ELECTRONIC VOTING IN A SECURE LEGAL IDENTITY ECOSYSTEM

Niall McCann, Lead Electoral Advisor and Legal Identity Focal Point
and Risa Arai, Election Policy Analyst
United Nations Development Programme

Electronic voting systems are facing criticism. Could the solution lie not in voting machines themselves, but in modern, integrated civil registration and national ID systems?

Electoral administration has always relied on confidence. Political contestants, civil society and voters need to have confidence that the entire system of electoral administration – from registration of voters, registration of candidates, voting and results tabulation by electoral management bodies (EMBs) – is credible, safe and secure. If parties lose confidence in the system (whether concerns are related to political influence on the EMB, a lack of EMB capacity or manipulation by other external actors), the system breaks down. In a number of countries that have moved partially or wholly to electronic voting systems,[1] EMBs increasingly appear to be "playing defence," with many publicized cases of electoral officials having to reassure their citizens and political parties that e-voting machines are secure and can withstand cyberattack.[2] Some electoral administrators in 'older democracies' are calling for a full return to paper-based systems as the only sure way to avoid external compromise.[3]

On the face of it, this is surprising, in that technology is so often crudely seen as evidence of 'innovation,' and moves away from paper balloting and towards e-voting have often been seen as inevitable signs of progress. But given the retreat of paper systems from so many areas of public administration in recent years (from, for example, social security systems to taxation to identity documents issuance), one could argue that electronic voting – used as the primary methodology for national elections in less than 25 countries[4] – has not nearly 'caught on' the way it could reasonably have been expected to. In recent years, Norway, Germany, Japan, Ireland and the Netherlands have all introduced elements of electronic voting into their electoral administration, only to remove it partially or fully at a later date[5]. The failure of e-voting in Ireland in 2004 was so profound that adoption in this modern 'digital nation' appears off the cards for the foreseeable future.[6] How did we get here?

[1] *'E-voting' or 'EVMs' (electronic voting machines) are the terms usually used to describe the casting of ballots on purpose-built voting machines in polling centres. They can be fully electronic (such as the touch screen models used in Venezuela), or partially electronic (such as where paper ballots are scanned by electronic scanners to record the vote cast as used in a number of US states). 'E-voting,' for the purposes of this article, does not refer to any form of internet voting ('i-voting'), or to electronic election results management, which are separately discussed in this paper.*

[2] *For example, in India, claims that the EVMs were 'hacked' during the 2014 general elections were rejected by the Indian EMB, https://www.bbc.com/news/world-asia-india-46987319. In the 2018 parliamentary election in Iraq, one of the reasons the partial recount was conducted was due to the alleged vulnerability of voting machines to hacking, https://www.reuters.com/article/us-iraq-election-exclusive/exclusive-iraq-election-commission-ignored-warnings-over-voting-machines-document-idUSKBN1KQ0CG.*

[3] *https://www.newsweek.com/dutch-election-electronic-voting-hacking-russia-france-macron-trump-clinton-564198*

[4] *https://epthinktank.eu/2018/09/12/digital-technology-in-elections-efficiency-versus-credibility/e-voting_countries/*

[5] *Norway (https://www.bbc.com/news/technology-28055678)*

[6] *Second report of the Commission on Electronic Voting on the secrecy, accuracy and testing of the chosen electronic voting system, 2006. http://catalogue.nli.ie/Record/vtls000249414*

Copyright© Verified Voting Foundation

Electronic voting systems largely focus on how ballots get cast but very little on who is casting them.

Fully electronic systems (such as touch screen machines), or hybrid systems (such as where voters run paper ballots through scanners) have advantages, but there are a number of hidden costs to, and disadvantages of, moving to e-voting systems, which merit some attention.

EVMs may eliminate the need for complex procedures on how to determine the will of the voter on an unclear ballot paper, for example, but polling officials require complex training on how to deal with the challenge of system failure; polling staff are usually challenged to conduct system reboots in real time, or explain complex technical problems to technical support staff (assuming there is network coverage) by phone to explain the problem and find solutions.

In terms of sustainability, on top of the initial outlay of the machines themselves,[7] costs related to air-conditioned storage, electricity use, software upgrades, etc. – none of which are required for paper systems – tend to get under-budgeted.[8] EMBs committed to rolling out e-voting systems could consider software-based systems that at least sit on core operating systems[9] that would allow those machines, often deployed in their tens of thousands, to serve other public administration authorities.

In terms of results processing, while results, at the level of the individual machine, might be faster to produce than counting paper ballots at the polling station, modern electronic results management systems that rely on mobile connectivity are arguably able to transfer tabulated results from individual polling centres to centralized data centres just as fast as EVM systems, and collate them centrally just as fast. The speed that results arriving in electronic format in centralized electoral management body (EMB) data centres get processed has little to do with how they were cast and counted at the polling location.

The truth is that there are many ways to cheat on elections. Indirect means include: abuse of state resources by incumbents; campaign finance violations; vote buying; media control; intimidation, harassment or outright attack of candidates and/or their supporters; and, increasingly, manipulation of social media to sow public discord that pushes voters to extremist voting options, etc. **E-voting solves none of those problems.**

The main ways to directly commit electoral fraud include: manipulation of voter registration (whether it be the inclusion of ineligible voters or the exclusion of eligible voters); voter suppression (e.g. via restrictive voter ID laws or coercive threats of severe penalties for voter fraud); gerrymandering of electoral boundaries to reduce the voting power of particular groups, and; manipulation of election results (in systems where counting takes place immediately on-site after polling) after they have left the polling centre (often times via changing results sheets, or via entering incorrect data in data processing centres). **E-voting does not necessarily solve these problems.**

EVMs also do not solve the problems of low voter turnout, of electoral systems that produce outcomes disproportionate to the votes that political options receive, of disillusionment with representative democracy and the rise of populism, with the demonization of minorities or immigrants or the civil service class, or with challenges to the rule of law. EVMs do not automatically bring more people to the polls. Voters voting by EVM still have to travel to a polling location, stand in line, verify their presence on the voters list, and cast their ballot. And for some older people, e-voting may present a major challenge, as they may be more familiar with the paper ballot system they have known for years. Problems such as the latter would be analysed in the course of conducting proper feasibility studies when countries are considering moving to e-voting systems, but alas, evidence suggests that countries often make the decision to move to e-voting without either carrying out such studies, or ignoring inconvenient findings.

In fact, the only problem that e-voting can arguably address is ballot fraud, whether it be ballots cast for a particular voting option against the wishes of the voter, or ballot stuffing, where polling officials themselves – often times contracted for as little as two days – cast ballots either in place of, or on top of, those cast by eligible voters. In either case, the fraud is either wholly or largely committed by polling station officials themselves, either pro-actively, or under duress by local political leaders or their cadres.

[7] *EVMs for the 2018 general elections in DRC allegedly cost over US$160m. (https://www.apnews.com/1764856db1b74c7790a05a65d7a9c5b0)*

[8] *In Ireland, following the e-voting experiment in 2004, annual storage fee costs ran at €140,000 Euro annually (even after the machines were taken out of circulation), and the machines were eventually sold for scrap for €70,267. (https://www.irishtimes.com/news/e-voting-machines-to-be-scrapped-1.722896)*

[9] *E.g. Windows, Apple or Linux systems.*

However, if polling fraud can largely only be conducted by or with the complicity of polling officials, then what would prevent a polling official marking an extra 100 voters as present and pushing a touch screen 100 more times? If polling officials plan to commit polling fraud, are they any more deterred from doing so because it is a machine, rather than a book of ballots, that is their path to fraud?

Where polling fraud has been seen to have taken place or has been suspected of taking place, examinations of "what happened" present a further problem for e-voting systems. While examinations or recounts in paper-based systems can clearly take place in full view of observers and political parties, either at the point of discovery or later via post-electoral audits, etc., this option, as so clearly articulated in the 2009 decision of the German Constitutional Court that resulted in Germany abandoning e-voting, is much more difficult to achieve in EVM systems, where system auditing or verification in public view of observers or parties, etc. is very challenging.[10] You often simply have to trust the software, or trust the software analysts.

This has not stopped some countries from adopting other technology solutions to combat polling fraud, however. Countries such as Kenya and Afghanistan, for example, have deployed 'biometric voter verification' (BVV) systems that check voters' biometric data at the polling centre to ensure that they are registered to vote there, prior to the ballot being issued.[11] As effective as such systems may be in any individual country, they are not foolproof. What is to stop corrupt electoral officials, for example, or local political leaders, lining voters up and entering them in the BVV system before either taking their ballots, or instructing them on how to vote? The truth is that while new digital innovations such as distributed ledger technology (blockchains), BVV systems or camera systems in polling centres[12] can improve the transparency of polling fraud detection, there is currently no known proven technology that can prevent corrupt electoral officials, particularly when supported by local political leaders, from cheating on elections. As the UN Secretary-General has noted in a succession of biennial reports to the UN General Assembly documenting the UN's work in support of democratic elections, it is the responsibility of political leaders to inspire confidence and trust in the credibility of electoral administrators and the legitimacy of electoral outcomes that leads to credible elections, and not misguided faith that any suite of technological solutions will somehow guarantee the legitimacy of elections.[13]

How can electronic voting systems truly empower?

Looking to the future, does technology have a meaningful role to play in the voting elements of an electoral process? Advances are clearly being made on electronic results transmission and on electronic results processing. For example, blockchains and other innovations should be able to eventually assist parties and observers to have real-time, off-site access to election results as they are entered into results databases. This can certainly bring greater transparency to this most sensitive of electoral administrative tasks. Governments and electoral administrators would do well to consider, however, the role of technology in voting in a broader digital governance context. Is there a case for looking more closely on how technology can enhance the credibility of the voter register, for example, thus focusing more on who casts the votes rather than on how they are cast? After all, a valid vote cast by an ineligible voter is just as damaging to an electoral process as an extra ballot cast fraudulently by an electoral official.

Estonia is still the only country in the world, for example, that facilitates internet voting for national elections.[14] More than 30% of voters have chosen to cast their vote online in the last three national elections.[15] Which will be the first country to facilitate largescale voting in national elections from smart device applications? Critics have voiced concern about possible internet-based "voting in a non-controlled environment" for many years. Concerns largely focus on two issues: how can electoral administrators be sure that the person eligible and registered to vote is the one actually casting the (electronic) ballot, and; how can electoral administrators be sure that the voter is not voting under the influence of others. These concerns have some merit and need to be addressed.

Yet as we have seen in the case of ballot stuffing or other cases where polling staff either prevent a legitimate voter from voting, or facilitate a fake voter to vote, in-person voting in polling centres is no guarantee of electoral legitimacy. And as for 'family voting' – the most common form of voting under the influence of others – this has been a feature of in-person, 'controlled environment' voting in polling centres across the globe for decades, and regularly features in the reports of domestic and international elections observers.

In fact, internet voting cuts out fraudulent polling officials – or at least those hired or engaged on a short-term basis at the local level – almost entirely. As of now (and noting the levels of 'turnout' in popular culture 'vote-in' competitions, where young people's participation ranks significantly higher than in some elections), anecdotal evidence would suggest that internet voting would increase voter turnout in many countries. And experience in Estonia has shown that old people are just as likely to embrace internet-based systems as younger people (although this may not be the experience of all countries). But to address possible side-effects, Estonia has adopted two procedures to limit the negative influence of those (presumably family members or local political leaders) that may wish to influence those that cast their vote at home. Firstly, the window for voting online is extended to approximately seven days[16] prior to in-person polling day, and the voter can vote online as many times as they like, where only the last vote received is the one that is counted. Secondly, even if the vote has been cast online, the voter can turn up in-person at their registered polling centre on polling day and cast their ballot in person, at which point the online vote is cancelled.

[10] https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany
[11] As used in the 2018 parliamentary elections in Afghanistan, however, there was no prior biometric database of votes to check prior registration against. The technology was therefore limited in its ability to detect voters who had attempted to vote at other locations.
[12] Such as those recently used in elections in Armenia.
[13] "..the overriding responsibility for a successful election lies with political leaders, from both government and opposition parties. That encourages political actors to remain engaged in an electoral process once they have joined it and to refrain from alleging widespread fraud without evidence." 'Strengthening the role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization, A/27/260, August 2017.
[14] https://epthinktank.eu/2018/09/12/digital-technology-in-elections-efficiency-versus-credibility/internet_voting_countries/
[15] Vassil, K. et al, "The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015, Gov. Inf. Q. 33(3), 453–459 (2016).
[16] https://www.ndi.org/e-voting-guide/examples/internet-voting-in-estonia or https://www.valimised.ee/en.

But internet voting is not for all countries. Many countries face too many uphill challenges to ever make mass internet voting the method of choice for a majority of its voters. Those challenges fall broadly into two groups: technical and political. Technical challenges include poor technology infrastructure and capacity, as well as under-developed civil registration systems that provide enormous challenges in compiling a credible voter register. Political challenges include deep suspicion of political opponents' ability to manipulate voting that takes place outside polling centres, particularly in countries that suffer from deep 'identity politics' divisions; at least 'in-person' voting, even if chaotic and destined for contentious outcomes, can be observed. Overall, lack of faith in the capacity of the EMBs to organize credible elections is not likely to be dissipated by internet voting.

But what lessons can we learn from why internet voting works in Estonia? Estonia's 'smallness' – only 1.3m people spread out over a rural hinterland – played a factor in Estonia's transformation into the world's leader in digital governance. Estonia's move of many previously paper-based or in person transactions into the digital sphere is the subject of much commentary, with Estonians conducting much of their transactions with the state online, from registering a business, declaring and paying tax, and having documents issued.[17] **The backbone of the entire system, however, is the country's integrated, digital civil registration and national identity register.** Still operating on a PIN system (rather than biometrics) to authenticate identity, Estonians use their national ID card[18] or number[19] to log into a government gateway portal to access state services, and increasingly, private services.[20] In spite of occasional challenges with regards to system integrity, Estonians that vote online largely do so with confidence that their vote will be recorded correctly and securely. And political parties that support the system largely have confidence in the integrity of both the identity register – thus guaranteeing that only eligible voters can cast their vote – and the security infrastructure behind it.

While Estonia is at a different stage in its development than many countries, the Estonian experience with i-voting begs one question – would countries at all stages of their development be better served by examining whether technological investment for elections could help build robust legal identity systems (via holistic, birth-to-death, integrated civil registration and national ID systems) that may support digital innovations such as online voting, rather than at in-person electronic voting machines that may end up going the way of fax machines?

Questions or comments?
Niall.McCann@undp.org
Risa.arai@undp.org

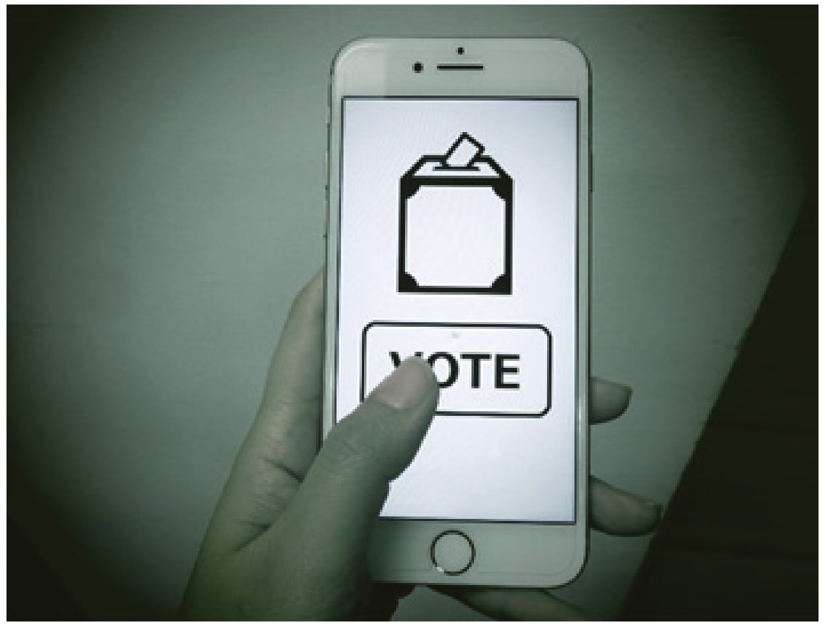

Photo credit: Risa Arai/UNDP

[17] http://www.bbc.com/future/story/20171019-could-estonia-be-the-first-digital-country
https://www.economist.com/the-economist-explains/2013/07/30/how-did-estonia-become-a-leader-in-technology
[18] Via a USB extension port.
[19] A number of mobile carriers and banks assist the state to authenticate the national ID number and accompanying PIN when used as entry portals to other services.
[20] E-Estonia: https://e-estonia.com/

Estonia Portal (new):
https://tara.ria.ee/login?service=https%3A%2F%2Ftara.ria.ee%2Foauth2.0%2FcallbackAuthorize%3Fclient_id%3Dtim_toodang%26redirect_uri%3Dhttps%253A%252F%252Ftim.www.eesti.ee%252Ftim%252Fauthenticate%26response_type%3Dcode%26client_name%3DCasOAuthClient
Estonia Portal (old):
https://www.eesti.ee/eng/services