Labour Party

Electronic Voting in Ireland

A Threat to Democracy ?

Report prepared for the Labour Parliamentary Party by

Shane Hogan and Robert Cochran

"The voters don't decide the election,

the counters decide the election,

so keep counting"

from Gangs of New York, 2002

November 2003

Table of Contents

1 Executive Summary

The currently proposed solution for Electronic Voting in Ireland presents a number of significant threats to the democratic process. Unless these are effectively dealt with, there is a significant risk that public confidence in the voting system will be lost.

The absence of a 'Voter Verifiable Audit Trail' (V.V.A.T.) means that the openness and transparency which characterised the traditional manual system are consigned to history. The voter will now be required to have 'blind trust' in the system which determines the composition of their local authorities and the Oireachtas and their representatives in the European Parliament.

The absence of formal control processes and procedures around the usage of the current system exposes the electoral process to possible interference from unauthorised persons. Documentation received from Dept of Environment, Heritage & Local Government (DoEHLG) indicates that there are no formal processes for;

- Restricting access to count centre PC's during the count
- Installation of software on count centre PC's
- Verification of software installation on count centre PC's & Nedap voting machines
- Purchasing of 'ballot modules' (the memory device from the Nedap voting machine)

We recommend that an audit and supervisory role around the implementation of electronic voting is given to an independent body, such as the Standards in Public Offices Commission.

While the individual components of the system have been extensively tested in isolation, **no integrated 'end-to-end' test of the entire system has been conducted to date.** An integrated 'end-to-end' test would generally be considered a key part of the implementation of any new technology. It is a particular concern that the randomisation feature of the IES Powervote system was excluded from the DoEHLG testing.

It appears that the promised cost savings resulting from reduced manpower during counting may be outweighed by the increased personnel required to operate the voting machines. Each voting machine requires a 'control operator' to enable the machine for each voter. On the assumption that the 'control operator' is additional to the existing staff, the additional cost of thousands of control operators will more than outweigh any saving on count centre staff.

We recommend that further usage of Electronic Voting in Ireland is suspended, until

- A Voter Verifiable Audit Trail is available to give each voter absolute confidence that their vote had been correctly recorded and counted.
- Appropriate control processes & procedures are implemented by DoEHLG, with audit & supervisory responsibility vested in an independent body.
- Integrated 'end-to-end' testing, including statistical analysis of the randomisation feature, is carried out to verify the accuracy of the entire system
- DoEHLG commits to providing full details of tally information in database form after each election.

2 Context & History

From the latter-half of 1990's, electoral authorities across the world have been seeking to use computer technology to improve the electoral process. The same basic model has been utilised in many countries – a 'voting machine' is used at the polling station to allow the voter to select their preferences, and votes are then transferred to a centralised counting system. In the UK, some pilot tests of alternative approaches using telephone and internet based voting have taken place in recent years, eliminating the need for voting machines and polling stations, but with limited success.

However, concerns have been growing worldwide about the integrity of electronic voting. These concerns largely originated in the academic world, but have now spread to political activists, commentators and concerned citizens. In general, the traditional paper-based systems were hallmarked by openness and transparency, while still protecting the secrecy of the ballot box. These concerns have been underlined by a number of worrying incidents which highlighted the potential for abuse of the electronic systems.

- Republican Senator Chuck Hagel (Nebraska) was discovered to have failed to declare his part-ownership in ES&S, the company which manufactured the voting machines which counted 85% of the votes in his 1996 & 2002 senate elections.
- In Louisiana in 1999, a $8m bribery scheme involving the purchase of Sequoia voting machines was uncovered and netted convictions against state elections commissioner Jerry Fowler and Sequoia's exclusive agent David Philpot. *[Jefferson Smurfit plc owned 100% of Sequoia Voting Systems prior to disposal of 85% to De La Rue in May 2002]*
- In Sheffield UK in May 2003, many polling stations were without an Internet connection on polling day. As a result voters could get a vote at a polling station while still being able to vote again online from home.

In Ireland, there is a growing concern that the current Government is 'shifting the goalposts' in an attempt to secure victory in the next general election. Restrictions to the Freedom of Information Act, changes to political contribution limits and the review of constituency boundaries along with the implementation of electronic voting have contributed to an atmosphere of scepticism around the whole political process. Given that Dail seats may well be decided by a handful of votes (remember the recent case in Wicklow, and in Kerry North a few years ago) and the next Government may well be decided by a handful of seats, the possibility exists that a focussed attack on a small number of voting machines and/or count centres could be enough to make (or break) the next Government..

More generally, the Irish people have rightly developed a strong degree of confidence in the existing manual system, built up over the years. If anything were to happen which damaged this confidence (e.g. arising from a court challenge to the electronic voting results), then the already weakening support for representative democracy could be dealt a serious blow, with unforeseen and far-reaching consequences.

3 The Irish Solution

3.1 History

In June 2000, the DoEHLG issued tenders for supply of electronic voting systems. In December 2000, Nedap was selected as the supplier for voting machines, and the Integrated Election Software (IES) system from Powervote was selected as the vote counting software.

The system was first piloted in the May 2002 general election in three constituencies (Meath, Dublin North and Dublin West). For the Nice II referendum in October 2002, a further pilot was carried out in seven constituencies (Dublin Mid-West, Dublin North, Dublin South, Dublin South-West, Dublin West, Dun Laoghaire and Meath). As the pilots were deemed to be 'successful', it is planned that the Nedap and IES system will be used to operate all local & general elections and referenda for the foreseeable future. A total of 7,000 Nedap voting machines have been purchased bringing the total cost for the system to €36m. A further €1.5m has been earmarked for a PR campaign to educate the public on electronic voting.

3.2 Key Components

The Nedap voting machines is a suitcase-sized, portable computer-based voting machine. It can handle up to 5 simultaneous ballots, with up to 30 selections (candidates) per ballot. It uses a removable 'ballot module' memory device to store the voter selections in random sequence. Each ballot module is pre-programmed with a unique identification number, and can hold up to 30,000 voter selections. Each voting machine has a backup ballot module and a battery backup. Voting is enabled for each voter by the 'control operator' using a separate control unit.

The Integrated Election Software (IES) system supplied by Powervote Ltd runs on a standard PC, using a Microsoft Access database. This is used to load details of the election onto the ballot modules in advance of the poll. At the end of the poll, the votes are loaded from the ballot modules into the IES system, mixed into a random sequence and counted. The IES system then makes the count results available on printout and on screen.

3.3 Operating Procedures

Details of the elections and candidates are keyed into the IES system. Each ballot module which will be used for that election is then connected to the IES system via a programming unit and details of the election are downloaded onto the ballot module.

The ballot module is then installed into the voting machine at the polling station. A printout is generated to verify that the ballot module is empty of votes at the start of the poll. Voters are authenticated using the electoral register as per the traditional system. Once a voter is authenticated, they are issued with a token and they proceed to a voting machine. They give the token to the control operator, who will then enable the machine for voting. The voter records their preference for each election by pressing buttons in the relevant column. When the voter is complete, they must press the 'Cast Vote' button to record their preferences.

The control operator can see on their control unit when the 'Cast Vote' button has been pressed. The voter's preference(s) are then stored on the ballot module. If the voter leaves the voting machine without pressing the 'Cast Vote' button, the control operator may advise them that their vote has not been completed. The control operator must log each uncompleted vote on a paper form before resetting the voting machine for the next voter.

At the end of the poll, a printout is generated on the voting machine to show the number of votes recorded. The control operator and presiding officer can reconcile the number of tokens issued, the number of votes recorded and the number of uncompleted votes for each machine. The voting machine copies all votes on the ballot module onto the backup ballot module. The ballot module is removed and sent to the count centre.

At the count centre, each ballot module is connected to the IES system and the votes are loaded into the database (after verifying the unique identification number on the ballot module). If more than one PC is being used for loading of ballot modules, then votes can be transferred between PC's on disk. When all ballot modules have been downloaded, the IES system mixes the votes received into a random sequence and then proceeds to count the votes via the PR-STV rules. The count is only interrupted if the drawing of lots in case of a tie is required. When the count has completed, the results can be printed and viewed on screen.

4 Voter Verifiable Audit Trail (V.V.A.T.)

There is a growing local & international movement calling for a Voter Verifiable Audit Trail (V.V.A.T.) to be part of all electronic voting systems. The basic principle of V.V.A.T. is to ensure that each voter can be 100% certain that their vote has been recorded accurately and has been included in the count.

The current Nedap/Powervote is not designed to produce a 100% guarantee for each voter, as it has no paper-based backup or audit trail. Regardless of what is displayed on-screen on the voting machine, it is possible that the voting software has been designed to store a different or incorrect version of the vote in its memory. While it is possible to test the inputs & outputs of voting machines to give a reasonable degree of certainty regarding their accuracy, it is theoretically possible that;

- The software has been designed to operate normally during testing but to bias one candidate or party after getting a certain 'trigger', e.g. a sequence of keys operated by an early voter

- While the tested version of the software operates correctly, a corrupted version of the software (which will bias one candidate or party) is installed on the voting machine. This may have the appearance of the tested version (i.e. same version number displayed on screen & on printouts) but the votes are recorded differently.

The core principle of V.V.A.T. requires that a backup or audit trail (usually paper-based) be implemented to give each voter a clear guarantee that their electoral preferences will be included in the final count. This could work as follows;

- The voter makes their selections on a voting machine as normal
- A printed 'receipt' generated showing the choices selected (but not identifying the voter) and the voter views receipt through a see-through panel
- The voter confirms that the receipt reflects their choices, or may cancel & restart the process
- Once the voter confirms that the receipt is correct, the printed 'receipt' automatically goes into a ballot box & the vote is also stored electronically
- Electronic votes can be counted automatically, but in case of dispute, the printed version is the primary source and a manual count is carried out.

There are also some emerging technologies which create electronic 'receipts' for each vote using digital signatures.

The random selection used when distributing a surplus in the Irish system presents a particular challenge for V.V.A.T. Where two counts are carried out (one electronic and one manual) using two different random selections, the results of the counts may well be different. This is particularly likely in constituencies where the last seat may be decided on a handful of votes. It is not the case that one is right & one is wrong – both are right, but because of the random selection, the two results may be different.

There are two possible approaches resolving this issue. Using the existing software, the randomisation & count could be repeated many times. A legal procedure could therefore be established so that when the outcome of an election, following randomization, is decided by a margin less than the expected randomization margin, a full statistical analysis in undertaken. If that margin is determined to be say 5%, then if a result less that 5% from the next candidate, the system is instructed to repeat the randomisation & count at least 30 times, and to do an analysis of the results. Comparing these results should (if the randomization is done correctly) show a 'bell curve' from which the statistical mean (average) can be calculated. This mean value could then determine the formal result of that count.

Alternatively, this issue could be resolved using 'fractional votes', though this would require a change in policy, culture & legislation. Instead of selecting specific votes at random to represent the surplus, all votes for the candidate would be transferred, but would be 'weighted' to ensure that the total number of votes transferred matches the surplus. Take an example where the surplus is 4,500 votes and the last candidate elected had 5,000 votes. This leaves a surplus of 500 votes to be transferred. Instead of selecting 500 votes at random to be transferred, each of the 5,000 votes would be transferred, but each transferred vote would be weighted at 10%. This could result in fractional votes, where a candidate receives, for example, 80.4 votes. The fractional vote calculation would be extremely difficult to implement in a manual system, but would be manageable in an automated system.

Recommendation: **The Government should recognise that V.V.A.T. is an essential requirement for electronic voting in Ireland.** The DoEHLG should investigate options for upgrading the existing Nedap/Powervote system to produce a V.V.A.T. If this is not possible, the existing system should be replaced, though this will incur considerable costs for the exchequer.

5 Possible Threats

5.1 No 'End-to-End' integrated tests

While the individual components of the system have been extensively tested in isolation, **no integrated 'end-to-end' test of the entire system has been conducted to date.**

The testing of the IES software was carried out on behalf of DoEHLG by the UK-based Electoral Reform Society in 2002. However, for this test, the 'random mix' feature of the IES software was disabled. This was presumably done to simplify the testing process and ensure that repeat tests give the same result each time, without any random effect. However, the impact of this means that the IES software, as it will operate at a real election count, has not been tested.

An integrated 'end-to-end' test would generally be considered a key part of the implementation of any new technology. This would involve entry of a known set of votes into the system processing the votes through to the final results. These results would then be compared against the expected results to verify the accuracy of the system. The piloting of the system in the 2002 general election and Nice referendum could not be considered an 'end-to-end' test, as there was no 'expected result' available for comparison.

Recommendation: **We recommend that DoEHLG arranges a set of integrated 'end-to-end' tests of the entire system, including the 'random mix' feature of the IES software**. While the random effect may produce different results with each tests, the tests should be repeated until a statistically significant result is evident.

5.2 No 'Formal Methods' used in development of software

'Formal methods' refers to a set of mathematically-based techniques that are used in the development of safety-critical software, such as airplane navigation systems or life-support machines. These techniques make it possible to mathematically prove, or at least significantly raise, the accuracy of the software. However, software development using formal methods can be slower than traditional methods and the skills required are typically more expensive.

While DoEHLG have not made the actual source code publicly available, it is clear from the technologies used and the source code review that formal methods were not used in development of either the IES system or the Nedap voting machines. Therefore (unless these systems are absolutely unique in the world of software development), we know that there must be bugs in the software – it is just a question of how many bugs and how significant they are.

Recommendation: **We recommend that DoEHLG releases the source code and test results of both the IES system and the Nedap software to public review, in order to independently assess the quality and reliability of the software**. The release of the source code in the public domain will ensure that the system in analysed by a broad range of experts in Ireland and beyond. This would also help to reassure the public that there is 'nothing to hide'. These independent assessments will allow for public confidence in the software used to drive the electronic voting system. **We also recommend that 'formal methods' be used considered a key requirement for any future electronic voting systems for Ireland.**

5.3 Possible attack on central database during counting

The database used by the IES system is Microsoft Access. The entire database is held within a single file.

It is possible that the entire database on the count centre PC could be overwritten by a replacement pre-prepared database (which would be designed to give a specific result) by a single 'copy' command. In order to implement this threat, the attacker would need knowledge of the database structure in advance and physical access to the count centre PC (at least for a brief period). Indeed, it is possible that the database could be overwritten simply by inserting a pre-prepared CD into the CD drive on the count PC (via 'Autorun' technology).

Documentation received from DoEHLG refers to the possibility of vote information being transferred between count PC's by floppy disk, in cases where more than one count PC is used to download votes from the ballot modules. Any such transfer of voting data between PC's requires strict systems and procedural controls to maintain the integrity of the database.

Recommendations:

- Implement formal procedures to restrict access to the count centre PC (At present, there are no formal procedures in place and individual returning officers are responsible). Also implement procedures to ensure restricted and controlled access to these PC's and the voting machines prior to use and while in storage (including control of technical support and maintenance staff). Use password-based and/or token-based security to restrict access to authorised users
- Implement systems & procedural controls to cover the transfer of voting data between count PC's
- Implement formal procedures to disable or restrict access to floppy disk drive, CD drive, USB ports, wireless network devices & network connections on count centre PC's, and to ensure that only clean uncorrupted software is installed.
- Implement Voter Verifiable Audit Trail

5.4 Possible tampering with software

It is possible that unauthorised persons could produce a version of the Nedap voting machine software and/or the IES software which is designed to give an incorrect result in favour of a particular party or person. The corrupt version of the software would give all the appearance of normal operation on the surface, but the end result would not reflect the democratic choices of voters.

It would not be easy to attack the election process in this way. Collusion between current or former staff of the software suppliers/testers and election staff would be required in order to make this happen.

Recommendations:

- Implement a formal verification process to ensure that only tested version of software is installed on each voting machine (possibly via use of 'checksums' as used in the UK-based trial of Nedap voting machines in Stratford)
- Implement hard-disk imaging software and/or digital signatures to ensure that only tested version of IES software, tools & operating system is installed on each count PC
- Implement Voter Verifiable Audit Trail

6 Key Recommendations

Our key recommendation is that the Government recognise that a Voter Verifiable Audit Trail (V.V.A.T.) is an essential feature of any electronic voting system to be implemented in Ireland. The current Nedap/IES system should not be used in any further elections unless a V.V.A.T. is implemented. Full tally information and copies of the vote database should be made available to political parties, to allow independent analysis of the results.

The Government should immediately investigate whether the current Nedap/IES can be retrofitted with V.V.A.T. facilities similar or equivalent to those outlined earlier. If this proves possible, the retrofit should be implemented at the earliest opportunity. If it is not possible to implement a V.V.A.T. on the current system, then the Nedap machines may have to be sold off or scrapped, resulting in a considerable loss to the exchequer.

For any future uses of electronic voting in Ireland, we recommend that DoEHLG produce mandatory control procedures for returning officers and presiding officers, with an audit or supervisory role to be vested in an independent body, such as the Standards in Public Offices Commission. It is unreasonable to expect that each individual returning/presiding officer will have the technical expertise to understand the potential threats to the system arising from seemingly innocuous items, like the insertion of a CD by a technician, or the presence of a small rubber aerial at the back of the PC. The control procedures should cover (at a minimum);

- Restricting access to count centre PC's during the count
- Installation of software on count centre PC's & voting machines
- Verification of software installation on count centre PC's & Nedap voting machines
- Transfer of data between count centre PC's
- Purchasing of PC's, voting machines, ballot modules or other equipment

We recommend that DoEHLG carry out full statistical analysis and also integrated 'end-to-end' tests of any proposed solution before it is used for any further actual elections.

7 Appendices

7.1 Further Reading

Dept of Environment & Local Government – Electronic Voting

http://www.environ.ie/DOEI/DOEIPol.nsf/wvNavView/wwdElections?OpenDocument&Lang=en#l12

Electronic Voting in Ireland (Margaret McGaley)	http://www.redbrick.dcu.ie/~afrodite/E-Voting
Verified Voting (David Dill – Stanford University)	http://www.verifiedvoting.org
Electronic Voting (Rebecca Mercuri)	http://www.notablesoftware.com/evote.html
Electoral Reform Society (UK)	http://www.electoral-reform.org.uk
Black Box Voting (Bev Harris)	http://www.blackboxvoting.com

7.2 Report Methodology

This report was produced over the summer of 2003 following a request from Eamon Gilmore. It was based on reviews of documentation provided by DoEHLG in response to an FOI request and several follow-up queries. International activity on electronic voting in Europe & the USA was also reviewed. The review focussed on the practical issues surrounding the implementation of electronic voting, given that other parties had already reviewed technical aspects of the proposed Irish selection.

Initial findings in presentation format were presented in late August 2003. This written report was prepared for discussion at the Labour Parliamentary Party Meeting of 21 October 2003.

7.3 About the Authors

Shane Hogan is currently branch secretary of the Ballinteer/J Larkin branch of the Labour Party. Shane holds a B.Sc. degree in Computer Science from Trinity College and a diploma in Applied Project Management from U.C.C. & Institute of Project Management. Shane has worked as an IT professional for more than 20 years, originally in the development of commercial systems and later in consultancy & IT management. Shane currently works for a multinational technology company and specialises in eCommerce and web-based ordering systems.

Robert Cochran is currently branch secretary of the Dundrum/Sean Fitzpatrick branch and constituency treasurer for Dublin South Labour Party. Robert has over 30 years experience in a wide variety of roles in the software field, including Director of the Centre for Software Engineering in Dublin from its inception until early 2003. He has been an expert advisor to the Irish Government, the OECD, UNIDO, European Commission and others. He has been Director of R&D at the National Software Centre and Head of the Software/IT section of the National Board for Science & Technology. He is a Chartered Statistician and a Chartered (Software) Engineer, and has a masters Degree in Public Administration.

7.4 Acknowledgements

The authors would like to express their thanks to the following persons who helped in the preparation and review of this material;

- Keith Martin – Labour Party, Dublin South East
- Paul Gibson & Margaret McGaley – NUI Maynooth