
# Observing E-enabled Elections: How to Implement Regional Electoral Standards

*Jordi Barrat*

# Contents

International IDEA

SE – 103 34 Stockholm

Sweden

## Acronyms and Abbreviations

| | |
|---|---|
| CEC | Central Electoral Commission |
| CoE | Council of Europe |
| E2E | End-to-End |
| EFFI | Electronic Frontier Finland |
| EMB | Electoral Management Bodies |
| EOM | Election Observation Missions |
| IDEA | International Institute for Democracy and Electoral Assistance |
| IFES | International Foundation for Electoral Studies |
| IT | Information Technology |
| KNB | National Security Committee |
| MP | Member of the Parliament |
| NDA | Non-Disclosure Agreement |
| NGO | Non-Governmental Association |
| OAS | Organization of American States |
| OEA | Organization of American States |
| ODIHR | Office for Democratic Institutions and Human Rights |
| OSCE | Organization for Security and Co-operation in Europe |
| PIN | Personal Identification Number |
| POUREVA | Pour une Ethique du Vote Automatisé |
| VVPAT | Voter Verified Paper Audit Trail (VVPAT) |

## Where Are We?

During the last decade, election observation bodies have paid increasing attention to the problems generated by electronic voting, or, in more general terms, by the use of electronic means as a way to improve traditional electoral processes. Although the term e-enabled elections can refer to a broad range of activities, from candidate registration to tallying, this paper will focus on electronic voting: that is to say, casting a ballot by electronic means. E-counting will be excluded since electronic tabulation always has traditional paper-based back-up, and therefore the problems that it raises, such as the efficiency of the process or the ability to recognize handwritten characters, are very different to those generated by electronic voting procedures.

This first section will describe the official documents that are currently available for assessing the state of the art in this field. The Organization of American States (OAS/OEA) and the European Union, as well as other international organizations, have already issued reports that aim to frame the methodology to be used for elections that include e-voting mechanisms. However, the extremely different profiles adopted by each document make it difficult to establish a common approach. Moreover, there are also specific reports issued by Electoral Observation Missions (EOMs). This section will therefore provide an overview of the different written international tools that form the current starting point for the observation of e-enabled elections.

### Recommendations, Handbooks and Discussion Papers

As stated, there is already a set of documents intended to frame a sound methodology for electronic voting procedures. The OAS, for instance, approved a manual in 2010 for observation missions that focuses on new electoral technologies and includes specific sections devoted to e-voting as well as other chapters that analyse various electronic procedures such as electoral mapping, voters' registers and final tabulation (see OEA 2010). The document is chronologically divided and underlines the issues that are important in the pre-voting stage, during the election day and afterwards. The European Union's Handbook for Election Observation also has a specific section devoted to e-voting challenges (see European Commission 2008), but this document has a much broader scope than the American one: it is a comprehensive handbook on election observation that includes guidelines on both electoral procedures and the organization of an EOM itself.

Other European bodies have provided a heterogeneous set of papers on e-voting standards. For instance, the Office for Democratic Institutions and Human Rights (ODIHR) has published a discussion paper on these issues (OSCE and ODHIR 2008). The Council of Europe (CoE) also adopted a formal Recommendation in 2004 (CoE 2004) and in 2011 produced both an e-voting handbook (CoE 2010), specific guidelines for e-voting observation (CoE 2011) and certification procedures (CoE 2011a). While the ODIHR's paper is conceived only as a starting point for discussion of how to address e-voting challenges, the documents issued by the Council of Europe aim to provide both analytical and practical advice. The CoE document approved in 2004 has an official status: the Committee of Ministers has endorsed it as a formal Recommendation. The other documents have lower legal status.

Finally, it is worth noting that there are private non-profit entities with worldwide activities that have also issued specific reports on e-voting mechanisms, in particular the International Foundation for Electoral Studies (IFES) and the Carter Centre.

In addition, the International Institute for Democracy and Electoral Assistance (IDEA) produced in December 2011 a policy paper on "Introducing Electronic Voting: Essential Considerations".

### Election Observation Missions (EOM)/ Election Assessment Missions (EAM) Reports

While the OAS deployed missions in Venezuela (2005 and 2006), the European Union also sent election observation missions to countries using voting machines, such as Venezuela (2005 and 2006) and Peru (2011). However, the ODIHR is probably the international regional entity with the widest experience in e-voting observation as it has deployed several EOM/EAM missions to countries using e-voting devices. Among others, these have included France (2007), Belgium (2006 and 2007), Kazakhstan (2007), USA (2008), Estonia (2007 and 2011), Norway (2011), Switzerland (2011) and Russia (2011).

### What Do We Need?

Despite the documents described above, it must be noted that we still do not have a sound methodological framework with which to address the problems that arise when observing elections where e-voting mechanisms are used. While EOM/EAM reports focus on a single country, the generic approach used by official handbooks undermines their usefulness, and the ODIHR's discussion paper is not intended to be used as a tool for practical implementation. Finally, among the CoE's documents, only the guidelines on transparency seem directly linked to observation problems.

A comprehensive e-voting observation handbook is therefore still a pending task. But in the meantime the current mix of theoretical handbooks and practical reports can be used to identify the key issues that election observation missions have to face. The following section will conduct a mapping of these issues and include cross-references to those observation reports that have already detected similar problems. The map is intended to improve the understanding of the current theoretical handbooks by linking them to the missions already conducted in countries using e-voting devices.

## Observation of E-enabled Elections: the Main Challenges

Election observation always means employing transparency as a way to independently verify that an election has been correctly conducted. But the ways to achieve such a goal may differ depending on the voting solutions adopted. Certain voting applications, like those using electronic means, may entail some problems. As expressed in the ODHIR's discussion paper on this issue, 'electronic voting poses challenges to the traditional and broadly accepted concepts of transparency and accountability of election processes … The obvious challenge of electronic voting, in terms of transparency and accountability, is that it is more difficult

to observe. Electronic events take place that are not subject to ordinary examination with the naked eye of an observer. Further, electronic voting consists of technological components that are not readily nor easily understood by the average observer.' (OSCE/ODIHR 2008: 2)

Therefore our initial task should consist in finding out how e-voting might allow for independent and external observation: that is to say, how it would provide evidence concerning its correct performance. Once we accept that the scenario will be somewhat different to one with paper-based ballots, we have 'to be aware of the fact that new e-voting technologies might require novel observation methods in order to reach meaningful conclusions' (CoE 2011: n. 5). The key element for this new approach should be trust by proxy: that is to say, a trustworthy framework achieved through indirect means. Given that this kind of confidence relies upon the data provided by third parties, and taking into account that an average observer would not be able to understand such information, this system of trust should not be based on the information as such. Rather, it should be founded on a procedural approach that will assess whether the overall supervisory measures are properly laid out to achieve sound verification of the system.

## E-Voting: is There Anything Meaningful to Observe?

In order to be observed according to correct methodology, e-voting technologies need a two-fold approach. While some features can be supervised using traditional patterns, e-voting also includes strategic components that are based on computerized means and therefore require completely new observation approaches. Election day, for instance, provides interesting data regarding the correct performance of the overall e-voting project, but most of this data is not linked to the core computerized voting structure. Inter alia authentication mechanisms, usability approaches or training standards might be partially supervised during the election day, but the internal performance of the voting machine itself is not observable, at least not by the average citizen. As stated in the EU Handbook, 'the use of e-voting equipment, including software operating under confidentiality agreements, may reduce the transparency of an electoral process, and potentially limit the opportunities for independent observation by party/candidate agents and observers. Observation of e-voting can be challenging, as it requires specialist expertise, and can be less readily accessible to scrutiny. However, the standards for assessing elections using traditional ballot papers apply equally to e-voting.' (European Commission 2008: 85)

This paper will focus on this second approach: concerning those aspects of e-voting that cannot be addressed by traditional observation tools and which require new methodologies. However, this is not to forget the importance of the other approach. Training, for instance, is a cornerstone in any e-voting implementation, given the fact that all election stakeholders have to adapt their behaviour to new frameworks. They have to learn which specific new topics will become suddenly important or how to handle different electoral material. Usability is another key component of any exhaustive e-voting observation, since voting machines will probably generate barriers that have to be overcome with ad-hoc layouts, voter education and appropriate assistance.

However, as mentioned, training, usability and other similar features can always be observed without changing conventional patterns. Obviously, several technological issues

have to be included, but this innovation has no relationship with the observation of purely computer-related issues. While training, usability and so on can be assessed to a degree by the observer's naked eye, technological issues need specific knowledge. This is the great difference, and the reason why this report will focus on the second approach: that is to say, on how to observe data that are normally only understood by computer experts.

The introduction of paper trails is the only exception to this problematic framework. Given that a receipt is intended to prove that the voting machine has recorded each ballot as cast, a parallel paper-based recount becomes feasible, and an average citizen can verify final results, both individually and universally. These kinds of receipts are not problem-free, however, and generate important concerns, such as correct layout or fair resolution of potential discrepancies. Nevertheless, they still provide data that can be understood by anybody.

## Trust by Proxy. Yes, but …

If there are no paper receipts, an average citizen, without specific knowledge, will not be able to supervise e-voting procedures that are based solely on computerized means. Given that only computer scientists, provided they receive enough data in a reasonable timeframe, can understand what is going on, an individual will no longer have personal oversight over the project and his or her confidence will depend on the data provided by third parties, normally a pool of experts. The citizenry will have delegated its control task—what might be called trust by proxy—and therefore citizen confidence will have to be built up by other means. While the tools used to generate this confidence might change depending on the voting solution, the trustworthiness of the system itself, as a final outcome, has always to be maintained.

Such delegation of control has to take into account the fact that electoral and democratic confidence is always based on a political background whose main features are overall distrust and pluralism. While the former stresses that, within a democratic structure, any power has to be limited and controlled, the latter emphasizes that democracies need to combine majorities and minorities. Taking into account these features of the political background is important for e-voting projects because it encourages citizens not to accept in blind faith what electoral authorities do. Even those countries whose governments have achieved a high level of citizen trust need e-voting observation procedures not limited to blind belief in what is said by official computer experts. Moreover, the minority might reject what is accepted by a majority of the population, and observation procedures have to be laid out with enough independence and transparency to convince this minority as well.

Following this reasoning, the EU Handbook advises that e-voting implementation should take into account the existing background regarding citizen confidence in public authorities: 'e-voting is most appropriate in countries with very high levels of public confidence in the integrity of the voting, counting and tabulation processes. In countries where public confidence in the electoral process is low, e-voting may further diminish trust. Public confidence in the use of e-voting is enhanced where there have been inclusive and transparent attempts by the authorities to test, verify and certify the equipment used.' (European Commission 2008: 84)

In conclusion, e-voting observation protocols usually rely upon technical data that can only be understood by computer experts. Average citizens, therefore, will have to base their

confidence on different approaches that take into account how plural, independent and transparent the observation/supervision is that is conducted by technical, legal and social experts. The following section explores which principles have to be adopted in order to achieve such procedural confidence.

## Trust by Proxy Leads to Procedural Trust

Following the EU Handbook, it is worth recalling that 'international observation missions will generally not be in a position to undertake a full verification of the technical aspects of an e-voting system, such as software applications and security systems' (European Commission 2008: 85). Even when EAM/EOM is deployed far in advance, as suggested by the OAS Manual (OEA 2010: 10), the relevant reports will obviously include appropriate disclaimers to acknowledge the actual observation framework.

However, observation reports should not limit their scope to description of the external evidence received during the deployment of the mission. In Peru, for instance, the EU EOM in 2011 included a paragraph describing what happened inside the polling station, but there was no reference to other stages that could have been even more important (EUEOM Peru 2011: 22). Certainly, it only was an experimental trial limited to one location, but the document could have adopted a wider profile.

A procedural approach might become a supplementary way to cover aspects that observation missions cannot verify by their own means, and, in the case of e-voting, such an approach might even become the main strategy not merely a supplementary one. Given that e-voting devices are normally set up by the electoral authorities or by private suppliers directly hired by them, election observation missions might be able technically to verify some issues by their own means, but they also have to identify which other tools are being implemented by election authorities to independently and impartially assess whether the e-voting structure is correctly set up. Audits, certifications and tests are normally used for such purposes, although each one might be implemented in many different ways. Observing does not necessarily mean auditing, testing or certifying, but simply monitoring how these different control procedures are developed. The EU EOM mission to Venezuela in 2006 clearly makes this difference when it recalls that it 'was also present during several of these audits; although not with the aim of auditing per se, but to carry out its observation mandate' (EUEOM Venezuela 2006: 21).

Besides the specific features of each control procedure, there are some general principles that have to be met in every case: integrity of data, comprehensiveness, plurality, independence and transparency.

### *Integrity of Data*

Auditors (here understood to include testers, certifiers and other similar players) should receive any relevant data necessary to conduct their task. Although attention is normally focused on the source code and the compilers, any technical assessment also needs other sources of information in order to gain a detailed overview of the e-voting project.

Both the EU Handbook and ODIHR's discussion paper refer to this issue. The EU Handbook includes the issue as a topic in its code of conduct: '[it] guarantees unimpeded access of the

international election observer mission to all stages of the election process and all election technologies, including electronic technologies and the certification processes for electronic voting and other technologies, without requiring election observation missions to enter into confidentiality or other non disclosure agreements concerning technologies or election processes, and recognizes that international election observation missions may not certify technologies as acceptable' (European Commission 2008: 197; my italics). ODIHR follows this same path. Taking into account that 'elections are a public process exercised collectively by voters in order to realize basic human rights, the electronic voting system should not be made secret by a *private agreement* between a vendor and the election administration. Elections are not for vendors or the election administration; elections belong to the voters' (OSCE/ODIHR 2008: 17; my italics).

Both documents primarily refer to the observers themselves - a term that may actually include both the experts conducting audits and any citizen aiming to conduct an electoral observation. My approach is focused on the first group because such players are the only ones with the knowledge needed to check the voting system.

The advice in these two quotes is intended to prevent what often happens in e-voting implementation. Enhancing transparency may be contradictory with the suppliers' interests, who would perhaps prefer minimum disclosure of their internal methodology. They would argue that voting applications are the result of long-term investments that should not be disclosed to other players. Industrial property rights may protect such an approach as a normal market practice. However, industrial secrecy is not unlimited and has to acknowledge other legitimate interests. In this case, an auditor who receives incomplete information will not be able to develop correct supervision, and election observers will have to take this into account as a weakness that could undermine the overall democratic process. What 'relevant data' actually means in each case might be discussed, but, in doubtful cases, it would always be better to adopt a broad meaning and to allow access to the relevant data.

Finland is a good example of how difficult it can be to meet these criteria. In 2009, the Finnish government decided to pilot internet voting during municipal elections, and the suppliers (TietoEnator and Scytl) provided the opportunity to conduct an audit once a Non-Disclosure Agreement (NDA) was signed. The University of Turku issued a report, but Electronic Frontier Finland (EFFI) refused to sign a document 'that would have severely constrained the auditors' possibilities to publish their findings' (Vähä-Sipilä 2009: 4; see also Tarvainen 2008). An MP and a 'highly experienced IT expert' also refused to sign (see Aaltonen 2010: § 4).

Moreover, the Ministry had previously declined an EFFI demand based on free access to public information, arguing that such disclosure would endanger security arrangements for information and communication, and also private trade and professional secrets (Vähä-Sipilä 2009: 3). Regardless of this governmental decision and the subsequent judicial endorsement, the government itself realized afterwards that 'a situation, where a citizen wants information about the e-voting system in order to make sure that the system acts correctly, but where the authority cannot allow access to the information, cannot be considered satisfactory' (Aaltonen 2010: § 7).

When we analyze the NDA proposed by the suppliers, we easily discover some controversial items (see Barrat 2010). For instance, one paragraph includes a significant disclaimer

regarding the information provided by the suppliers: 'companies do not warrant the accuracy or completeness of any information disclosed under this Agreement. All information is delivered on an "as is" basis, without a warranty of any kind' (TietoEnator 2008: § 8-2). Given this limited starting point, we can legitimately foresee that the confidence enhanced by such agreements will only be an 'as is' perception: that is to say, third parties will rely upon given technical devices assuming theoretically that these are the ones actually implemented. The document also includes other similar requirements that finally led to the refusals mentioned above. As expressed by Whitmore, in the conclusion of a detailed election observation report: 'the measures to ensure transparency could also benefit from a review … More general information about the experiment, in particular system certification, could also possibly have been made available by the organising authorities' (Whitmore 2008: § 58).

Given the importance of a sound disclosure policy, it is worth noting that e-voting implementation is slowly moving forward to such a scenario. While many initial e-voting applications intended to use criteria that were valid for other market areas, suppliers, as well as public administrations are increasingly aware of the special features of this field, and they intend to adapt their internal protocols and NDAs to meet these new needs. Norway, for instance, may be a good model for this new stage of e-voting projects. The Norwegian government deployed an internet voting channel in September 2011 and required vendors to disclose all relevant information. As recalled by Christian Bull, the project pursues 'complete openness and transpare[n]cy in all aspects of the project' (Bull 2011: 15). This entails a 'fully open source system' (Bull 2011: 7), a requirement that would have to be clearly set up in the procurement process. There is a general license that limits potential commercial use of such data, but it is the only significant (and reasonable) limitation for third parties, and states: 'the Norwegian Ministry of Local Government and Regional Development and EDB ErgoGroup AS hereby grant to you (any third party) the right to copy, modify, inspect, compile, debug and run the software for the sole purpose of testing, reviewing or evaluating the code or the system solely for non-commercial purposes' (Government of Norway, Ministry of Local Government and Regional Development 2011).

The integrity of data will also fail if the relevant information is received with great delays, or when access to such data is so cumbersome that it in fact becomes infeasible. Given that bureaucratic burdens may be a risk even for proactive Electoral Management Bodies (EMBs), a specific protocol on how to manage this sensitive information is advisable. As noted by the EU Mission to Venezuela in 2006: 'technical cooperation was not always accompanied by administrative agility; the CNE's excessive bureaucracy on occasions hindered the fluidity of communications. The lack of a procedure by which the CNE could respond in a timely and formal manner to questions and observations, which could have increased the degree of transparency of the system, was also noted' (EUEOM Venezuela 2006: 21).

### *Comprehensiveness*

In addition to the disclosure of all relevant data, the auditors' mission should be laid out so that it covers all the problematic issues that any e-voting project generates. Although this is an obvious goal for any supervision, it is often forgotten because the audit is limited to certain technicalities that actually exclude some key issues. For instance, some certification procedures are based on a passive or reactive verification scheme, which limits

the scope to verify that the machine is doing what it is expected to do once a given set of data has been introduced. Therefore the verification scheme does not include a proactive methodology able to discover hidden gaps within both the theoretical design and the practical implementation. The audit can verify the correct performance of the voting devices, but it is not able to assess which level of computerized attacks will be faced by the voting machine.

The audit in Estonia, for instance, followed these patterns. As recalled by ODIHR, 'the auditing undertaken appeared to be conducted in a very thorough manner. However, it does not appear that the auditors were asked to examine whether the procedures in place were adequate to achieving their objectives' (OSCE/ODIHR 2007b: 15). However, Estonian authorities also implement other tests that, in conjunction with the current one, could achieve the comprehensiveness required by this section. Whether or not this is so, what is important to note is that an audit, or even several supervisions, might not be enough if the overall scheme does not encompass all relevant concerns.

Another common way to start a biased audit consists in excluding certain procedural phases. When using local voting machines, suppliers have a key role, but there are other stakeholders with important tasks as well, such as those charged with the storage of the voting machines and their day-to-day handling. In France, municipalities buy the voting machines and take care of them, but 'the certification process [only] covers the machines and the internal management procedures of the suppliers, including the information that they give to the local authorities … [It] does not cover the security and management standards used by local authorities. The vendors are required to provide general guidelines to their clients, but the implementation depends largely upon the local authorities' (OSCE/ODIHR 2007a: 11). Therefore this certification protocol would not meet the principle of comprehensiveness because it should necessarily include all relevant steps and devices that have an impact on the e-voting itself.

Split authentication and voting procedures can also limit an audits' scope when only the latter is submitted to an exhaustive review. When using local machines, 'observers should make sure that the identification system and the voting system are not connected or interlinked, in order to guarantee the secrecy of the vote' (OEA 2010: 18), but, if internet voting is applied, 'the main challenges in this type of system are the ability to reliably identify the voter, which may be done using a personal identification number (PIN) or an electronic signature' (OEA 2010: 19).

In Norway and Estonia, for instance, internet voting solutions include authentication procedures commonly used for other public services, and it is worth asking to what extent these ID channels would have to be submitted to the same measures foreseen for e-voting mechanisms. Norwegian authorities stress the importance of transparency and have adopted an open policy that consists of the full disclosure of relevant data. But, significantly, such openness does not encompass authentication, which is partially handled by another public entity. Actually, the list of issues that need to be included is much longer than identification (and includes, for example, contingency plans) and none of these issues should be treated as isolated topics not linked to the e-voting system itself.

Finally, another way to limit the comprehensiveness of an audit may consist in using criteria so general that it becomes extremely difficult to track whether or not the audit has

been correctly conducted. In France, for instance, any e-voting system has to comply with a set of 114 rules approved by the Ministry, but these requirements have very different profiles. While some of them are described in great detail (normally those linked to physical stability), others have only general frameworks. As noted by Chantal Enguehard, 'accuracy requirements deteriorate sharply when critical organs related to security are discussed, since testing procedures are not set up … Therefore the security of voting machines is far from assured. The State does not seem to have realized how difficult it is to secure a computer system and verify that there is no fault at all' (Enguehard 2007, my translation). Something similar happens in Belgium, where the list of requirements is very short. Consequently, ODIHR stressed in 2007 that 'the tests should cover all aspects of the system. A detailed comprehensive list of required criteria should be developed as the basis for testing' (OSCE/ODIHR 2007c: 11).

Recent e-voting implementations tend to use the so called End-to-End (E2E) Verification, an audit of the e-voting system that relies upon cryptographic protocols and allows external auditors to verify the correct performance of the whole application, including all steps. The system would be laid out in such a way that external auditors could understand and monitor its functions while maintaining and not disturbing the ordinary roles of internal managers. Norway, for instance, used this kind of technical structure during the internet voting trial conducted in ten municipalities in September 2011. While theoretically optimum, its actual usefulness probably depends on the number of assumptions that auditors have to accept: that is to say, E2E verification might only be feasible provided some preliminary conditions are met, and therefore such pre-requirements might jeopardize the actual comprehensiveness of this mechanism.

### *Independence*

Any e-voting project normally includes its own audit protocol. Actually, these internal verification mechanisms are strategic components of the overall structure because they actively detect gaps. Auditing is therefore a normal quality guarantee in any computerized framework, but this type of audit is not useful for our purposes. From the point of view of an electoral observer, internal audits may be interesting data, but they always need some supplementary external supervision. Such internal controls can conduct their own technical verification, but what observation requires is an external assessment of whether or not the internal protocol used by the provider is well designed, covers all relevant issues and is fully implemented. As stated by the OAS, 'in order to guarantee that the final vote tally reflects the will expressed by the voters, the results may be submitted for a security audit conducted by an independent outside party' (OEA 2010: 27).

If we are pursuing external verification, independence obviously becomes a key word. Those people or entities conducting an external audit should be able to prove that they are not subject to influence by the e-voting supplier. Theoretically, it seems easy to meet this requirement, but implementation often becomes problematic. Entities that are presented as independent are actually hired and paid by the provider, or by the electoral authorities. Others claim to be independent because they are not included in the electoral department, but they belong to the overall administrative sphere, and, despite their professional performance, it is worth wondering whether such links may undermine their independence and ability to analyze freely the e-voting project.

Venezuelan reports provide interesting data regarding the issue of independence. For instance, in 2006 some audits were coordinated by professors from the Universidad Central de Venezuela (EUEOM Venezuela 2006: 62). Although national and international observers, as well as representatives of each candidature, attended such audits, what is really important from our point of view is the actual level of independence of this academic pool, and the report does not provide further information with which to assess this. Something similar also happens in Coahuila, a pioneer e-voting State in Mexico, where the EMB intends to enhance citizen confidence by recruiting academics from local universities.

It is worth noting that the use of academics does not necessarily guarantee independence. Behind a neutral appearance, pretending only to foster scientific improvements, there are private and/or economic interests that can jeopardize supervision methods. However, other solutions also have similar problems. In France and Belgium, for instance, private auditors are selected and even paid by providers themselves, and it would be worth asking to what extent this relationship is able to generate a reliable outcome.

Election authorities in other countries commission single persons or entities to conduct given audits, but again independence might be compromised. Norway, for instance, adopted a proactive transparent policy that even included spontaneous E2E verifications, but its authorities also hired some players, like IFES, to carry out different assessments. Given that they are being paid, it is legitimate to have some initial doubts as to the impartiality of such auditors. Estonia follows a similar pattern because its authorities hired both an international audit firm and an IT expert to carry out the audits.

Belgium takes an interesting approach: the commissioning of an audit to be conducted by an administrative body. There is a formal certification assumed by private entities, but there also is a supplementary control conducted by the so-called Collège d'Experts, an ad-hoc committee appointed by the parliamentary chambers from among their internal staff, normally from the Information Technology (IT) departments. The Collège is given access to all relevant information, including the certification report that is only delivered to the Ministry and the provider, and it issues a report fifteen days after the elections. Regardless of the professional behaviour of its members, it is worth asking to what extent such a body can meet the independence requirement. Despite the functional autonomy that it is accorded, it still is an internal branch of the public administration and some details even endanger such theoretical independence.

As recommended by the ODIHR assessment mission, the tasks of the Collège should be enhanced because right now 'experts are neither paid for this task, nor relieved from their day-to-day duties during this period' (OSCE/ODIHR 2007c: 12). Moreover, 'the NGO [Pour une Ethique du Vote Automatisé] PourEVA raised concerns over the system of nomination of the College of Experts, underlining that the Chambers of Parliament are also the ultimate judges of the validity of the election of their own members' (OSCE/ODIHR 2007: 12). Finally, the Collège itself has asked for a more practical independent framework. In its last report, it states again that 'its mission generates both real responsibilities and a significant surplus of work. Considering that most experts are usually officials of their respective parliamentary assemblies, it is essential that such institutions (and especially their internal administrations) are aware of the importance and the time required for their mission when selecting experts' (Collège d'Experts 2010: 6, my translation).

To conclude this section, it should be noted that it is extremely difficult to find a fully independent actor. Regardless of particular professional behaviour, each profile has features that can jeopardize the activity. Academia, individual experts, private auditors or administrative bodies might not meet, for different reasons, the independent profile that any e-voting project should look for. Perhaps the best option would be to assume that there are no fully independent players and, having assumed this fact, determine how to achieve the same goal by other means. From this point view, a reasonable solution might be plurality.

### *Plurality*

Plurality is closely linked to transparency. Even if electoral authorities manage to submit the e-voting system to a fully independent external auditor, the outcome will probably be insufficient from a democratic point of view. Apart from the professional reliability or unreliability of an external auditor, the main weakness of any e-voting system, as previously noted, consists in the difficulty for average citizens to conduct their own verification. This difficulty cannot be overcome where there is only one auditor, since all voters are forced to have confidence in one single person or entity. Citizens will probably discuss the actual independence and reliability of the auditor; there is unlikely to be common acceptance; and therefore a single auditor, even if highly qualified, is unable to achieve the main social and legal goal of his or her task: that is to say, a new way to generate citizen confidence in the e-voting system.

Plurality might thus be a good solution. There would be a pool of independent and external auditors, each one appointed by different means and by different stakeholders. In the optimum framework, specific appointments would not even be needed since full disclosure of all relevant data would empower every expert to perform his or her own verification. This plurality would provide citizens with a wide range of opinions about the e-voting project, and citizens would not have to blindly believe either electoral authorities or a single person or entity. The OAS Manual also stresses the same idea: 'It is important for the OAS/EOM to observe that evaluation and auditing systems are applied in electoral technology projects, especially that the various political actors participate.' (OEA 2010: 24; my italics; see also 10)

The EU Handbook also includes this kind of reference: 'Political contestants (parties, candidates and supporters of positions on referenda) have vested interests in the electoral process through their rights to be elected and to participate directly in government. They therefore should be allowed to monitor all processes related to elections and observe procedures, including among other things the functioning of electronic and other electoral technologies inside polling stations, counting centres and other electoral facilities, as well as the transport of ballots and other sensitive materials.' (European Commission 2008: 198; my italics) Another guideline stresses the same criteria for individual citizens.

Although this guideline intends to encompass a wide range of data disclosed to such stakeholders, the wording might also be understood narrowly, as limiting their oversight only to what happens inside polling stations. Voting machines provide little or no evidence of their correct performance inside polling stations, and therefore sound oversight should also include previous stages.

A quick overview of some e-voting examples will show us cases where providers disclose relevant data to anybody once an NDA is signed. Theoretically, there would be a plurality of stakeholders conducting audits, although, as already noted, NDAs can also become a master key that limits the effectiveness of such plural auditors.

Belgium intends to meet both independence and plurality by disclosing the source code to political parties before the election day. Although there also is a formal certification procedure, assumed by private audit firms, political parties do receive the source code and they may carry out their own audits. Given that political parties are the main players within this competition, and taking into account that they pursue contradictory interests, disclosing this critical data to all of them clearly meets the principle of plurality. Venezuela seems to pursue the same goal, as reported by the OAS mission in 2006: 'During the pre-election phase, the CNE audits the most critical components of the process. These audits have the active participation of technicians from the contesting candidates, who endorsed the systems, as well as the accompaniment of the EOM / OAS. The timing and nature of the audits were previously agreed between the parties and the CNE'(OEA 2008: 36 and 39, my translation).

Following this path, the full disclosure of all relevant data would definitively consolidate the principle of plurality, since anyone, even without a prior official authorization, could analyze the e-voting system. Belgium approaches this scenario by disclosing the source code after the election day. It is uploaded to a website and everybody can analyze what previously was known only by political parties, formal auditors and the Ministry. Norway is also taking a step forward by publishing all technical data with no restrictions. There is a general licence limiting authorized actions to the audit itself and excluding profit-making activities, but nothing else. In conjunction with the E2E verification, this framework meets both the principles of comprehensiveness and of plurality.

### *Transparency*

Last but not least, a further important principle is that of transparency. In this case, transparency does not mean the transmission of technical data; this issue has already been addressed in the first section, when talking about the integrity of data. Nor does transparency mean free and universal access to technical data, as we are assuming that trust by proxy, independence and also plurality could be met without providing information to everybody. However, what it seems non negotiable is that the results generated by the different audits implemented are published. If these reports remain secret, as happens in some countries, an average citizen will have no way to assess whether the audits have been correctly implemented and subsequently whether the e-voting system is performing correctly. Once it is assumed that citizens have to trust third parties, the secrecy of these reports will generate again the blind faith that we are trying to avoid. Negative conclusions, for instance, will never be published and citizens will never receive a balanced assessment.

As mentioned, this dark scenario is ordinary practice in some countries. In Kazakhstan, for instance, the opacity encompasses both the reports and the previous guidelines: 'The certification documentation for the most recent changes to the system prior to the 2007 election make reference to system requirements set out in a document of the National Security Committee (KNB). This is not a public document. The Central Electoral Commission (CEC) was unable to provide the OSCE/ODIHR EOM with any documents

regarding the KNB requirements, and the KNB did not reply to a written request for information.' (OSCE/ODIHR 2007: 13)

In France and Belgium, certification reports are handled in a very restrictive way, and this has even provoked formal recommendations by international electoral assessment missions. France, for instance, 'informed the OSCE/ODIHR EAM that according to a 26 January 2006 recommendation by the Commission d'accès aux documents administratifs, an official consultative board, the certification reports could not be provided to the public on the grounds that industrial secrecy and the proper implementation of the elections could be compromised' (OSCE/ODIHR 2007a: 11). The latter includes the Collège d'Experts within the limited pool of stakeholders who receive this document, but political parties, electoral observers as well as individuals remain excluded.

Following other reports from ODIHR missions, it is worth noting that Estonia also has several restrictions. In 2007, for instance, the final report listed the following documents as being kept secret: the results of informal reviews of the software by representatives of banks, universities and state officials at various times; a report issued by KPMG Baltics, an audit firm; and probably the audit of the source code conducted by an independent expert (see OSCE/ODIHR 2007b: 15-16).

Surprisingly, certain stakeholders sometimes stop the transmission of data, the citizenry does not receive information, and only a selected pool of players can meaningfully assess the e-voting project. In the Venezuelan 2006 Presidentials, for instance, 'the conclusions of the audits were not always communicated by the leadership of political parties to the general public or the media during the election campaign. Thereby, doubts persisted regarding the reliability of the system among the citizenry' (EUOEM Venezuela 2006: 21).

## Voter Verified Paper Audit Trail (VVPAT)

As stated above, paper trails could become a good solution to provide enough evidence about the performance of an e-voting system. I include this option within a separate section because this kind of audit is completely different to those already analyzed. It is not computer-based, and therefore a voting receipt is something that can be handled by every voter, even without specific knowledge. However, this simplicity does not exclude other problems that should be taken into account. The layout of the paper trails, their use and the legal framework in case of contradictions are three aspects that can generate different challenges.

Regarding the layout, some usability issues are unavoidable. The voter receipt has to be read and monitored by the voter, but this task will require specific layouts adapted to every sort of citizen, including those impaired or somehow uncomfortable with managing such devices. Moreover, the design of the voting machine may differ a lot from one country to another. While some solutions include a printer and a receipts' box that are embedded into the voting machine itself (thereby avoiding any physical manipulation by the voter), other options use a separate traditional ballot box and voters have to transport the receipt from the voting booth to this ballot box. Venezuela and Coahuila (Mexico) are using this second option, and the Mexican capital (Mexico DF) is using the first one.

There also are some countries that have implemented unusual VVPATs. In Belgium, for instance, election authorities commissioned an academic consortium to assess its current e-voting solution and suggest how to update it. The final report listed five options, but preference was given to a system where the voter, having selected his or her candidature with a voting machine, received a ballot with two sections to be inserted into the automatic ballot box. One section is electronically based, but the other one is human readable and therefore assumes the role of a paper trail.

Norway is also implementing paper receipts in new formats. Taking into account that there will be internet voting from non-supervised environments, the delivery of paper trails with the votes' value is critical and may contraven international standards. However, the Norwegian authorities intend to overcome such barriers. First of all, voters have the opportunity to revoke their votes, and therefore the receipt might not be sufficient evidence for third parties—something international standards seek to avoid (see CoE 2004: n. 51). Second, complex cryptographic measures will allow the delivery of receipts with the content of a given vote to the relevant voter without linking his or her identity with a single ballot (see Gjøsteen 2011).

The introduction of voting receipts does not mean that they will always be counted at the end of the election day. Some electoral authorities only foresee such recounts in the case of specific complaints. This is the case, for instance, in Coahuila, Mexico. Moreover, as seen in Venezuela in 2005 and 2006, this parallel recount can have an impact on citizens' confidence. In 2006, the paper-based recounts occurred in 54% of polling stations, much more than in the previous year. From a statistical point of view, this decision made no sense, since fewer percentages would have provided sound evidence of the correct performance of the electronic tally. However, the referendum in 2005 raised some concerns about the centralized procedures used to select which polling stations would be submitted to a second recount (see Hausmann and Rigobon, 2004) and, due to this sort of criticism, election authorities decided to increase the number of polling stations and decentralize the procedure so that each voting centre, with several polling stations in it, would decide which stations would use paper trails for the second recount.

Finally, it is worth asking what the legal solution will be to a scenario that is to some degree inherent in the voting trails themselves. If there is a chance to compare electronic results with the paper based recount, discrepancies could be discovered and legislation would have to be used to determine which outcome should be taken into account: the electronic one, the one provided by the receipts, or none. The decision is even more important if we realize that this is not merely a theoretical scenario.

In the 2006 Presidentials in Venezuela, for instance, the OAS attested that 'in 92% of observed polling stations audit results matched the results of the Tallying Record printed by the voting machine' (OEA 2008: 47). This means that up to 8% of polling stations were not be able to match electronic and paper based recounts. Paradoxically, the report of the EU mission provides different figures because it includes a small 0.19% of discrepancies (see EUEOM Venezuela 2006: 24), mainly due to a mishandling of blank ballots by the official boards of several polling stations.

Regardless of the importance of such discrepancies, both reports do not focus their attention on the legal framework regarding these cases, perhaps due to the nationwide tallying of

votes and the absence of close results. However, in local elections, one single ballot may become essential to decide the winner, and therefore rules governing discrepancies should be clearly set up.

## Concluding Remarks: Things to Do and Things Not to Do

Electronic voting is not a merely cosmetic electoral change. Nor is it a mere electoral update. It entails important challenges that encompass different voting issues, such as the principles of secrecy, freedom and universal franchise. Electoral observation methodologies should also adapt their conventional patterns to this new framework taking into account the specific features of electronic devices. Therefore full awareness is the first goal that electoral authorities have to meet. They have to assume that electronic voting is a major innovation that will have an impact in several electoral spheres. Failure to do so could lead to this voting channel being implemented wrongly, and to greater problems in the future.

A common problem that makes it difficult for election authorities to comply with the goal of full awareness is the lack of in-house expertise. Election authorities may accept vendors' marketing strategies without further legal, social or technical assessment, and there may be no internal capacity with which to balance the arguments provided by suppliers. If e-voting were finally implemented, vendors might assume a central role and election authorities lose their primary task, the control of the electoral procedure. They will not fully understand what is going on and will not therefore be able to conduct sound supervision.

From a perspective focused on electoral observation issues, the opacity of e-voting poses an initial barrier. Given that the voting channel is based on computerized means, a non-specialist observer is not able to understand how it works. Specific knowledge is needed and therefore average citizens and observers are excluded from such observation tasks. Taking into account this problematic scenario, election authorities should look for appropriate measures to compensate for such weakness: that is to say, actions that would balance a framework where the control over the electoral procedures has been transferred to a pool of specialists.

Trust by proxy is a reasonable way to achieve such a goal, but the proxy solution has to be based on a procedural approach. Given that audits, certifications and other similar controls will necessarily include a complex technical basis, citizens will not understand the relevant outcomes but could assess whether the procedure adopted to conduct such controls is sufficient from a democratic point of view. Therefore election authorities should adapt their observation protocols to include a two-stage methodology. The first stage would include computer experts, who might also be electoral observers, and the second stage would include the remaining stakeholders, who would have to ensure, through a procedural assessment, the integrity and accuracy of the first group.

There are a couple of principles essential to such a procedural assessment: the integrity of the data disclosed to the auditors; the comprehensive scope of such controls; the independence, number and ways of appointment of the stakeholders who assume these tasks; and, finally, how the relevant outcomes are delivered to the citizenry.

Integrity of data means that computer experts must receive all the relevant information needed to conduct their technical task. Given that suppliers might be reluctant to make such a disclosure, election authorities should establish clear rules regarding which data are actually needed and which are not.

Audits, certifications and tests should be comprehensive and cannot exclude given components of the voting system. In this case, election authorities should be aware that e-voting applications are normally the result of mixing several technical components, but this complexity cannot lead to a splitting of these elements and a review of only the core of the e-voting system. Every device that could affect the performance of the e-voting application needs to be tested.

Given that we are assuming that e-voting electoral observation will be based on a proxy solution, the independence of the players to be trusted is essential. Moreover, once we accept that no player can provide a profile of full independence, plurality also becomes important, as citizens should not have to trust a single person or entity. Election authorities should establish clear rules regarding the appointment of auditors so that both independence and plurality are met. Full disclosure should also be assessed as an optimum framework to involve many players.

The proxy method also requires that the outcomes of technical reviews are not kept secret, as sometimes happens. If the relevant final reports are not published, an approach based on trust by proxy makes no sense, because the citizenry will not receive any data. There will be no debate and potential weaknesses will not be made public. Election authorities should therefore require the publication of such final output regardless of the potential opposition coming from vendors and even from auditors themselves.

Finally, VVPATs might become in some cases a good means of enhancing citizen confidence without proxy solutions. But it is worth noting that paper trails also have other problems with their implementation. The layout, their actual use, and the legal framework concerning potential discrepancies are issues that need to be correctly addressed for the proper use of paper receipts. Therefore, election authorities should be aware that the introduction of VVPATs as such would only be a correct solution provided there is a sound technical and legal framework that foresees and addresses the risks.

## References and Further Reading

Aaltonen, Jussi, 'Electronic Voting Pilot in 2008 Municipal Elections', Third meeting to review developments in the field of e-voting since the adoption of Recommendation Rec (2004)11 on legal, operational and technical standards for e-voting (Strasbourg: Council of Europe, 2010), available at http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E- voting%202010/Biennial_Nov_meeting/GGIS%282010%2914_Finland%20e- voting%20report%20E.asp#TopOfPage , accessed 26 November 2011.

Barrat Esteve, Jordi, 'Observació electoral i vot electrònic', Revista Catalana de Dret Públic, 39(2009), pp. 277-296.

Barrat Esteve, Jordi, 'El voto electrónico ante intereses contradictorios: La razón comercial contra el principio democrático. A propósito de los compromisos comerciales de confidencialidad (CCC)', Democracia digital, participación y voto electrónico (València: CEPS, 2010), pp. 57-69.

Bull, Christian, 'Safety first! Verifiability in the e-vote 2011-system', The Norwegian E-voting Conference (Oslo: Ministry of Local Government and Regional Development, 2011), available at http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/e_vote_conference/ChristianBull.pdf , accessed 30 November 2011.

Collège d'Experts, Rapport fait au nom du Collège d'Experts chargés du contrôle des systèmes de vote automatisés Sénat et Chambre des représentants de Belgique, July 6th 2010 (extraordinary session), available at http://www.poureva.be/IMG/pdf/53K0014001.pdf , accessed 8 November 2011.

Council of Europe (CoE), Recommendation Rec(2004)11 on Legal, Operational and Technical Standards for e-Voting (Strasbourg: Council of Europe (CoE), 2004), available at https://wcd.coe.int/ViewDoc.jsp?id=768793, accessed 8 November 2011.

Council of Europe (CoE), E-voting handbook. Key steps in the implementation of e-enabled elections (Strasbourg: Council of Europe [CoE], 2010), available at http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/ID10322%20GBR%206948%20Evoting%20handbook%20A5%20HD.pdf, accessed 8 November 2011.

Council of Europe (CoE), Guidelines on transparency of e-enabled elections (Strasbourg: Council of Europe [CoE], 2011), http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf , accessed 8 November 2011.

Council of Europe (CoE), Certification of e-voting systems. Guidelines for developing processes that confirm compliance with prescribed requirements and standards (Strasbourg: Council of Europe [CoE], 2011a) http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E- voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf , accessed 8 November 2011.

Enguehard, Chantal, 'La sécurité des machines à voter n'est pas vérifiée: c'est prévu!', Agoravox, http://www.agoravox.fr/actualites/citoyennete/article/la-securite-des-machines-a-voter-n-22655, accessed 8 November 2011.

European Commission, Handbook for European Union Election Observation, Second Edition, (Brussels: European Commission, 2008), available at www.eueom.eu/index.cfm?objectid=535F9509-2872-11DF-ACBDE2808AECDBDC, accessed 8 November 2011.

Eueom Venezuela Final Report. Presidential Elections. Venezuela 2006 (Caracas: European Union Election Oservation Mission [EUEOM], 2006), available at http://www.eueomvenezuela.org/pdf/MOE_UE_Venezuela_2006_final_eng.pdf , accessed 8 November 2011.

Eueom Peru Final Report. Second Round of the Presidential Election. June 2011 (Lima: European Union Election Oservation Mission [EUEOM], 2006), available at http://www.eueom.eu/files/pressreleases/english/EUEOM_Peru_2011_Final_Report.pdf , accessed 10 November 2011.

Gjøsteen, Kristian, The Mathematics of Internet Voting (Oslo: Kommunal- og regionaldepartementet, 2011), available at http://www.regjeringen.no/upload/KRD/Prosjekter/e- valg/e_vote_conference/Gjosteen_evalgskonferanse.pdf , accessed 10 November 2011.

Government of Norway, Ministry of Local Government and Regional Development, 'About the license', at http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/source-code/about-the-licence.html?id=646006, accessed 30 November 2011.

Hausmann, Ricardo, and Rigobon, Roberto, 'En busca del cisne negro: Análisis de la evidencia estadística sobre fraude electoral en Venezuela, 2004', available at http://www.sumate.org/Elecciones/2004Revocatorio/20040903_analisis_evidencia_estadistica_fraude_ electoral_venezuela_haussman_rigobon.pdf, accessed 8 November 2011.

Krimmer, Robert, and Volkammer, Melanie, 'Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting', Working Paper Series on Electronic Voting and Participation, Nr. 01/2006, available at www.e-voting.cc/files/Working-Paper-1-2006, accessed 8 November 2011.

Organización de Estados Americanos[OEA], Informe final de la misión de observación electoral de la OEA sobre las eleciones presidenciales celebradas en Venezuela el 3 de diciembre de 2006 (Washignton DC: Organization de Estados Americanos [OEA], 2008), available at http://www.oas.org/sap/docs/DECO/informemoevenezuelaeleccionespresidenciales2006.pdf, accessed 8 November 2011.

Organización de Estados Americanos[OEA], Observing the Use of Electoral Technologies. A Manual for OAS Electoral Observation Missions (Washington DC: Organization de Estados Americanos [OEA], 2010), available at http://www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf, accessed 8 November 2011.

Organization for Security and Co-operation in Europe (OSCE), and Office for Democratic Institutions and Human Righs (ODIHR), Republic of Kazakhstan. Parliamentary Elections 18 August 2007. OSCE/ODIHR Election Observation Mission Report (Warsaw: Organization for Security and Co-operation in Europe [OSCE] and Office for Democratic Institutions and Human Righs [ODIHR], 2007), available at http://www.osce.org/odihr/elections/kazakhstan/28438, accessed 8 November 2011.

Organization for Security and Co-operation in Europe (OSCE), and Office for Democratic Institutions and Human Righs (ODIHR), France. Presidential Election. 22 April and 6 May 2007. OSCE/ODIHR Election Assessment Mission Report (Warsaw: Organization for Security and Co-operation in Europe [OSCE] and Office for Democratic Institutions and Human Righs [ODIHR], 2007a) http://www.osce.org/odihr/elections/france/27768, accessed 8 November 2011.

Organization for Security and Co-operation in Europe (OSCE), and Office for Democratic Institutions and Human Righs (ODIHR), Republic of Estonia. Parliamentary Elections. 4 March 2007. OSCE/ODIHR Election Assessment Mission Report (Warsaw: Organization for Security and Co-operation in Europe [OSCE] and Office for Democratic Institutions and Human Righs [ODIHR], 2007b), available at http://www.osce.org/odihr/elections/estonia/25925, accessed 8 November 2011.

Organization for Security and Co-operation in Europe (OSCE), and Office for Democratic Institutions and Human Righs (ODIHR), Belgium. Federal Elections 10 June 2007. OSCE/ODIHR Election Assessment Mission Report (Warsaw: Organization for Security and Co-operation in Europe [OSCE] and Office for Democratic Institutions and Human Righs [ODIHR], 2007c), available at http://www.osce.org/odihr/elections/belgium/28213, accessed 8 November 2011.

Organization for Security and Co-operation in Europe (OSCE), and Office for Democratic Institutions and Human Righs (ODIHR), OSCE/ODIHR Discussion Paper in Preparation of Guidelines for the Observation of Electronic Voting (Warsaw: Organization for Security and Co-operation in Europe [OSCE] and Office for Democratic Institutions and Human Righs [ODIHR], 2008), available at http://www.osce.org/odihr/elections/34725, accessed 8 November 2011

Stonestreet, Jonathan, 'Finalités de l'observation des élections dans le vote électronique' in Laurence Favier (dir.) La démocratie dématérialisée. Enjeux du vote électronique (Paris: Seuil, 2011), pp. 75-89.

Tarvainen, 'Tapani Salassapitosopimuksen anatomia' (Helsinki: Electronic Frontier Finland [EFFI], 2008), available at http://www.effi.org/blog/2008-03-20-Tapani-Tarvainen.html, accessed 8 November 2011.

TietoEnator, Salassapitosopimus: Non-disclosure Agreement (Helsinki: TietoEnator, 2 February 2008), available at http://www.effi.org/blog/2008-03-20-Tapani-Tarvainen.html, accessed 25 November 2011.

Vähä-Sipilä, Antti (ed.), A Report on the Finnish E-Voting Pilot (Helsinki: Electronic Frontier Finland [EFFI], 2009), available at http://www.effi.org/blog/2008-03-20-Tapani-Tarvainen.html, accessed 8 November 2011.

Venice Commission, Report on the Compatibility of Remote Voting and Electronic Voting with the Standards of the Council of Europe (Venice: Venice Commission, 2004), available at http://www.venice.coe.int/docs/2004/CDL-AD(2004)012-e.pdf, accesed 8 November 2011.

Whitmore, Keith, 'Information Report on the Electronic Voting in the Finnish Municipal Elections', at 'The Congress of Local and Regional Authorities', https://wcd.coe.int/ViewDoc.jsp?id=1380337&Site=Congress, accessed 26 November 2011.