- disaster recovery: preparing for back-up planning;
- replacements or upgrades, possibly for every election; and
- Disposal of outdated equipment.

Many of the costs above are difficult to quantify, which makes it difficult to establish the precise costs of using an ICT solution, to compare ICT costs between different solutions, or even to estimate any cost savings incurred by automating parts of the electoral process. While a realistic estimation of the TCO and securing the required resources is necessary to effectively control and manage the use of electoral technology, claims about savings through introducing new technologies or between different types of technologies should always be carefully examined, (Atkeson, & Saunders, 2007).

ICT Security and Costs

ICT security works like preventive medicine: one does not know if it is working or how well it is working until it fails. Moreover, there is no perfect security. Securing electronic systems is an arms race between those trying to protect them and those prepared to invest in breaking into them. Electoral stakeholders often demand the highest possible security standards for election technology, since a country's democracy is at stake when election technology seriously fails or is manipulated. But the highest security levels are expensive. Each EMB must determine, in consultation with all electoral stakeholders, how at risk its ICT systems are; how likely failure or various types of attacks are; what the consequences of such events are; and how much security investment is needed, possible and justifiable.

Internet-based systems raise additional security concerns since they are connected to a public network and thus exposed to an unknown threat environment with similarly unknown threat capabilities. This environment includes not only national actors but also, by virtue of the online environment, foreign governments and hackers.

Election Technology Vendors

In recent years, election technology vendors have started to provide more and more services to EMBs around the world. By deploying their solutions in more contexts and elections than a single EMB would usually be responsible for, vendors have developed a great amount of technical, operational and sales experience. EMBs are often confronted with many offers by vendors to evaluate and eventually purchase new types of election technology. The products and services on offer can be of great help in organizing an election, but there are also several challenges related to this increased vendor involvement in elections.

Needs-driven Approach

While vendors have an interest in the smooth conduct of elections they are involved in, their primary objective is naturally to expand their business rather than to improve the electoral process. Vendors will therefore shape their proposals in order to maximize the use of their products rather than look at the electoral outcome of using their technology. The EMB's role in selecting electoral technology needs to be the opposite: its primary objective must be improving the electoral process, which may or may not be facilitated by the different technological options available.

Therefore an EMB's starting point for evaluating technology should not be which technology to choose or how to implement it. An EMB should first and foremost define which electoral problem needs to be addressed and which are the best ways to do so, (Bhasin, & Gandhi, 2012).

Procurement

Elections are unique in each country, and elections technology needs to provide unique solutions for the country in question. Electoral procurement is expected to be conducted with a high degree of integrity, transparency and competitiveness. Yet with high-value contracts at stake, lengthy appeals procedures need to be included in the envisaged timeframe. Technology procurement is a complex process, and tends to take longer than initially expected. With a set election date, this can come at the expense of implementing the chosen solution. Therefore, tender exercises need to be initiated well in advance of the election in which the technology will be used.

The procurement process needs to carefully determine the appropriate systems to purchase. While a full specification would ideally be developed without vendor participation, an EMB may not be able to fully specify all needs and be aware of all technical options and possibilities. In such cases, a competitive dialogue can be considered as part of the procurement process: after several suitable vendors have been identified, the EMB can conduct a structured dialogue with all of them to identify feasible alternative solutions for the EMB's requirements.

Vendor Lock

Where technology is proprietary to a vendor, where data formats are not open or when an EMB relies heavily on a vendor for its electoral operations, it risks being locked into a particular vendor. In other cases, electoral stakeholders may have strong preferences for a well-established and trusted vendor and may not want the EMB to engage any alternatives. Any such tie to one particular vendor should be avoided to make sure the EMB remains in control of the systems it uses and the costs incurred.

When the transparency of an electoral ICT application is important to stakeholders, they frequently request open source software be used, which has source code that is accessible to all and comes with a software license that allows free usage and distribution. Access to source code is one requirement for experts to understand exactly how an ICT system works. In addition to the added level of transparency, open source software is also considered to be cheap and secure, and it limits vendor lock. At the same time, vendors tend to build their business models on proprietary software with closed source codes, mainly to protect their intellectual property and sometimes to limit access to security issues to a small internal audience.

According to James, (2011), Proponents of open source electoral management software argue that elections technology is 'mission critical' for democracy and should therefore be completely transparent and owned by the public. Initiatives such as the Open Source Digital Voting Foundation (OSDV) work on the development of fully open source electoral systems. However, open source initiatives for electoral management systems currently find it difficult to gain momentum and are increasingly confronted with a market that is already served by experienced vendors and their proprietary systems.

Vendors are increasingly recognizing the high demand for transparency by many electoral stakeholders. Norway made open source software a requirement for its Internet voting system and the selected vendor's source code was published online. While vendors may not always be ready to switch to open source and free use of their software, they are usually willing to disclose their source code for public scrutiny. Such disclosure can either be limited to certain time frames, controlled environments or selected experts, or it can be complete and public. Increased transparency and access to proprietary codes often come with significant additional costs; depending on the application in question, an acceptable trade-off may need to be made.

Commercial Off-the-shelf Systems vs. Customized System Development

A fundamental decision for electoral administrators is whether to obtain ready-made ICT solutions or pursue the development of a custom-built system. A ready-made system can usually only be adapted to a certain extent, and may therefore require changes in the electoral process to match the system. Such changes are in some cases beneficial and reflect best practices for using electoral technology; in other cases they are required for the sole purpose of making the selected technology work in the given context. By contrast, a custom-built system may more closely fit the existing electoral process. However, customized development is a lengthy and expensive process, and poses extra challenges in managing the development process.

Voter Education and Public Information

Voters and other electoral stakeholders are exposed to various electoral technologies in very different ways. Accordingly, the need for voter education and public information campaigns varies greatly. Overall, it is important to include all prospective users in the introduction of new technologies in order to increase acceptance and the likelihood of successful implementation.

Some new technologies, such as polling station locators and other voter information systems, are mostly a convenient additional service at the voters' disposal. Public outreach for such systems only focuses on the widest possible awareness and usage of such systems.

In other cases, voters will be required to comply with certain procedures or use the technology themselves and need to know what to do. In addition to disseminating the information through its regular communication channels, the EMB can also set up demonstrations in public locations where voters can try the technology, for example cast an electronic test vote or check their registration status on an electronic poll book before the election takes place.

Any technology that plays a central role in the electoral process will be of interest to stakeholders such as political parties, the media or election observers. For them, the EMB needs to provide appropriate detailed documentation and make competent EMB staff available for enquiries.

In cases where technology is potentially disputed, for example when it seems very costly or is not welcome by all stakeholders, information campaigns need to go one step further. The EMB then needs to inform or remind stakeholders why the technology was chosen, which trade-offs and options were considered, and how expected improvements to the electoral process outweigh the potential downsides. Such an information campaign will not only be conducted around the election itself, but begin in the early stages of considering and selecting a technology, when relevant stakeholders should be given an opportunity to have their say.

Training and Expertise

As stated by Mahoney & Thelan, (2010), Most EMBs have ICT departments that are tasked with operating at least the standard ICT solutions used by the institution. Larger ICT departments can play a leading role in the development, introduction and maintenance of specific elections technology. However, with more complex electoral solutions, private companies provide an increasing share of the development and operational work and related expertise. Therefore it is important to delineate the areas of responsibility between the EMB and the vendor, and ensure that knowledge and skill transfers to EMB staff takes place. Capacity building should be part of the vendors' deliverables.

With electoral technology being introduced down to the polling station level, EMBs' need for ICT capacity goes far beyond the ICT department. All levels of permanent and temporary election staff increasingly use technology in all aspects of their work. Efficient training for using elections technology requires at least basic computer literacy. ICT training from scratch is costly and time consuming, and the availability of a pool of computer-literate election workers is a key success and cost factor in the deployment of elections technology.

Administrative and Operational Objectives

Maintaining EMB Oversight

As EMBs are rarely able to develop all of the required elections technology themselves, most will need to rely on vendors to some extent. Where much of the electoral process is outsourced, the roles and responsibilities of the EMB and vendors need to be clearly delineated to ensure that the EMB has full oversight of the process. A reasonable option is that the vendor's role is to develop and maintain electoral ICT systems, while the EMB's role is to configure the system and operate it during the election.

Accountability and Integrity

The lack of any tangible evidence of transactions in computer systems and the incomprehensibility of computer programming to the bulk of the population lead to a lack of transparency. This lack of transparency—combined with the risks of interference with data and widely publicized media reports of computer viruses, hackers and system malfunctions; and an increasing awareness of online surveillance—can affect EMBs' credibility. When relying on computer systems for vital tasks such as voter registration, voting and vote counting, EMBs are expected to be openly accountable for their use of technology.

Measures that EMBs can take to ensure the integrity of their computer-based systems include:

- rigorous pre-implementation testing of computer systems and public release of the results of the tests;
- robust ICT policies that cover all aspects of technology use, including acceptable access to and use of ICT equipment and data, physical security of ICT equipment, data security, back-up, retention, archiving and disposal, appropriate of use email and social media, and disciplinary measures for cases of deliberate or serious breaches;
- regular auditing of computer systems, with particular attention paid to their security features;
- making test versions of source codes for computer systems available for public comment (for example, the Electoral Commission of the Australian Capital Territory posted proposed code for its computer-based vote recording and counting system on its website and invited comments from computer professionals);
- independent, third-party certification of computer systems based on national and international standards, guidelines, recommendations and requirements to confirm that the system complies with prescribed technical requirements and standards; and
- Holding an authenticated copy of the authorized codes in an independently controlled off-site location, as has been recommended in the USA. Regular comparison of this with the code being used in the EMB can detect and remove any unauthorized changes.

Focus on the Whole Electoral Process

When new technology is used for the first time, when a significant part of the election preparations and budget is invested in technology, and when there are great expectations of the impact of technology, ICT aspects of elections tend to attract a lot of EMB and public interest. In this situation, it is important that this attention does not come at the price of neglecting other, equally important, components of the electoral process.

Inclusiveness

Technology tends to benefit the more affluent and educated citizens more than other, disadvantaged parts of society. Therefore the introduction of new technology needs to be accompanied by measures that ensure equal access for the entire electorate, including voters with special needs, voters in rural areas with less access to infrastructure, elderly voters and those who feel less confident using technology.

Sustainability of Donor-funded Technology

With high costs and short usage spans, elections technology is difficult to sustain—particularly in post-conflict settings and emerging democracies, where a challenging environment, limited and unreliable infrastructure, and possibly low trust in a newly established EMB require even more complex ICT solutions. Unfortunately, this is precisely the context in which donors may be willing to invest heavily in technology, hoping to facilitate the smooth conduct of the election. Such an investment risks delivering one welladministered election, but creating sustainability problems in the long run. With only the next election in focus, little consideration is given to maintaining the system and related expertise for future elections, especially when donor funding is no longer available. Systems, services and expertise that can be efficiently procured by an assistance provider through their procurement channels and networks may be difficult and expensive to obtain following national procurement regulations on the local market.

Selecting Appropriate Technology

The most advanced, high-tech solutions are not necessarily the most suitable technologies for use in the electoral process. Appropriate technology is designed with consideration of its economic, social and environmental impact as well as its effect on the entire electoral process. Simpler systems that still fulfil all requirements are usually more appropriate, require fewer resources and maintenance, and have a lower TCO.

Issues of Electronic Voter Registration

According to Norris, (2014), the use of ICT in voter registration can become controversial for several reasons. The accuracy of voter registers is often a contentious issue, and technology upgrades may be seen as a solution to that. However, voter registration is a large and costly exercise, and increased ICT use comes at a high cost. The sustainability of high-tech approaches can be questionable, especially when substantial donor funding is required or when registration mainly focuses on establishing a single register for an upcoming election rather than a permanent system for continuously maintaining a register.

The operational complexity and cost of voter registration primarily depends on how voter registers are built and maintained. If an EMB can share data with other administrative bodies and build a voter register based on existing population registers (e.g. national identification card systems, civil registry data), this will require significantly less technical effort than if it has to compile the voter data itself. For use in elections, population registers must be maintained by a widely trusted institution, use high-quality data, have a high registration rate (with many incentives and few disincentives for registering) and contain all information about eligible citizens required for the electoral process. If these conditions are met, an inexpensive and highly accurate voter register can be extracted automatically from such a system.

If data sharing with other administrative bodies is not possible and the EMB needs to conduct voter registration on its own, costs will be significantly higher, as the EMB must operate a system that can reach all citizens and capture or update the personal details of all eligible voters. The simplest solution in such a case is to only conduct a paper-based registration exercise. However, paper-only voter registration data may often be insufficient: the data quality may be poor, data cross-checks and efficient updates of the register are not possible, and it is difficult or impossible to establish or publish accumulated registers for larger regions or an entire country. Any claims about inaccuracies of the register will be hard to verify.

One step up the technology ladder, and usually the cheapest way to capture registration data electronically, is the use of machine-readable paper registration forms. Data can be collected by manually filling in optical mark recognition (OMR) forms, from which registration data can later be scanned into an electronic database. The disadvantages of such a system include a lack of data integrity checks when the data is captured, a lack of feedback about any problems at the point of registration, the difficulty of correcting or completing any wrong or missing data discovered during the scanning process, as well as mistakes due to incorrectly filled in forms.

Further technical upgrades include the use of electronic registration systems at the point of registration. In their simplest form, electronic registration systems are offline and only capture registrants' personal details. Such a system may be sufficient if voters' details can be confirmed by widespread availability of reliable personal identification documents. In such a case, local duplicate checks and data validation must be possible. Data back-up plans at the point of registration need to be extensive, as any lost data cannot be restored.

Online registration systems require data connections to all registration points. They have the potential to immediately check a registrant's data against the entire voter register, and to detect and resolve duplicate registrations. Such systems can upload data directly to central registration databases and reduce the risk of data loss at the point of registration.

The most comprehensive registration data collection will include capturing registrants' biometric details such as fingerprints and facial or iris recognition data. The costs of such a system will increase due to the need for biometric data-capturing equipment for every registration system as well as more comprehensive data-processing requirements for storing and comparing biometric data. The additional cost of setting up biometric systems is usually justified by the difficulty of establishing registrants' identity due to a lack of reliable identification documents.

A Brief Background of Electronic Voting and Vote-counting Systems

Introducing new ICT systems in elections is always challenging, and requires careful deliberation and planning. Electronic voting (e-voting) is arguably the most difficult upgrade, as this technology involves the core of the entire electoral process: the casting and counting of votes. E-voting greatly reduces direct human control and influence in this process, and provides an opportunity to solve some old electoral problems, but it also introduces a whole range of new concerns. Therefore e-voting can be expected to trigger more criticism and opposition than any other ICT application in elections.

There are a number of e-voting and vote-counting systems that are marketed as a means of improving voting methods and reducing costs. Some of the systems claim to offer a high degree of reliability and resistance to electoral malpractice.

- Direct recording electronic (DRE) voting machines 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 are based on scanners that can recognize the voters' choice on special machine-readable ballot papers. OMR systems can be either central count optical scanning (CCOS) systems (ballot papers are scanned and counted in special counting centres) or precinct count optical scanning (PCOS) systems (ballots are scanned and counted in the polling station directly as voters feed them into the voting machine).
- Electronic ballot printers (EBPs) are similar to a DRE machine, and produce a machine-readable paper or electronic token containing the voter's choice. This token is fed into a separate ballot scanner, which conducts the automatic vote count.
- Internet voting systems transfer votes 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.

The accuracy and integrity of these machines depend not only on the companies and persons that design, programme, test and maintain them, but also on the systematic checks and balances introduced by the EMB, including system audits and certifications.

Comprehensive controls and accountability measures come at a price. More transparent and secure systems cost more. A system with the highest possible levels of transparency and security can increase costs so much that the benefits of the e-voting solution no longer justify the expenditure.

System Requirements, Certification and Audits

More than for any other electoral technology system, certifications and audits are of crucial importance for building trustworthy and credible e-voting and counting systems. Certifications and audits confirm the compliance of the e-voting system against a clearly defined set of functional and operational requirements. The exact requirements are different in each context, and need to take into account legal, technical, operational and functional aspects as well as key stakeholder needs.

System certifications provide EMB- and vendor-independent, third-party confirmation that an e-voting and counting system meets the requirements. System audits verify the proper functioning of the e-voting and counting systems through stringent testing before, during and after usage. However, thorough certification and audit can come at a significant additional cost, and can for smaller implementations come close to the technology costs of the system.

Voter Verified Paper Audit Trails

According to (Bhasin & Gandhi (2012), one response to concerns about the integrity, reliability and security of e-voting systems and the need to conduct transparent audits has been the use of a voter-verified paper audit trail (VVPAT) process. The voter is provided with a printout of the vote just cast, which can be checked on the spot and then placed in a ballot box, to be used if necessary to audit the validity of figures produced by the automated system. Many e-voting systems can provide audit trail facilities, including electronic voting machines (EVMs) that have been used in countries such as Belgium, the United States and Venezuela in recent years. In 2013 the Indian Supreme Court directed the Election Commission to introduce paper trails for voting machines, and the EMB has taken steps to introduce VVPAT after more than 20 years of using e-voting machines that did not provide such a facility.

The use of OMR devices to count votes, such as in the Philippines, can also provide accuracy and time effectiveness in the electoral process while producing a paper ballot that can be physically examined if necessary in post-election disputes. VVPATs only work for e-voting in the controlled environment of a polling station (not, for example, with Internet voting). The Venice Commission has undertaken a detailed analysis of the compatibility of remote voting and e-voting with the broader electoral standards of the Council of Europe. Beyond technical performance issues, some of the debate regarding the integrity of elections technology entails the propriety of politically aligned or foreign-influenced suppliers. Media reports of alleged integrity problems with mechanical and e-voting machines has increased pressure on EMBs to be open and accountable in their sourcing and use of technology.

Costs

Although there is no reliable cost-effectiveness analysis on the use of new technology for voting and counting, the evidence that technology such as EVMs may reduce election costs over time, especially costs associated with printing and storing ballot papers and vote counting, is controversial. India has used relatively cheap EVMs for decades and has concluded that EVM-based elections are much cheaper than paper-based ones. Yet the Netherlands abandoned old EVMs in 2007 and subsequently investigated the introduction of a modernized system. Their findings as of 2013 were that voting with new EVMs would be twice as expensive as paper-based voting, (Mahoney & Thelan, 2010).

Conclusion

1. Key challenges remain in the area of security, costs, sustainability, transparency, and vendor dependence. Trends are away from custom built systems for each EMB toward specialized vendors' ready-made solutions.
2. As a consequence of short ICT life cycles, most equipment needs major upgrades or complete replacement between elections.
3. ICT equipment that was only put in place shortly before an election is likely still immature and has higher failure rates.
4. The initial purchase price of ICT systems can be expected to be only a fraction of the total cost of ownership over the equipment's lifetime.
5. Specialized election technology vendors offer an ever increasing range of services to EMBs, but also require EMBs to be aware of the challenges involved in dealing with these companies.

Recommendations

1. Voter education, public information and EMB staff expertise are important success factors for election technology implementations.
2. EMBs are expected to be accountable for the use of elections technology and need the ability to maintain ultimate oversight of the systems in place.
3. Highest ICT security levels are expensive; each EMB must determine how much security investment is needed, possible and justifiable.

REFERENCES

Andrews, R., Boyne, G.A., & Enticott, G. (2006). 'Performance failure in the public sector'. *Public Management Review,* 8(2), 273-296.

Andrews, R., Boyne, G. A., & Walker, R. M. (2006). *Subjective and objective measures of organizational performance: An empirical exploration*. In G. A. Boyne, K. J. Meler, L. O'Toole Jr. & R. M. Walker (Eds.), Public Service Performance (pp.14-34). Cambridge, Cambridge University Press.

Atkeson, L. R., & Saunders, K. L. (2007). 'The Effect of Election Administration on Voter Confidence: A Local Matter?' *PS: Political Science & Politics,* 40(04), 655-660.

Bhasin, T., & Gandhi, J. (2012). 'The motivation, timing and targeting of state repression'.

Binder, C. (2008). *International Election Observation and Democracy*. In E. Harald, K. Lachmayer, G. Ribarov, & G. Thallinger (Eds.), Perspectives and Limits of Democracy (pp. 71–90). Wien: Nomos/wuv.

Donno, D. (2006). *The International and Domestic Politics of Election Manipulation.* Paper presented at the annual meeting of the American Political Science Association. Retrieved Aug 31, 2006, from http://www.allacademic.com/meta/p151446_index.html.

Eisenstadt, T. A. (2002). Measuring electoral court failure in democratizing Mexico. *International Political Science Review*, 23 (6) 47–48.

James, T. S. (2011). "Fewer' costs, 'more votes? UK Innovations in Electoral Administration 2000-2007 and their effect on voter turnout". *Election Law Journal,* 10(1), 37-52.

Mahoney, J., & Thelan, K. (2010). A Theory of Gradual Institutional Change. In J. Mahoney & K. Thelan (Eds.), Explaining Institutional Change: Ambiguity, Agency and Power (pp.137). NewYork, *Cambridge University Press.*

Norris, P. (2014). (Forthcoming).*'Introduction: The concept of electoral integrity'*. Electoral Studies.

Pierson, P.(2011). Politics in time: History, institutions, and social analysis. *Princeton University Press.*

Renwick, A. (2010). The Politics of Electoral Reform: Changing the Rules of Democracy. Cambridge, *Cambridge University Press.*