The Case for Election Technology

Abstract

Information technology permeates almost every aspect of our lives. Finally, after years of resistance, election technology is slowly helping the world's democracies increase transparency, facilitate turnout and reduce the cost of running elections whilst increasing integrity and security. The current article analyses some of the longstanding arguments against the use of technology in the election process, and the responses made by experts, including the demonstrated benefits of well-designed election technology. An entire section on security is provided, as are references to some implementations around the world and to the Election Automation Maturity Model. The article also touches briefly on the tools of Internet and mobile voting.

Keywords

Citizen engagement; Elections; Turnout; Online Voting; Cybersecurity; E-democracy

Antonio Mugica*

Introduction

Information technology permeates almost every aspect of our lives. The reason is simple. When a system is well designed, it makes everything better: speed, reliability, security, efficiency, convenience and capabilities are all increased, most often by many orders of magnitude.

No one would dream of running a bank without the computers and software that are the central nervous system of any institution. Every time you fly in a plane you put your life in the 'hands' of a computer for most of the trip, albeit with some human supervision. If you happen

to be in hospital in critical condition, your life-support system is likely to be controlled by software run by a computer.

We twenty-first century humans trust computers with the most difficult, the most critical and the most important tasks of our personal lives. It therefore seems strange that technology is largely absent from important areas of government, which is not taking advantage of the significant benefits that we are now used to everywhere else. One area where developments in technology have been especially slow is in the process of enabling democracy. Enormous opportunities in this area remain unrealised: citizen engagement, real-time participation, communication between government and constituents, and elections.

This article discusses government elections from start to finish. It focuses on polling station voting. All around the world, from the most developed countries to the most challenged ones, running a successful, clean election is the first step towards true democracy. The process of assuring the eligibility and enfranchisement of voters, the voting itself, counting the votes, producing election returns, canvassing and tallying is still mostly done manually in a majority of countries. In each one of these stages, the 2,000-year-old system is unreliable at best and corrupt at worst. This leaves room for all kinds of problems. In many cases these problems are swept under the rug, but they pervert the ideal of democracy, that in elections it is only the will of the people that prevails.

Many people perceive the election process to be straightforward and take for granted that it works. For this reason, very little attention is given to election administration. But as one of the founders of Smartmatic, the largest voting technology company in the world, I can say that the election process is much more complex than most people realise. I am deeply concerned about the election process and consider the convergence of technology and politics a matter of great importance. I invite the reader to join me as I discuss this topic that is so fundamental to our democratic systems.

Election technology: the case for and against

After 11 years conducting thousands of elections on every continent, and working side by side with countless election professionals and volunteers, Smartmatic election specialists have discovered common themes in the challenges faced by those with the difficult jobs of organising, running and managing elections.

Current opposition to the use of election technology is predominantly defended along two lines. The first is that an election is so straightforward that it does not need technology. How difficult can it be to count papers and declare a winner? The second is the inverse of the first (and thus an obvious contradiction): an election is such a complex and difficult process that no computer system is secure enough or robust enough to handle it.

Both arguments are flawed. Running a mid-sized election (say, in a country with 20 million voters) is not simple for a host of reasons. It is mission critical for the country, it is dispersed over a large territory, it can have thousands of candidates in hundreds of jurisdictions, it requires that millions of election instruments be under strict security while they move around the country's territory, and it requires the disciplined performance of hundreds of thousands of poll workers and subcontractors on a very tight schedule. Precisely because elections are so complex and difficult to conduct, well-designed computer systems are essential to make them reliable and to guarantee that the process is tamper-proof and free of errors.

How can the benefits of running an automated election be summarised? There are nine areas in which automation results in significant improvements over traditional manual voting and counting systems.

Security

The security of a paper-based, manual vote with a manual count is extremely low. Single copies of each vote make them easy to tamper with or destroy. Also, from voting to counting to final tally, and at every step in between, human error and tampering, not only with the votes, is easy and very common. The most vulnerable type of election is that which uses no technology at any stage. Well-designed, special-purpose systems reduce the possibility of results tampering and eliminate fraud. Security is increased by 10–1,000 times, depending on the level of automation.

Accuracy

Computerised voting, counting, aggregating and tallying eliminate the introduction of errors (the result of the human factor) that to a greater or lesser extent always affect results in a manual election.

Speed

Official results (as opposed to preliminary ones based on quick counts or exit polls) can be obtained a few minutes after the polls close. A good example comes from the Republic of the Philippines, where before automation it took 6 weeks to produce official results, compared to less than 12 hours after the automated elections of 2010 (Alave et al. *2010*).

Privacy

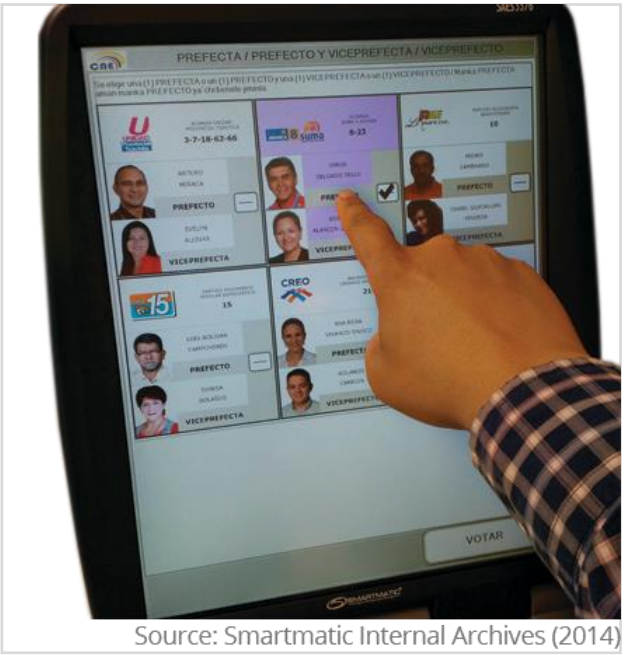
The sophistication of IT-based randomisation algorithms guarantees that votes are never stored in sequence. This, combined with the accessibility features (see point on accessibility), creates the most robust privacy settings available, making sure each citizen's vote is truly private and not susceptible to being influenced in any way.

Auditability

One of the biggest issues with manual voting is that it leaves a very weak audit trail, with very little or no redundancy of data. A well-designed automated election, by contrast, produces multiple copies of every data point both in electronic and paper-based forms, creating a very rich audit trail that cannot be circumvented. This gives parties, election officials, candidates, accredited observers and even citizens the capability to verify that the results truly reflect the will of the voters. This is one of the strongest arguments in favour of good automated elections.

Accessibility and turnout

The friendliness of the user interfaces—to which we are now accustomed via our phones and computers—can make voting more accessible. In automated elections, voters from all age groups consistently report that it is easier to vote electronically than with pen and paper. In addition, it has been widely demonstrated that it facilitates voting for those who are illiterate, because they can simply touch the face of their candidate or the colour of their party with a finger (Fig. 1). Voters with disabilities are lobbying governments for computer-based systems, because these systems allow them to vote and to do so unassisted, thanks to the use of audio voting and special controls that allow people with reduced motor skills to vote easily. So the technology would increase turnout of people with disabilities, strengthening inclusivity and the democratic process.



Source: Smartmatic Internal Archives (2014)

Fig. 1 **Automatic voting for illiterates.**

Integrity

Modifying, misplacing or spoiling a paper ballot or election return is a common occurrence in manual elections. With a well-designed automated election system, the possibility of this happening is reduced to zero. Multiple digital and paper copies of each element are created, which ensures that data is never lost, modified or destroyed.

Cost reduction

Even after taking into consideration the initial investment in technology, the cost per voter per election falls significantly. Smartmatic, the largest voting technology company in the world, has customers that have reduced the cost per voter per election by between 15 % and 50 % by automating their elections.

Sustainability

India used to cut down 280,000 trees and utilise huge amounts of energy and water to produce the paper ballots needed for each election. This cost to the environment was eliminated when elections were automated (Quraishi *2014*).

After observing how elections are run in more than 70 countries and interacting with election commissions around the world, researchers at Electoralmaturity.org, which is sponsored by Smartmatic, have developed the Election Automation Maturity Model. This model enables anyone to assess the benefits derived from varying levels of automation within an election.

Any country will advance from left to right and from the bottom up, as shown in Fig. 2, following the curve. However, an election commission sometimes takes many steps at the same time. Theoretically it is possible to complete all eight steps together, although no country has ever done this. Stage zero would be a purely manual election using no technology. Stage 1 is the minimum level of automation, where there is only automated monitoring of a manual election. The model proceeds all the way to Stage 8, where there is a combination of e-voting (using voting machines), I-voting (using the Internet), and the use of biometrics to authenticate voter eligibility and activate the voting session (Figs. 2, 3).

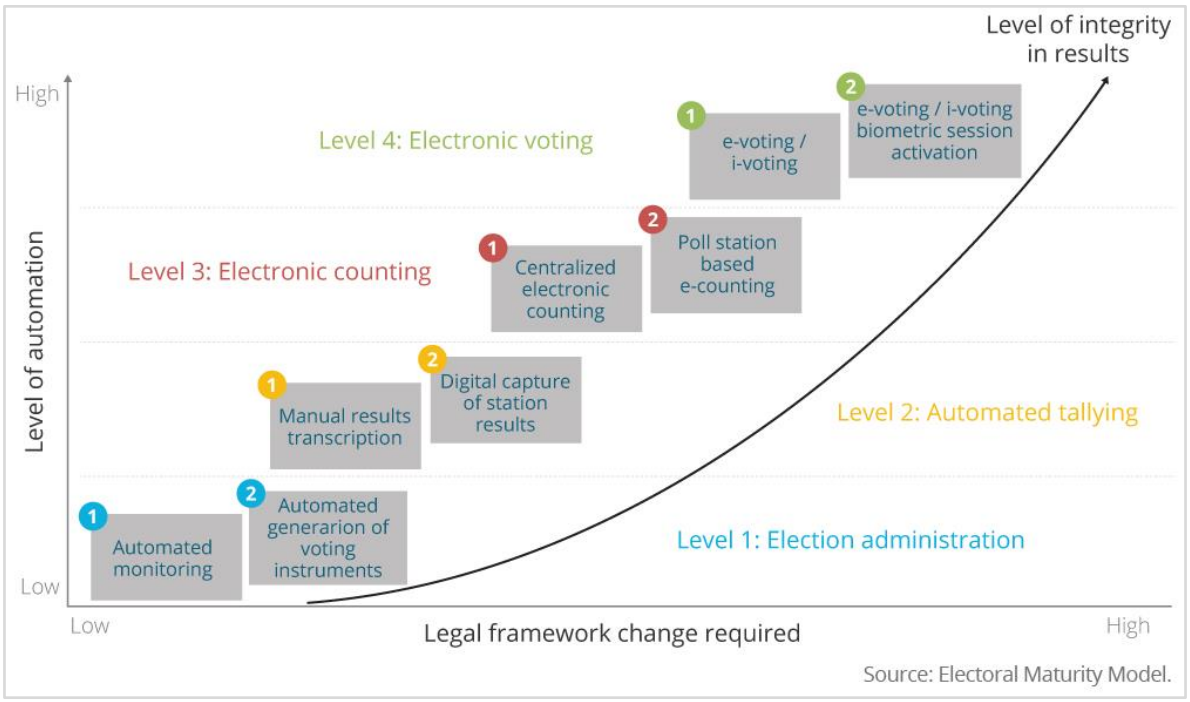


Fig. 2 **Election Automation Maturity Model**.

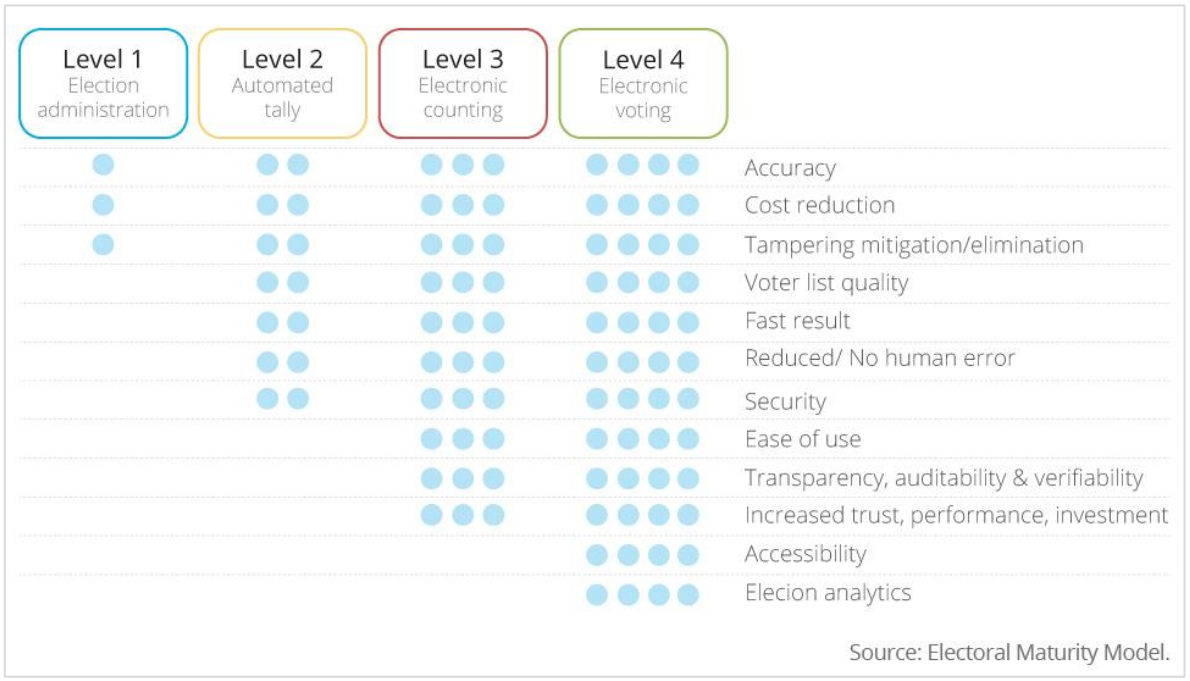


Fig. 3 **Election automation benefits**.

Shedding further light on good election system security

The following analysis is based on research conducted by Smartmatic since 2001, which provides a model of what constitutes good security design for election systems to work in any part of the world. Real and perceived threats to election security are highly culture-dependent. The security assumptions made in Brazil are entirely different from those made in Switzerland, which are again different from those in the US or in the Philippines. It is for this reason that our starting position is always to assume the worst-case scenario. We require the most constraining security requirements to be used, in order to ensure an approach secure enough to be used universally.

First and foremost, our design approach makes one key assumption: one cannot trust anyone. This is simply stated, but as far as we know, no other election system designer has taken this as the core key design variable on which to build a solution. But what is meant by not trusting anyone? It goes without saying that this includes hackers and criminals who could attempt to attack the system. But it also includes the political parties, the government, the election commission, everyone who works with the election commission, voters and, of course, the company building the system and its employees.

So how do you make an unhackable election system? As obvious as it sounds, let's first remember that, in order to hack a system, you need time and money (to purchase, e.g. a computer). The more robust and advanced the security and cryptography are, the more time and money you will need to successfully attack the system. Thus, the time and money needed are directly proportional to the level of security. However, if you want to hack a cryptographic system more quickly (less time), you need more computational power (more money). Therefore, the two are inversely proportional to each other.

This is all great news for digital voting technologists, as we will soon see.

To create a completely unhackable system, Smartmatic combined the following ideas: security fragmentation, security layering, encryption, device identity assurance, multi-key combinations and opposing-party auditing. Explaining all of them is beyond the scope of this article.

The important thing is that, when all of these methods are combined, it becomes possible to calculate with mathematical precision the probability of the system being hacked in the available time, because an election usually happens in a few hours or at the most over a few days. (For example, for one of our average customers, the probability was 1×10^{-19}. That is a point followed by 19 zeros and then 1). The probability is lower than that of a meteor hitting the earth and wiping us all out in the next few years—approximately 1×10^{-7} (Chemical Industry Education Centre, Risk-Ed n.d.)—hence it seems reasonable to use the term 'unhackable', to the chagrin of the purists and to my pleasure.

Although this level of security is astronomically high, it is not enough simply to provide mathematically perfect security. Why not? Because although it is true, people need *to know* it is true, and the mathematical explanation is just too technical for the general population to understand. It is for that reason that we created the citizens' audit: a simple, yet powerful method by which any concerned citizen can verify that the results of an election are indeed accurate and have not been tampered with.

The combination of perfect security with the awareness of that security created by the citizens audit is the reason why, after 2.5 billion votes cast and counted with our systems, and after multiple audits, including all citizens' audits, we have never experienced a successful attempt to hack or tamper with our technology. Moreover, despite thousands of 'sore-loser' candidates in many countries and well-funded movements trying to attack the election system for their own gain, not once has any election result ever been changed in any one of the elections conducted with Smartmatic systems, through which more than 38,000 public officers have been elected during the past 10 years, from hundreds of thousands of candidates.

Conclusion

The main message here is threefold:

1. First, manual elections are extremely vulnerable, prone to errors and very expensive.

2. Second, the arguments that have long been made in favour of keeping elections manual are scientifically flawed. They can be placed alongside other thoroughly discredited theories such as those promoted by anti-vaccination groups. Unsupported by facts, they can be immensely damaging.

3. Third, progress is already being made. Currently more than 70 countries are between Stages 1 and 8 of the Election Automation Maturity Curve, up from less than 30 a mere 5 years ago. The trend is unstoppable, but we will benefit sooner if we fully embrace technology for elections now, focusing only on what is important: that the quality of the solutions is sound and complies with the highest standards.

In addition to all of the above, it is important to mention that Internet (and mobile) voting is rapidly being piloted as a substitute for postal voting and to provide the best absentee, overseas and military voting systems. This will become very common in the next few years. Internet voting pioneer Estonia (Estonian National Electoral Committee n.d.; Eesti Reformierakont *2015*) has already gone further, having become the first country in the world to offer multi-channel voting. Any citizen can decide to vote online or at the polling station.

Few doubt that the future is digital, not only for elections but also for government–citizen interaction, participation, engagement and campaigning. Thus, the sooner we embrace voting technology, the more value we will extract from it. Pioneering countries are setting a new level of transparency, facilitating engagement and giving their citizens the advanced democratic tools that they demand and deserve.

References

Alave, K. L., Yamsuan, C. C., & Quismundo, T. (2010). Fast count stuns nation. Faster than you can say 'Garci'. Philippine Daily Inquirer, 12, December. http://newsinfo.inquirer.net/inquirerheadlines/nation/view/20100512-269508/Fast-count-stuns-nation. Accessed 27 March 2015.
118
Chemical Industry Education Centre, Risk-Ed. (n.d). Asteroid impact. The probability of an asteroid impact. http://www.risk-ed.org/pages/risk/asteroid_prob.htm. Accessed 27 March 2015.
Eesti Reformierakont. (2015). Prime Minister of Estonia explains how fast, simple and safe is e-voting. YouTube. 19 February. https://www.youtube.com/watch?v=yZ4s95lFkk4&feature=youtu.be. Accessed 27 March 2015.
Electoral Maturity Model. (2015). Related work. http://electoralmaturity.org/blog/related-work/. Accessed 27 March 2015.
Estonian National Electoral Committee. (n.d). Internet voting in Estonia. http://www.vvk.ee/votingmethods-in-estonia/. Accessed 27 March 2015.
Quraishi, S. Y. (2014). An undocumented wonder: The making of the great Indian election. New Delhi: Rupa Publications.
Smartmatic. (2014). Demo on accessibility. London, UK.

* Antonio Mugica is the founder and CEO of Smartmatic, the largest voting technology provider in the world, delivering secure and transparent elections across five continents. He also sits on the boards of SGO and the publicly listed company Anoto Ltd.