ADAPTING ELECTION OBSERVATION METHODOLOGY TO THE OBSERVATION OF E-VOTING – THE BIRTH OF "E-OBSERVERS"

By
Agnes Doka

Submitted to
Central European University
Department of Public Policy

In partial fulfilment of the requirements for the degree of Master of Arts

Supervisor: Professor Kristina Irion
Co-supervisor: Marie-Pierre Granger

Budapest, Hungary
2011

Acknowledgments

I would like to express my sincere gratitude to my supervisor Professor Kristina Irion, and to my co-supervisor Professor Marie-Pierre Granger for their continuous support, professionalism and flexibility. Their feedback and patience helped me throughout my research. I would also like to thank Professor John Harbor, for his invaluable feedback on drafts and enormous flexibility.

Abstract

An increasing number of countries use or plan to use different electronic voting methods and technologies. Issues of transparency, verifiability, security and certification of e-voting systems are keenly debated among experts, academics and electoral bodies alike. These issues are also having an impact on international observer organisations, who are facing challenges with the observability of e-voting and the need to tailor their traditional observation methodology to the observation of e-voting. In order to identify the most pressing issues and challenges in the adaptation of observation methodology to e-voting, this paper maps e-voting trends and provides an overview of the framework for the observation of e-voting. The paper also reflects on the findings of three EU Election Observation Missions (Venezuela 2005, 2006, and Bhutan 2008) to assess the degree to which these missions were able to adopt their traditional observation methodology to the e-voting challenge.

Table of Contents

Introduction

Democratic elections are cornerstones of democracy building and when undertaken in a transparent and credible way, elections can contribute to peace and stability. It is therefore absolutely crucial that elections are seen as fair and accurate. Observation and independent evaluation of election processes are methods which support these aims and therefore they play an extremely important role in providing "trust" in the election process.

For many decades elections have been relying on paper-based voting which is costly, (printing and logistics), prone to cheating, but provides ample opportunity for observation throughout the voting process and the aggregation of the results. The emergence of different electronic voting methods not only present challenges to governments, policy makers and the electorate, but also poses challenges to observer organisations and their traditional election observation methodology. Traditional, or paper-based voting and counting can easily be observed: for example in Uganda' 2006 elections after the close of the poll voters and onlookers of the whole village counted each and every vote cast out loud.

The use of new information technologies and the introduction of different electronic voting tools *(Direct Recording Electronic devices, (DRE), digital and optical scanning machines, kiosks, Internet, telephone voting)* however, have not had a favourable impact on the voting public.. Largely due to the fact that electronic machines diminish transparency during both the voting process and the transfer of the election results, as data processing happens inside the "black box".

The drawbacks of using e-technology in elections are many and spread almost evenly, from the design of the e-voting process, to the tallying of the result. Obviously, voters have difficulty in trusting machines, as machines can break down and can be altered and manipulated - in many ways. Trust in election processes - and in the case of e-voting, trust in machines - is crucial in shaping the public's perception of the functioning of democracy, and the acceptance of the results. Even without the use of machines the loss of trust by the public in the election result can cause havoc on democratic establishments, as happened in the Presidential election in Kenya in 2007 and in the most recent presidential election in Ivory Coast, 2010.

Technical challenges can impede all kinds of elections and involve the counting, aggregation and publication of results, as it was observed in paper-based elections (Ethiopia 2005, Yemen 2006, Nigeria 2002, 2007, and Kenya 2007) [1]. Electronically-enabled elections, or the application of e-voting have additionally raised serious concerns in the past few years (Meyer-Resende 2008, 3). These concerns are born from the lack of observation of the aggregation of results between the polling station and regional levels, and sometimes the limitation of access to all levels of tabulation centers by local election officials. If there is already an access and follow-up problem to results in traditional elections, the use of machines will definitely not make this process more transparent.

Additionally, experts and scholars are deeply divided over the observability of various aspects of new electronic voting techniques. Discussions revolve around security and verifiability issues. The flagship of

[1] Elections observed by the author

the verifiability issue is the provision of Voter Verifiable Paper Audit Trail (VVPAT), its prominent proponents include: Rebecca Mercury, David L. Dill, (works cited in later chapters), while Michael I. Shamos sees the alternative to paper trails in audits and open source software.[2] (Shamos 2004, 14) International organisations in their relating documents also tend to give favour to VVPAT voting computers. (Enguehard and Graton 2008, 6)

Those who support the introduction of e-voting technologies, argue that its benefits justify its use: flexibility in access provide participation for so far excluded voters, such as people being abroad on Election Day or being unable to physically access a polling station. The other often cited benefit is the speedy and more reliable tabulation of the result (often machines tally the results automatically). Some machines also prevent unintentional invalid vote casting (a major problem in developing countries' elections). Finally, election officials argue that electronic voting may be the cheapest, quickest and most efficient way to administer elections – as a kind of "investment" in the future. While the use of technology might simplify the administration of the election, and cost savings from the reduction of paper use should accumulate over time, the cost of online voting varies depending on the type of system employed and the type of security used. (Oostveen and Besselaar 2004, 73)

Since the late 1990s, governments which refused to invite reputable international observer organisations to monitor their elections have come under suspicion. As: "International elections observers are now present at more than four out of every five elections in the developing world." (Hyde 2009, 1) International organisations, like the European Union (EU), one of the

[2] See the discussion on open source software in details in sub-chapter 4.1.2

main organisations in the field of observation, deploys observers for the following reason:

> "Election observation is a vital part of the European Instrument for Democracy and Human Rights, which express the EU's intention to promote democracy, human rights and the rule of law worldwide. Since 1993, the EU has conducted more than 110 observation missions. (EC EuropeAid Development Cooperation homepage)

Election observation missions (EOMs) – even just by their presence - can contribute to public confidence, deter fraud, and strengthen respect for human rights and the rule of law. All the states, supranational organisations, IGOs and NGOs program their observation missions to achieve these goals. However, the scope of election observation depends on resources, training of observers and the local legal framework, all of which might limit the participation of observers.

Additional to the European Union, there are several organizations carrying out international election assistance and observation missions to contribute to democracy building. These organizations include the Organisation for Security and Co-operation in Europe (OSCE) as well as the Carter Center, the National Democratic Institute (NDI), the International Foundation for Elections Systems (IFES), the African Union, the Asian Network for Free Elections (ANFREL), and the Organisation of American States (OAS).The European Parliament and national governments are also deploying election observers upon invitation from the host government. All observation missions adhere to the Declaration of Principles for International Election Observation, commemorated at the United Nations in 2005. Accordingly organisations only send missions if they deem it advisable and feasible, based on whether a mission can fulfil its mandate and if yes, to what degree. Each of these

organisations aims to apply consistent observation methodology throughout the observation process: they plan for the long term observation of all major events before the actual Election Day (campaign period, registration of voters (if applicable) and the media campaign. The ultimate purpose of an observation mission is to assess to what extent an election complies with local and international regulations in its execution. International observers are non-interfering, impartial and independent in their findings and conclusions. (EU EOM Ethiopia homepage, 2010)

This paper aims to include all significant observer organisations approaches to e-voting observation, but focuses on the lead organisation, the European Union. The reason for this, is its contribution to the work of e-voting development and observation: The Council of Europe was the first one to publish a comprehensive set of guidelines for e-voting in its Recommendation (REC(2004)11) that is the only set of agreed guidelines by any organisation up to date. While the EU has been continuously working on framing and focusing on challenging issues of e-voting among its member states, it also anticipates being invited to an increasing number of elections as an observer outside the EU that will use e-voting technologies. There is a huge volume of research papers aimed at addressing a range of challenges in different e-voting practices; they sometimes touch upon the issue of observability. However, to my knowledge, there is no study so far that discusses all the main challenges posed by e-voting for election observers. The same can be said about observer organisations: while several have published handbooks on e-voting, these are mostly practical guides or complicated interpretations of

the 2004 Recommendation, without addressing the fundamental, but ever-evolving issues of observing e-voting.

Therefore in this thesis I identify the most challenging aspects of the observation of e-voting as at the moment it is unclear what observer organisations should focus on when developing their guidelines and methodology for the observation of e-voting. I aim to determine why and what needs to change in adopting election observation to the observation of e-voting.

The thesis structured as follows: Chapters 1 & 2 will give an introduction to e-voting and an overview of the frameworks for the observation of e-voting.

Chapters 3 & 4 identify the most challenging aspects of the observation of e-voting at the moment it is unclear what observer bodies should focus on when developing their handbooks and guidelines for the programming of observation missions. They will also examine the three main problematic areas of election observation where a coherent approach to election monitoring, framework and programming is needed. These three main areas are: the observation of legal framework, issues of e-voting verifiability and the issue of security.

Chapter 5 will provide conclusions and some recommendations focusing on the upfront planning of observability of e-voting systems, the minimum standards required and finally the necessary resources and skills for success.

This paper uses qualitative research methods in comparatively analysing several international documents, policy papers, academic research papers,

Final reports of the three EU Election Observation Missions (EOM) to Venezuela (2005, 2006) and to Bhutan (2008) were e-voting has been observed. Finally, I have also relied on my field experience as an election observer.

I hope that my work contributes to the development of an aligned approach to principle setting in e-voting observation.

Chapter 1 – E-voting: Cashing in on the Promise

This chapter overviews the different types of e-voting and identifies trends in their use; also identifies countries which have abandoned e-voting after trials. The purpose is to see how many countries "cash in" on e-voting promoters and sceptics arguments, and identifies the use of Voter Verified Paper Auditable Trail (VVPAT) which is presently seen as the only safeguard to verifiability.

1.1 Types of e-voting

There are different e-voting methods, categorized depending on location (whether machines are used in controlled or non-controlled environment), on the type of machine (registering, or simply forwarding data), or on the provision of paper records. Within a controlled environment, e-voting machines may be coupled with either paper issuing methods (Voter Verifiable Paper Audit Trail - VVPAT), or electronic transmission devices. To group different types of e-voting methods, this paper follows the categorization of the new E-voting handbook, issued by the Council of Europe in 2010. These categories are the following: 1. Direct Recording Electronic computers (DREs), 2. Digital/optical scanners, 3. Machines used for polling station data recording, and 4. Internet. While the Internet can be used in a polling station setting (kiosk) allowing vote casting to take place in a controlled environment, present practice shows that legally binding internet based ballot casting in Austria, Australia, Canada, Estonia, France, Japan, and in Switzerland (ACE Project 2011, 5) is used for absentee voting in an uncontrolled environment,

therefore it is not in the scope of election observation and will not be assessed in this paper. Other remote voting methods (postal voting, phone, are also excluded from the analysis due to the lack of observability and obvious lack of privacy in casting the vote. However, as a latest development, Norway is piloting Internet voting in uncontrolled environments in 2011, and has invited the OSCE to observe these upcoming elections.[3]

1.2 Trends in e-voting

The main purpose of this sub-chapter is to map the latest stage of application of different methods of e-voting, as at the development of this thesis there was no consistent data available. Table 1 below is a compilation reflecting available data until March 2011. (See Table 1.)

Presently there are 16 countries which are using different types of electronic voting machines with legally binding outcomes: Australia, Austria, Belgium, Brazil, Canada, Estonia, France, India, Japan, Kazakhstan, Peru, Russia, Switzerland, United States of America, United Arab Emirates, and Venezuela. (ACE Project 2011, 6) Several other countries are experimenting with trials and use e-voting techniques parallel to traditional balloting, with non-legally binding outcomes. These countries are: Argentina, Azerbaijan, Belarus, Bulgaria, Chile, Czech Republic, Finland, Greece, Italy, Latvia, Lithuania, Mexico, Nepal, Nigeria, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Africa, Spain, South Korea, and Sweden. (Tiresias.org, 2011) Finally, Germany, Ireland, United Kingdom and the Netherlands have terminated their e-voting projects. (E-voting CC. 2010)

[3] Press release, Ministry of Local Government and Regional Development, 25.01.2011

Table 1. Summary of E-voting methods, as of March 2011
Source: Created by the author[4]
Legally binding elections
/E-voting in 2011
+ Voter Verifiable Paper Audit Trail (VVAT) added

Country	1. DRE with touch screen	2. Digital/optical scanning	3. Polling Station recording	4. Internet (kiosk)
Australia*			x	
Austria*				x
Belgium*+		x	x	
Brazil*+	x			
Canada*				x and phone
Estonia*/				x
France*				x
Germany (suspended)	x			
Ireland (suspended) for financial reasons	x			
Japan*	x			x
Kazakhstan*			x	

[4] Table 1. has been created by the author of this thesis based on ACE Project, E-Voting CC, European Commission and Tiresiasorg, ICT websites as well as information in various research papers and government and election commission websites

The Netherlands (stopped)	x			
Norway/				x (trial)
Peru*	x			
India*	x			
Portugal+ (non- binding trial)	x + VVPAT			x (trial)
Russia*/	x			
Switzerland*/				x and phone
United Arab Emirates (UAE)*				x (kiosk)
U.K. Suspended	x			x
USA*	x	x		x (partial)
Venezuela*	x			

According to the data above, of all the 16 countries which use legally binding e-voting, 11 countries use DRE machines, but only 3 countries - Belgium, Brazil and Portugal (pilot) - have decided to add VVPAT features to their system. Activist groups, for example the Open Rights Group in the U.K., and the Verified Voting.org in the U.S., as well as academics (Ballas 2006, 33, Mercuri, 2004) are treating the use of VVPAT as a tool to curtail security risks associated with lack of paper receipts; however, a leading researcher in the U.S. (Shamos 2004, 1) concluded that paper trail paper records do not address security problems: "The failure rate of paper trail DREs is double that of DREs without paper trails. It should be obvious that adding a new device with moving mechanical parts to an existing electronic machine cannot improve its reliability."[5]

[5] Testimony of Michael I. Shamos Before the U.S. House of Representatives' Committee on House Administration, September 28, 2006

Paper trail – or lack of - is a major technical issue that is widely discussed by academics and experts, as well as governments which are considering the introduction of DREs. Paper receipts– or the lack of – can have implications on voters' trust and on the overall credibility of election; paper receipts ensure that the voter has made the proper choice on a voting machine, and provide possibilities for recount or the always crucial verification of the result in case of a dispute between contestants.

1.3 Why countries drop?

All the three countries, Ireland, The Netherlands and Germany, that have given up the use of DRE machines after extensive tests lacked VVPAT features. While Ireland officially communicated that it gave up e-voting for financial reasons, there have been much criticism of its planned use of a DRE system without a VVPAT (McGaley, 2005) Both in Ireland and in The Netherlands, hard wares and soft wares were vulnerable to hacking and manipulation with a DRE's built-in memory card violating international standards of security and secrecy of the ballots. These machines, produced by the Dutch firm Nedap, were decertified in 2008.

In the case of Germany, the Federal Constitutional Court ruled that the use of the electronic machines contradicts the public nature of elections and deemed the voting technique illegal (Federal Constitutional Court 2009, 1)

> „A petition signed by over 45 000 people in 2005, trying to ban e-voting, had been rejected by the German Government. Now, the court ruled that the Federal Voting Machines Ordinance having introduced e-voting was unconstitutional because it did not "ensure that only such voting machines are permitted and used which meet the constitutional

requirements of the principle of the public nature of elections." (Digital Rights in Europe 2009, 2)

According to the U.K. Electoral Commission in 2007 all forms of trials (Internet, SMS, DRE, Internet kiosks) were suspended citing lack of security and strategy in the implementation of full-scale e-voting. DRE machines, in the U.K., have also lacked VVAT, and had been heavily criticized by the Open Rights group which has observed the U.K.'s 2007 and 2008 elections:

> „The Open Rights Group (ORG) believes that the problems observed at the English and Scottish elections in May 2007 raise serious concerns regarding the suitability of e-voting and e-counting technologies for statutory elections. E-voting is a 'black box system', where the mechanisms for recording and tabulating the vote are hidden from the voter. This makes public scrutiny impossible, and leaves statutory elections open to error and fraud. The Government has prioritized the introduction of e-voting because of the perceived convenience of new technologies, ignoring other vital considerations such as confidence and trust in the electoral system. ORG considers that the problems observed and difficulties scrutinizing results delivered by e-counting systems bring their suitability for statutory elections into question. (Open Rights Group 2007,)

Scholars have long been raising concerns over the use of DRE machines without verifiable paper trail audits, especially since the U.S. voting scandal in 2000. This animosity is also mirrored in Brazilian academics and scientists' condemnation of this type of e-voting. (Rodriges-Filho et.al. 2006, 88) Another blow is delivered to the proponents of DREs; in a comparison between paper ballots and DRE's error rate, the authors found that paper ballots' error rate was about 1.5 %, while DREs error rate was 4.2 % in the U.S. presidential race (Everett et.al. 2008, 883) highlighting serious challenges to e-voting advocates who claim that machines provide less opportunity for errors.

In conclusion, we can see that even though public sentiment is strong against DREs with no paper trail audits, only 3 of the 11 DRE-using countries adapted VVPAT, leaving many countries at the mercy of e-voting machines and concealed or invisible data processing. With the lack of elaborate safeguards and without the provision of paper-based audit ability, e-voting machines will continue to fuel controversy.

Chapter 2 – E-voting and its observation - principles, standards and guidelines

In order to frame the most challenging aspects of the observation of e-voting, this chapter overviews available documents, principles and guidelines from which the context of e-voting observation should emerge. The first sub-chapter explores what has been done so far by international observer organisations in terms of identifying focus areas for the observation of e-voting. This cannot be done without over viewing where universal election principles are challenged by e-voting methods, so the second sub-chapter is dedicated to do so. The third sub-chapter reiterates the fact that the lack of standards in the methodology of the observation of e-voting needs to be addressed.

2.1 The status quo

All major organizations involved in the promotion of democracy and development have undertaken the hard task of adapting observation methodology to e-voting, embarking on developing guidelines and framing controversial issues.

The National Democratic Institution, NDI has published a book titled "Monitoring Electronic Technologies in Electoral Processes", (2007). IFES has also published a book titled "Direct Democracy: Progress and Pitfalls of Election Technology, in September 2010. The Carter Center, "Developing a Methodology for Observing E-voting", published its discussion paper earlier, in

2007 with the aim of supporting its development if its observation methodology based on the Venezuelan elections in 2006. Earlier, the Council of Europe (CoE) Committee of Ministers with the 2004 Recommendations (Rec(2004)1). is considered a guide-setting body in the field of e-voting by all international organizations, collating knowledge in its recently published E-voting Handbook. (2010). The Recommendations have been used as the only agreed international guideline today, a starting point on which e-voting systems develop and on which observer organizations can base the development of their e-voting observation. The CoE reviews its recommendations periodically, and has conducted its third meeting on the developments in the field of e-voting at the end of last year. (Third meeting review, 2010). The group of experts focused on two main issues; the transparency and certification of e-voting systems as crucial components in trust building among the electorate. The Guidelines on Transparency (GGIS (2010) 5E) note that:

> "Although transparency, through the availability of documents to voters and stakeholders, is important, it will not be possible for everybody to understand an e-voting system."

Thus the guidelines highlight that the role of other stakeholders - party agents, accredited NGOs, observers – should increase during e-voting in monitoring procedures. However, the provision of clearly regulated (and ensured) access to documentation of a given e-voting method is complicated by another issue, namely the access to source codes.[6] Non-disclosure of source codes and other technical specifications are considered as a hindrance in the

[6] See Chapter 4.1.2 for further discussion of source codes

transparency of e-voting.[7] As Hall found it: "However, in a public source code disclosure or open source code model most members of the public will be unable to engage in independent analysis of the source code and will need to rely on independent, hopefully trusted and trustworthy, experts." (Hall 2006, 2)

Organisations which program and deploy election observation missions will have to keep this in mind when resourcing field missions. It seems that including a computer scientist in the core team of experts is the new minimum requirement for missions.

Certification is the other focus that all international observer organizations, including OSCE/ODIHR, The Carter Center and NDI, recognize as a necessity to build electorate's trust, therefore all wrap their guidelines around it, as well as around the importance of the composure of the certification body. The Council of Europe' latest focus on transparency and certification underlines the generally accepted expectation that

> "E-voting shall respect all the principles of democratic elections and referendums. E-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means. This general principle encompasses all electoral matters, whether mentioned or not in the Appendices;…" (Rec(2004)11, 7)

The principles, or the widely acknowledged and internationally accepted eight standards in democratic elections, stem from basic human and political rights, such as the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights and so on. Citizens participate in government through periodic and genuine elections that offer universal and equal suffrage, with a right to cast secret ballots. Standards also recognize the right to stand for election, to vote and to express voter's will

[7] Chapter 4.1.2 deals with the issue of open source software and the issue of source codes in details

freely. All these standards must be met during elections to evaluate a vote positively. Observer organisations must evaluate an election' compliance with these international election principles; however, electronic voting procedures are set to alter the manifestation of these principles by introducing new tools, stripping away verification processes and interfering with the observability and the secrecy of the vote. The universal, equal and secret nature of the ballot and the principle of free expression are the basic principles that are in danger and at times suffer violation when applying e-voting procedures. Consequently, these are the very challenges that need to be analyzed and answered when the classical election observation method is adapted to the observation of e-voting.

2.2 E-voting and universal election principles – where they conflict

This sub-chapter deals with universal election principles which elections have to fulfil. E-voting provides several identifiable threats in procedural compliance to these principles, thus these problematic issues can be singled out by observers when evaluating e-voting.

> ″Everyone has the right to take part in the government of his country, directly or through freely chosen representatives. The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures." Article 21, Universal Declaration of Human Rights, 1948

Universal, or general suffrage means that everyone has a right to vote and the right to be elected, and via this process a political representation is produced. One can view an e-voting machine as a brilliant technological tool

to simplify the election process, but it can be an intimidating new tool for others, thus negatively impacting participation. E-voting could pose a serious challenge to this election principle – still yet to be proven that technology has an impact on general suffrage. Furthermore, there is a clear difference between remote voting and voting done in controlled environment. While polling place voting ensures that all voters have access to technology by using readily established voting machines, internet based voting clearly disadvantages those who are at the bottom of the digital divide. This challenge to one of the basic universal principles should be considered by any election observation mission and the requirement to establish the existence of this criteria, namely that no universal election principle is hurt by a given e-voting system, should be part of the standards observer organisations will have to agree on. As CoE have suggested earlier as a guideline:

> „Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting." (Rec(2004)11).

While the observation of this principle in practice is very important in establishing compliance with international election standards, election observation missions cannot objectively measure the correlation between access to technology and its possible effect on participation. What it can do, however, is to aim to explore the degree to which population is potentially disenfranchised due to technology.

The equal suffrage principle means that a voter can only cast one ballot, or, in case of parallel e-voting and paper-based traditional method - multiple-

cast ballots only count once. Basically, each voter has one vote, and votes are equal. This principle in reality is often violated in traditional balloting as well by the unequal weight of votes as some constituencies have more voters than another. However, during e-voting - and especially during Internet voting - a voter can cast his/her votes several times, and only the last vote cast count. This of course poses an additional challenge in adapting observation to e-voting; while paper ballot casting is easy to observe, it is impossible to unearth multiple vote-casting as it happens away from the observers' view.

The secrecy of the vote**,** the other e-voting endangered principle, is embodied in most countries' constitution, signifying its importance. It is a prerequisite for any democratic election that a voter casts his/her vote in secret, free from intimidation and future repercussions. Only votes cast in total secrecy - when there is no way to prove whom the voter for – count toward equal suffrage and free elections. The requirement that votes cannot be traced back to a voter in any way –constitutes another issue of observation during electronic voting.

The Recommendation does spell out to keep the anonymity of the vote and that „the e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters." (Rec(2004)11,10) Therefore, observation missions should be able to establish the guarantee for anonymity of the vote and this should also become an e-voting observation standard.

The right to freedom of expression embodied in the election principle of free suffrage. The principle traditionally means that expression of the voter's

opinion shall be secured, and the voter should have the opportunity to freely choose his/her candidate, without any external interference; Voting from an uncontrolled environment, such as via Internet from home is the one that poses a challenge to this principle, but as it was mentioned before, is not subject to this thesis due to complete lack of observability.

2.3 Lack of standards for observation methodology

Traditional EU EOMs have, and are facing political and methodological challenges that the EU governing bodies are trying to remedy as observation missions evolve. A range of political fallouts are explored in a briefing paper for the European Commission [8] (Meyer-Resende 2008). However, challenges that have direct implications for e-voting can be traced back to the lack of international standards:

> "Once the EU has gathered sufficient experience on this issue [e-voting], it should define a methodology for the observation of e-voting and minimum conditions for observers' access to information. At the same time there is a need for international standards on minimum conditions for e voting. The Council of Europe already determined standards for e-voting, but given that the EU observes elections outside Europe, it cannot rely on these. Standard-setting would need to take place in the UN context; the EU should contribute to relevant policy initiatives." (Meyer-Resende 2008).

Even though tackling methodological challenges of e-voting observation are a hot topic for all International organisations involved in democracy promotion, without international standards and without the minimum conditions for observability established, these organisations are running the risk of evaluating elections on a fragmented base, with a patchy focus, thus jeopardizing the credibility of election observation.

[8] Please see the European Parliament Directorate General Policy Department, External Policies, EU Election Observation, Achievements, Challenges, page 1-10

In conclusion, the discussed documents do not provide a unified context for the development of observation of e-voting.

Chapter 3 – Challenges and experiences in observing legal frameworks

As was mentioned in Chapter 2, there is not yet a determined, comprehensive methodology for the observation of e-voting. However, the analysis of the legal framework for each and every election observed is crucial for all election observation missions and therefore they always include a legal expert. Given that the legitimacy and ultimate success of an election is based on laws and local regulations, the observer's job is to determine the extent to which registration, voting, tallying and complaints procedures comply with local and international laws. This chapter therefore analyses the discrepancies in the approach by different observer organisations to the observation of legal framework, and analyses EU election observation experiences to see the extent to which EU missions were able to capitalise on existing EU guidelines in this matter.

3. 1 Different approaches in the observation of legal framework

The comprehensive NDI handbook on Monitoring Electronic Technologies in Electoral Processes (2007), suggests focusing on, the legislation of observer's access to voting procedures, the adequacy of the accountability mechanisms in place and the provision of independent audits of the technologies involved. The handbook, for the first time also raises a

possible ambiguity: observers' interest in maximum access might challenge the security of the technologies used and the „appropriate protection of intellectual property". This issue has merits: even if an election software source code is made public[9], there are plenty of technical questions that can arise regarding proprietary elements, because observers must understand the system in order to evaluate its safeguards. Consequently, the legal framework must address the privileges observers can have in this regard and the exact procedures that must be followed.

OSCE' Discussion paper (2008) also recognizes this dilemma and states that legal texts must specify „the minimum level of transparency" to be established for observers, augmented by scope of access for observers and accountability provisions for elections officials. Other specific areas include the regulation of technological failure, procedures for audits and recounts, the necessity of VVPAT. These areas – as regulated in a given election legal framework – should be used as observation areas. The Carter Center (2006) is rather vague in its suggestions as it encourages observers to assess the degree to which international rights of voters are enshrined in election legislation, (as discussed in sub-chapter 2.2, different threats to principles difficult to substantiate) and also to focus on the election body' role in promoting transparency and the accountability of stakeholders.

While the legal provision of maximum transparency seems to be a common denominator for observer organisations, the key elements and standards for the evaluation of the legal framework are still missing. Observer

[9] The issue of souce codes and their accessibility is further discussed in sub-chapter 4.1.2

organisations must therefore think over, in each and every election observation mission, their approach to legal framework evaluation, and try to compensate for the lack of guidelines with ad-hoc approaches, depending on a given mission's election expert's expertise and preferences.

Consequently, this issue needs to be taken up by think-tanks and an agreed set of minimum criteria determined which supports both the approach to the observation and the evaluation of the legal frameworks of the host country. Different observer organisations should use a standard set of criteria for the observation of the different types of e-voting methods, but most importantly, one upon which their own observation methods can be based upon.

3.1.1 The EU approach

As there is no handbook explicitly written on the observation of e-voting by the EU, its rather practical "E-voting handbook, Key Steps in the implementation of e-enabled elections (2010), the Handbook for European Union Election Observation, (European Commission, 2008, and the previously mentioned 2004 Recommendations as well as various CoE guidelines can be used when the EU embarks on the observation of e-voting.

The "E-voting handbook, which at times simply repeats the Council of Europe (CoE) Recommendation (Rec (2004)11. was written to provide guidance to countries in the adaptation of e-voting.

The 2008 Handbook for traditional election observation suggests to focus on, the constitutional and legislative changes e-voting requires, with no specific details, in spite of the fact that the Recommendations from 2004

already established the principles for effective legal standards. The Handbook also suggests that when observing e-voting, observers must first ask whether the e-voting system facilitates an election that is in accordance with international standards. While this appears to be a simple and legitimate expectation from observers, as discussed in sub-chapter 2.2, in reality it is very complicated and requires the formulation of a whole range of e-voting-tailored observation objectives based on presently non-existent standards.

The Handbook however also suggests that observers focus on the certification procedures, and the issue of lessened transparency that limits opportunities for independent observation.

3.2 EU-observed e-voting

The European Union so far has conducted three election observation missions (EU EOM) that involved e-voting technologies: two in Venezuela (2005 and 2006) and one in Bhutan (2008).[10] This sub-chapter analyses their Final Reports in the context of the observation of the legal framework to see:

1) to what degree these missions were able to identify and observe the constitutional and legislative changes e-voting requires,

2) to what extent they were able to observe the certification procedures

3) if they encountered problems with transparency.

1) Regarding the first question the EU EOM Venezuela 2005 Final report simply notes without further implications that:

[10] For details about the types of voting machines used in Venezuela and Bhutan please see sub-chapter 4.3

> " …many aspects of the current electronic voting system have in fact developed so fast that they have surpassed the legal provisions that regulate it." (EU EOM Venezuela Final Report, 2005, 22)

The evaluation of transparency was limited to attending a one-day audit by observers, in which the possible endangerment of the secrecy of the vote was noted. (EU EOM Venezuela Final Report, 2005, 27) Experts also attended source code reviews, but noted that "while these sessions provided a first significant insight into voting machines and tabulation system they could only be followed and understood by a very limited number of observers." Further note that "…no detailed system documentation was available, neither for use during the audits nor for further study outside the audits." (EU EOM Venezuela Final Report, 2005, 28)

For the 2006 Presidential Elections however, the observation mission issued a detailed final report with systematic analysis of the existing legal framework mentioning on-going legislative changes. The biggest legal change regarding e-voting was that "the CNE (National Electoral Board) created a certifying authority, with two subordinated certifying authorities, one for the transmission infrastructure, and another for the voting machines, in order to generate cipher and signature certificates." (Final Report EU EOM Venezuela 2006, 20)

In the case of Bhutan, there was no attention given to the analysis legal provisions in light of adaptation of e-voting.. The report simply notes that: "…The legal framework provides a solid basis to conduct elections and generally meets international standards." (EU EOM Bhutan 2008, 3)

2) Unfortunately, none of these EU EOMs observed the certification procedures. For the 2006 Presidential elections however, the report notes that "Based on the analysis of the electronic system, the EU EOM considers that both the physical security of the system, backup and contingency plans, together with the logic security, encryption and electronic signature, are defined in conformity with internationally accepted security mechanisms and standards. (EU EOM Venezuela Final Report, 2006, 20)

3) E-voting and transparency

The issue of transparency was not explicitly addressed in any of these reports, indicating that observers relied on and accepted previous reports on certification and did not see the necessity to address this aspect of e-voting in these particular missions. What the 2006 Venezuela mission addressed is the cooperation with the electoral body: "In general, a good degree of cooperation was observed between the CNE and the external technical experts. However, the 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. (EU EOM Venezuela, Final Report, 2006, 21)

Findings above show that these election observation missions proceeded with the observation of an e-voting mission in the "business as usual" paper voting manner; approach to the analysis of legal framework, its implementation and the observation methodology is exactly the same as in traditional elections For the future, the CoE just published its guidelines on the

Certification of e-voting systems in which it suggests to update election methodologies to enable observers to observe the certification of e-voting systems. For this observers will need full access to the e-voting system. (CoE Guidelines GGIS, 2010, 5) This requires longer missions and a sufficient number of IT-savvy elections experts. Although the adaptation of e-voting and security of the system requires sound and elaborate legal provisions, it is obvious that the EU observation missions, studied within this chapter, were not equipped with the necessary expertise, standards (or perhaps will) to analyse in-dept the legal provisions required for these e-voting missions.

Whilst there are currently no standards or procedures for the evaluation of the legal frameworks for e-voting, it is imperative, for consistency of approach, that these are developed, agreed and universally applied forthwith.

Observation Missions of e-voting elections must have the correct level of technical resource, both in terms of people and equipment, to validate that standards and procedures applied to the legal framework are being adhered too,

These standards and procedures must be reviewed, and if required, updated and agreed on a regular basis as technology develops.

Chapter 4 – Technical and Security challenges in e-voting

The debate about technical issues stem from the security and verifiability of e-voting systems. Namely, they are centered on the issue of paper trail records, source codes and certification. This chapter therefore overviews current technical issues in the context of verifiability and security, in order to clarify challenges the different types of e-voting methods pose to observers. Sub-chapter 4.1 is discussing verifiability issues, and sub-chapter 4.2 discusses the issues of security.

4.1 Issues of verifiability

Electronic voting that takes place in controlled environments, are distinguished based upon either their provision – or lack of - a Voter Verifiable Paper Audit Trail (VVPAT) in any form. Citizen rights groups in the U.S. and in the U.K. are heavily campaigning for the use of paper trail records. VVPAT, however, can pose a challenge to voter' anonymity and secrecy. (Jones, 2004) In the following I recap the argument surrounding the use of paper trail and look at were observer organisations stand on this issue.

4.1.1 Observation of paper and non-paper trail methods of e-voting

Similarly to traditional paper-based voting systems, the secrecy of the ballot is a key component of any election to be observed. Secrecy implies that all voters are anonymous and their vote cannot be linked to back to them.

While (Mercuri 2000,1 and Hall 2008, 1), argues that a VVPAT is an absolute necessity for the verifiability of DRE machines, provision of paper receipts has also been associated with risks to voter's anonymity. (Xenakis and Macintosh 2004), Voter anonymity could be endangered by checks performed on printed paper receipts during audits, however, paper receipts add to the reliability of audits and provide "end-to-end verifiability" as allows for checking of the input (the candidate chosen) and the end result (via recount). (Jones 2004)

DREs with VVPAT could provide opportunities for the ballots to be traced to the voter (either via the paper receipt or by identifying voter's sequence in the DRE.) Mercuri (2004) however, developed a method to display the paper record behind a glass window for the voter to validate his/her choice before the ballot is cast for verification and later for auditing. She is supported by many others:

> „Over 900 computing professionals, including many of the top experts in computer security and electronic voting, have endorsed the "Resolution on Electronic Voting" petition, urging that all DRE voting machines include a voter-verifiable audit trail." Voting and Technology: Who Gets to Count Your Vote? (Dill et.al, 2003)

In India, one of the world oldest EVM-using country experts also campaigns for the use of paper trail: „A security analysis on of India's electronic voting machines also found that even simple electronic voting machines are vulnerable to attacks and suggest adding VVPAT to the existing hardware, use scanning machines or simply returning to paper-based voting. (Prasad et.al.2010,20)

While the application of VVPAT is widely viewed as desirable, some examples show that its benefits can easily be lost when it comes to the application of the system. Doug Lewis testified on behalf of the National Association of Election Officials in the U.S., in 2007[11] as follows:

> „VVPAT were found 20 % unreadable, blank or defective. Also, voters were not able to verify the VVPAT accurately, as research showed that over 60% of voters did not notice if the votes shown on the review screen were different than the choices they had selected. (Everett, 2007). The paper-count of the result therefore seems to be an inevitable component of the audit ability of any given election. While electronically tallied results seem to be best checked through some form of paper record, there is evidence suggesting that VVPAT is not a guarantee for fair elections"

With all that said, election observers face several challenges in evaluating both paper trail and non-paper trail methods. In the cases were VVPAT is applied, a mission - similar to paper-based methods - must establish whether paper records can be manipulated and in what ways, and whether ballots can be taken out of polling stations. This, in practical observation, can be treated as the observation of paper ballots count. However, VVPATs add a new challenge for observers: how to deal with the possibility of VVPAT showing paper confirmations, but DREs recording something else inside of the machine? The issue is the provision of system security, which requires a seasoned IT expert as part of the mission core team, to monitor the certification procedures, test runs, and who can analyse the system or can evaluate the findings of a third party. Election observation

[11] Testimony of R Doug Lewis, Executive Director, CERA National Association of Election Officials (Election Center) U S Senate Rules Committee July 25, 2007

mission IT experts therefore should be present from the earliest stages of software and hardware certification and testing.

Observers must also carefully analyze legal provisions on whether the priority has been established between the paper based and electronic records in case of discrepancy. While electronic results seem to be more accurate than human count, statistically relevant audit procedures must be put in place - which observers should be able to observe. Observer missions should focus their deployment of observers on the particular polling places where audits take place in order to witness this crucial aspect of the verifiability of the result. Consequently, observing e-voting require changes in the practices of deployment planning of observation missions.

Alternatives to DREs, such as optical scan ballots, and touch screen machines that print paper ballots can be treated as DRE + VVPAT by observation missions. Non-paper based methods in controlled environments, such as DREs, however, provide no physical platform to observe the transmission of result or the tally procedures. Should recounts become necessary due to complaints, there are no paper records to verify the vote (as it happened in the U. S. in 2000). The institution of recount is a long-used safeguard for validating any election and it has always been closely monitored by election observers, NGOs and party agents. Without this guarantee in the election process it would become very difficult, if not impossible for observers to evaluate the fairness of the election as reliance on audits of electronic data – given its limited scope - would not substitute a paper-based recount and

definitely doesn't provide for transparency when it is needed the most: during the challenge of the result.

In this regard, NDI summarised all observer organisations' stand on this issue:

"The requirement that the electoral process must be transparent and verifiable means an easily auditable record of the voters' choices is required; therefore the lack of proper paper record is unacceptable." (NDI Monitoring Electronic Voting Technologies 2007, 75)

4.1.2 Open source software

Open Source software - by definition - is "software that is made available freely to all (Beirne 2009, 4), meaning that e-voting soft wares that utilize open source should be generated by public means, freely exchanged and allow user-generated adjustments. (Open Source Initiative criteria, OSI, 2009). At the moment, there is no e-voting system in existence developed fully on an open source development model (Hall 2006, 6) , as the first fully open source voting system in Australia was developed by a Software firm, Software Improvements. Therefore the real issue is the disclosure of proprietary source codes by developers. This entails the protection of intellectual property, which goes against the provision of transparency.

As (Beirne 2009, 3) points out, e-voting systems are developed by experts to be used under strict procedures, therefore a private investment is involved entailing copyrights and licensing restrictions. This, according to Shamos however, is not entirely justified:

> "The manufacturers of voting equipment claim that their software is a trade secret and go to extraordinary lengths to preserve that myth. The author has been looking at the source codes of voting systems for over 20 years and has yet to find any significant differences in their design except possibly for the number of bugs they contain. They all do the same thing, albeit in somewhat different ways." (Shamos 2004, 18)

Beirne also points out that "software does maintain a level of security through the lack of available public knowledge on the inner workings of the software program", signifying claims that if proprietary soft wares are "forced" to become open to the general public, security of the system can become endangered. The same point is shared by Joseph Hall:

> "However, there are risks associated with fielding an open or disclosed source voting system. Since computer scientists have yet to find a method for writing bug-free software, public disclosure of the system source code will inevitably result in disclosing vulnerabilities. Voting systems are not the same as general-purpose computing technology. Voting technology is used highly infrequently, runs specialized software and is difficult to up-grade or change without extensive vendor involvement. In the case of voting systems, disclosing information on unknown vulnerabilities arguably helps would-be attackers more than system defenders." (Hall 2007, 9)

The applicability of open source software is largely under documented among the requirements and criteria for e-voting set by international observer entities, and clearly lacks academic and practical analysis. There is no guidance on the observation of software source codes however several non-profit groups, for example the Open Voting Consortium in California, the Open Rights Group in the U.K. have actively been campaigning for public access to software source codes. Furthermore, making source codes open does not immediately guarantee that all transparency requirements of a given election are fulfilled - over viewing source codes is clearly not in the capacity of an average voter, observer or party agent. Verification of a source code should always be done by an independent third party and election observation

missions should monitor and evaluate access to the source code in this context and analyze the degree of its contribution to the transparency of an election. The issue of security in open source codes or proprietary source codes made public – not only opens up questions on adaptability in e-voting, but further complicates observation challenges. While in theory it is desirable that the public, or different individuals have access to source codes, and therefore can be in a position to independently verify results and the good workings of a given election software, no criteria has been developed for election observers to monitor the extent to which open source software might contribute to the transparency and therefore the credibility of elections.

A solution could be that the public is given read-only access in order to leave source code modification to authorities backed by properly and timely codified legal provisions. The IT experts of observer missions could then analyze the source codes like any other member of the public. If, however, election software with open source code is employed, election observation missions will be facing the hard task of adapting observation methodology to an ever-changing technical environment. Issues of accountability, (who is legally responsible for the software, licensing, etc.) will needed to be studied, and the observation of legal framework – a key component of election observation - will have to be analyzed based on a newly developed set of criteria focusing on all aspects and timing of certification (and re-certification) procedures.

4.2 Security of the system

This sub-chapter focuses on two important aspects of e-voting related security: In 4.2.1 I overview general security challenges as they are discussed by scholars and the problem of result transfer. In the second part (4.2.2) I assess the present approach of observer organisations to the issue of certification. (Note: I found that none of the e-voting observing EU EOMs has embarked on the observation of the certification procedures.[12])

4.2.1 "State of play" – security and result transfer

As the NDI handbook cites Enguehard and Graton (2008) : "Perhaps more than any other aspect of electronic voting technology, the security aspect is where the devil is - truly - in the details." (NDI 2007, 60)

Further, OSCE Observation Mission's report on the Belgian 2005 election concluded that the: "observation of the e-voting system is de facto limited to an analysis of the security mechanisms in place, and to an observation of their implementation." (Enguehard and Graton 2008, 6)

Indeed, election observation organisations can find themselves in murky waters when trying to evaluate the security of a given election system. According to an overview on electronic voting development and trends submitted to the CC Conference on E-voting in 2010, authors state that

> "the security of any e-voting system starts with the development of the system, however, up to date there is „no classification to understand the common characteristics, objectives, and limitations of these (development) approaches Thus the lack of a comprehensive comparative study provides little or no direction on choosing the

[12] See sub-chapter 4.3 on EU-observed e-voting

> appropriate development techniques for particular needs."
> (Weldemariam and Villafiorita 2010, 2)

Recapping the development of requirements, the authors point out, that the existing international documents (CoE Recommendations, 2004, Venice Commission, 2004) mainly specify principles relating to each component of e-voting systems and there is a lack of a proper and comprehensive requirement definition – especially regarding security. The lack of pronounced requirement definition makes it extremely difficult – if not impossible – to specify observation objectives in analyzing a given election system from the security point of view.

Threats to security and voter anonymity are actually very complex based on the place of balloting and the genre of e-voting devices. Following the Venezuelan elections in 2005, (Krimmer and Volkamer 2006, 4) comprehensively framed the threats to voter anonymity and supplied future observation missions with a clearly defined set of tasks to observe all e-voting methods. According to the authors, the observation of security should focus on the functionality of the system and environmental challenges – and observers must address both. They identified major threats as illegal cameras in the polling station, software problems, insecure communication lines, breakable encryptions and the risk of taking the paper receipt out of the polling station. The authors also suggest that encrypted data is only secure until someone finds a way to break it – no absolutely safe encryption exists therefore in data transfer the possibility of linking voters to their vote lingers – long after an election observation mission concludes its findings.

In all elections – may it use traditional paper methods or e-voting machines – there is a line of data-flow: each and every polling station sends its result to a district or regional level point of compilation, before the regionally tallied results are sent to the central tabulation center. This process – the transmission of results – is carefully monitored at each step by observer organisations as ballots, ballot boxes, as well as tally sheets, are the so called "sensitive materials" to be treated under strict safeguards. Observers follow the ballot boxes and other sensitive materials back to tally centers and evaluate the safety procedures applied to protect the integrity of the material.

With e-voting, firstly, the sensitive material, the results, are transmitted via unsecured electronic networks (internet, telephone), without VVPAT tallies, the election result can be easily attacked and manipulated away from observation. Secondly, even if the data is transmitted in a controlled environment, elaborate security measures should be put in place to prevent the corruption of electronic data – and observers should be able to verify that the procedural measures are adequate to do this. This requires election observer mission experts to fully understand all the documented security requirements and be able to translate these requirements into questions that observers on the ground can sufficiently answer and verify.

Other than defining the minimum security requirements on e-voting - which observers can adopt as a base criteria - observer organisations should also compile observed security risks in recent e-voting systems and analyze these risks. Security shortcomings – perceived or real, proven or theoretical –

have a significant impact on the trustworthiness of a given election and this can greatly influence the (perceived) fairness of the election.

4.2.2 Certification and testing

"Certification is a process to establish whether a given electronic voting system satisfies previously established standards and legal requirements" (OSCE 2008, 9). All international observer organisations address the issue of observation of the certification procedures to various degrees. As the proper functioning of e-voting machines, transfers and controls are directly linked to the validity of elections. While "Certification procedures on their own "do not solve the majority of security or usability problems", (Enguehard, Graton 2008), there are pronounced efforts by the observer community to address the observation of this important step of confidence building.

In an important development, The Council of Europe has recently published, in October 2010, guidelines titled "Certification of e-voting systems". Its recommendations include various aspects but also emphasises the need for the publishing of the certification procedures, with clear guidelines identifying who and when, have access to information regarding certification reports. To make a concentrated effort to communicate certification reports – in any democracy – in my opinion, serve as a huge step in confidence building and observers should monitor the extent and timeliness of publishing.

However, according to (Esteve 2008, 199) the publication of certification reports and public' access to certification procedures have been subject to

controversy and often denied due to private developers involvement in the systems. It is clear that anybody who aims to increase transparency by allowing access to most aspects of e-voting systems and reports, inevitably conflicts with developers' business interests. The Recommendation recognizes this ambiguity and allows for exemption, but the extent to which system providers can keep, for example, security aspects secret, will have an impact on the quality of the analysis observer organisations will be able to produce. Esteve suggests that "Despite current framework, … how some minor data is coming from given countries actually suggests that the opacity is well grounded and that it would be easily feasible to include a certain degree of transparency without breaching the industrial property." (Esteve 2008, 205)

Other observer organisations, the Carter Center 2006, CoE, Recommendation 2004, OSCE 2008) also suggests to observe the functioning and the composition of the certification body and its relationship with stakeholders. The certification body should be independent all election stakeholders, however an observation mission can only assess its independence (or bias) based on verified reports, documentation and licensing.

Consequently, the ways to establish the certification body's independence, the degree of access to documentation (in the light of protecting business interests) and the publication of certification reports and procedures should be considered when formulating observation methodology for the observation of e-voting certification.

The transparency of certification goes a long way, as an observation criteria, given that governments often have to rebuke accusations of switching to e-voting technologies from paper-based voting technologies for business gains. Therefore, the independency of the certification body is crucial for an observation mission to report on, as it has an impact on the wider political environment in which an election takes place..

4.3 EU-observed e-voting

This sub-chapter aims to overview how past EU election observation missions addressed verifiability and security challenges to e-voting regarding technological challenges, certification procedures and audits. The issue of security was extensively addressed in the Recommendation (Rec (2004)11[13] providing basic guidelines for formulating particular observation objectives.

Unfortunately, the three analysed missions by the EU have somewhat been inconsistent in their observation, as each focused on different aspects of security within the e-voting process.

The EU EOM Venezuela Final Report, 2005 – in compliance with the Recommendation to the secrecy of the ballot – observed a threat to this principle and

> "noted a possible security breach, namely that: if the two parts of the voting system, the electronic voting machines and the print capturing devices were to be integrated, it can provide a complete electronic record of election, i.e. a record of votes cast and who cast them. It is important to note that, it is not necessarily the case that the automatic collection of this information violates the secrecy of the vote. Only if these two systems are linked, either in real time or offline, and the sequence of voters is the same in both activities and recorded or

[13] For details please see Recommendation (Rec (2004)11, page 17-20.

> revealed, could this violation occur." (EU EOM Venezuela Final Report, 2005, 22)

While the threat for the breach of secrecy was admitted by the EU EOM, unfortunately the term "not necessarily" is not objective, nor meaningful in evaluating a crucial aspect of the vote in lieu of minimum security standards established. As discussed in sub-chapter 4.2.1 it is evident that in 2005 the mission had no common criteria and standard to base its evaluation on. The mission also noted the possible "leakage" of personal information of voters stored on USBs as follows:

> "However, the theoretical possibility that the information eventually transmitted by the SAVs to the central data processing level could be misused and manipulated by CNE officials to perform various checks on the identity of the voters, expressed by some opposition parties, could not be ruled out. " (EU EOM Venezuela, Final Report, 2005, 24)

The mission also noted that the CNE, (National Electoral Board) owned the source code of all Smartmatic software they used. And that an IT team at the CNE fully audited the source code, both to verify functionality and to identify areas that need improvement or redesign. However, the report does not mention the details of this audit, its observation by independent observers, party agents, or any other election stakeholders. According to the final report, audit activities were also "conducted due to their limited nature, both in time and in resources, cannot in fact replace a full system audit by a commonly accepted independent third party ." (EU EOM Venezuela, Final Report, 2005, 28)

The 2006 EU EOM to Venezuela noted some improvement in the administration of electronic voting. Experts abolished the machines' capacity to reconstruct the voting sequence, and changes were made to the fingerprint

reading machines to avoid the sequential transmission of data. (EU EOM Venezuela, Final Report, 2006, 20) The report also commended the presence of technical experts during audits, - which were evaluated as "contributing significantly to increase the reliability of the voting machines" (Final Report EU EOM Venezuela 2006, page 22) and listed the „various verification instruments that allow for the identification of possible inconsistencies in the different phases of the polling process and therefore, permits the definition of audit procedures."(EU EOM Venezuela Final Report, 2006, 21) Further,

> "the fingerprint readers raise doubts and fear among the population, based on the perception of a possible control by the authorities that could bring about negative consequences for their personal and working life. A fear exists in some sectors of the population that the fingerprint readers allow for the reconstruction of the voting sequence and thereby violate the secrecy of the vote, but this fear is unfounded." (EU EOM Venezuela Final Report, 2006, 27)

The EU EOM to Bhutan 2008 noted that the country is using EVMs - similar to EVMs used in India - and evaluated these self-contained devices as simple machines consisting of two basic parts: 1) the ballot unit (with a simple digital counter for votes) and 2) the control unit. At the end of polling, the EVM tallied the votes for each candidate, (inside the black box problem) which then was entered by the Counting Supervisor in a results sheet. Each candidate or political party had the possibility to be present during the polling and the count.

In terms of security evaluation, the mission simply noted that "The use of advanced electronic voting machines (EVMs) simplified the overall voting process and procedures, and significantly reduced a large potential area of human error. In every polling station that the EU EOM observed, portable,

battery-operated Electronic Voting Machines (EVM) were used. Polling officials were well-trained in the practical use of EVMs and voters were well aware of voting procedures." (EU EOM Bhutan, Final Report, 2008, 28)

In conclusion, inconsistency of approach in the observation of various security aspects of e-voting calls for a standardised application of the existing framework and the application of EU observation methodology. The Handbook for e-voting can be used as a basic guide in the future (until an e-observation handbook is produced) as it explicitly spells out the critical areas of security to observe,. Without this, EU election observation missions risk loss of credibility.

Chapter 5 - Conclusion and Recommendations

In the past 15 years international election observation has gained momentum. Several organisations, including the European Union, have been fielding numerous election observation missions. The EU, the OSCE, the UN, the Carter Center and other democracy promoting organisations have developed their methodology and best practices to consistently observe paper-based elections. By the appearance of e-voting technologies, however, traditional observation methodologies are challenged as they need to be altered and developed in order to address the legal and technical challenges these new - and rapidly evolving - technologies entail. In spite of the fact that there is a strong public sentiment against voting machines, that provide no transparency in vote processing, a growing number of countries are experimenting with e-voting methods and are considering their use for legally binding elections.

Transparency, as it directly relates to the credibility of the vote, is a crucial aspect to observe under any circumstances, but different e-voting methodologies pose several new challenges to transparency and consequently, its observation. Currently Observation missions do not adhere to an agreed set of criteria when it comes to the evaluation of e-voting processes, this in spite of numerous handbooks, guidelines and recommendations on the field. Instead, in the three cases observed, the European Union Election Observation mission followed an evaluation methodology and programming that was developed for the observation of paper-based elections. This lead to a minimised observation of some of e-voting's' crucial aspects, such as degree of transparency. Additionally, a

complete inconsistency of approach, in the observation of various security aspects of e-voting can be found, which necessitates a review and standardisation of the existing framework.

The purpose of this thesis was to identify the most challenging aspects of the observation of e-voting that require immediate policy response from international organisations. These aspects of e-voting are the observability of legal provisions, the issue of verifiability and its observation, and various aspects of ballot security and data transfer.

Recommendations

5.1 The provision of observability in e-voting' planning

The CoE guidelines on transparency already suggest (for member states, but it can be useful to any other country that adopts e-enabled elections) to analyse the changes required to the relevant legal framework before adopting new technologies. Among this is the recognition that provisions need to be made for domestic and international observers regarding access to the process. However, as was analysed in the case of the three EU-observed e-voting missions, access to the present procedures was not enough to make a truly meaningful and verified observation. One way of tackling the enormous and inherent observability problem of e-enabled technologies is to "build-in" observability factors into the planning of the system. Namely, countries should not choose e-voting systems without identified observability measures.

5.2 Early policy guidance – minimum standards of observation

The Council of Europe has recently developed guidelines for best practices in e-voting certification and transparency, as well as an E-voting handbook for the development of e-voting systems. However, the lack of a comprehensive policy on the observation of e-voting was demonstrated throughout the cases analysed. Therefore the EU should publish a comprehensive policy for the observation of e-voting, and develop its own

Handbook addressing above mentioned major challenges in observation; including best practices.

5.3 Need for new skills, resources and methodology

According to the analysed EU election observation missions in Venezuela and Bhutan, the composition of the expert team followed the need of missions deployed to observe paper-based voting. As it was found in chapters 3 and 4 of this paper, the inclusion of an IT expert, (or more) is an absolute necessity, not only to technically analyse the hardware and software used, but to verify technical procedures, the merits of security-related assessments, and reports made by third parties. Observation missions should also review the expertise they require from their observers. Voters look to observers to interpret and verify the good workings and the security of e-voting systems, therefore it is crucial that the EU (and other observer organisations) prepare previously deployed observers on the particularities of e-voting. Adaptation to the observation of e-voting also requires changes in methodology. As the observation of certification is a crucial issue in the evaluation of e-voting, experts should be deployed before the traditional 2 month lead time to Election Day.

In summary, a standardised, clearly documented, expertly resourced, meticulously planned and well communicated approach is needed to guarantee that the EU delivers the same renowned quality of electoral observation in its upcoming e-voting missions, as it currently does in its traditional observation missions.

List of references

Ballas, Alexios. 2004. E-Voting: The Security Perspective. Department of Information Systems, London School of Economics.

Beirne, D. 2009. Open Source: Understanding its Application in the Voting Industry, April page 3, 4. A publication of the Election Technology Council

Council of Europe. 2010. E-voting handbook - Key steps in the implementation of e-enabled elections. Directorate of Democratic Institutions, Council of Europe Publishing, Strasbourg.

Carter Center. 2007. Developing a Methodology for Observing Electronic Voting. One Copenhill. Atlanta.

Council of Europe, 2008. Geseelschaft für Informatik and E-Voting.CC. 3rd international conference on Electronic Voting 2008. Bregenz.

Council of Europe, 2004. Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Rec(2004)11.Adopted by the Committee of Ministers of the CoE on 30 Sept. 2004

Dill. David L. 2010. Electronic Voting: An Overview of The Problem. Professor of Computer Science, Stanford University

Dill, David L., Schneier, Bruce, and Simons, Barbara. 2003. Voting and Technology: Who Gets to Count Your Vote? Paperless voting machines threaten the integrity of democratic process by what they don't do. Communications of the ACM, Vol. 46, No. 8, August 2003

Enguehard, Chantal and Graton, Jean-Didier. 2008. “Electronic Voting: the Devil is in the Details” Security Institute (ECCSI) Brussels, Belgium.

Esteve, Jordi B. The Certification of E-voting Mechanisms. Fighting against Opacity. Universitat d'Alacant : 6, 199, 205

European Commission, 2008. Handbook for European Union Election Observation. Election Team. Directorate General External Relations.

Everett, Sarah P. 2007. The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection, Ph.D dissertation, Rice University.

Federal Constitutional Court. 2009. Judgment of 3 March 2009 – 2 BvC 3/07 and 2 BvC 4/07 –Use of voting computers in 2005 Bundestag election unconstitutional Press release no. 19/2009 of 3 March 2009

Hall, Joseph L. 2006. Transparency and Access to Source Code in Electronic Voting School of Information, University of California at Berkeley

Hall, Joseph L. 2008. Design and the Support of Transparency in VVPAT Systems in the US Voting Systems Market. UC Berkeley, School of Information.

Hari K. Prasad et.al. Security Analysis of India's Electronic Voting Machines Hyderabad y The University of Michigan, April 29, 2010

Hyde, Susan D. Experimenting in Democracy Promotion: International Observers and the 2004 Presidential Elections in Indonesia. Political Science and International Affairs Yale University.

Jones, D. W. 2004. Auditing elections. Communications of the CM 47(10): 46-50. *In E-Voting: The Security Perspective*, Alexios Ballas, London School of Economics, 2006, 33

Krimmer, Robert and Volkamer, Melanie. 2006. Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting. Working Paper Series on Electronic Voting and Participation. Nr. 01/2006

Council of Europe, 2010. Guidelines on transparency of e-enabled elections. GGIS (2010) 5 E. Strasbourg, 25 October 2010

Shamos, Michael I. 2004. Paper v. Electronic Voting Records – An Assessment. School of Computer Science. Carnegie Mellon University

Mercuri, R. 2000. Voting automation (Early and Often?). *In E-Voting: The Security Perspective*, Alexios Ballas, London School of Economics, 2006, 33.

McGaley, Margaret. 2005. Electronic Voting in Ireland, Computer Science Department June 29, 2005. Available from http://www.cs.nuim.ie/~mmcgaley/e-voting/submission.pdf

Mercuri, Rebecca.*,2000.* " Electronic Vote Tabulation, Checks & Balances". Ph.D. dissertation. University of Pennsylvania.

Meyer-Resende, Michael, 2008. EU Election Observation Achievements, Challenges.

Directorate-General for External Policies of the Union, Policy Department. European Parliament

Mulligan, Deidre K. and Hall, J. Lorenzo. 2006. Open Source Software – Does it Have A Place in California's Electoral System? Prepared Statement.

National Democratic Institution NDI. 2007. Monitoring Electronic Voting Technologies Publisher: National Democratic Institute for International Affairs. Author(s): Vladimir Pran; Patrick Merloe.

Office for Democratic Institutions and Human Rights. 2008. *OSCE/ODIHR* Discussion Paper in preparation of Guidelines for the Observation of Electronic Voting. Warsaw:

Oostveen,Anne-Marie,and Besselaar, Peter van den. 2004. User 's perceptions on the security of electronic voting systems. Department of Social Sciences, Royal Netherlands Academy of Arts and Sciences.

Rodriges-Filho, Jos´e; Alexander, Cynthia J. and Batista, Luciano C. 2006. E-voting in Brazil – the risks to democracy. In: Krimmer, R ed. Electronic Voting 2006, GI Lecture Notes in Informatics. Bonn, Germany: Bregenz, pp. 85–94.

Shamos Michael Ian Paper v. Electronic Voting Records – An Assessment, School of Computer Science, Carnegie Mellon University, April 2004

Xenakis Alexandros and Macintosh, Ann (2004). Procedural Security in Electronic Voting. 37t Hawaii International Conference on System Sciences. 7th Hawaii International Conference on System Sciences – 2004.

Weldemariam, K. and Villafiorita, A. 2008. Fondazione Bruno Kessler, A Survey: Electronic Voting Development and Trends Center for Scientific and Technological Research (FBK-IRST)

Consulted websites

European Commission. 2010. EU EOM Ethiopia 2010. Online. Available from: http://www.eueom.eu/ethiopia2010/home 5 April 2011.

European Commission, 2011. Election Observation Available from: http://www.eueom.eu/ 4 March 2011.

Tiresias.org, Making ICT accessible, 2011. Available from: http://www.tiresias.org/research/guidelines/evoting_projects.htm, 30 March 2011.

E-voting CC, 2011. Competence center for Electronic Voting and Participation, Available from: http://www.e-voting.cc/stories/6184497/, 1 March 2011,

Electronic voting in Belgium. Wikipedia Website: http://en.wikipedia.org/wiki/Electronic_voting_in_Belgium#cite_note-4

The Electoral Knowledge Network, ACE. E-voting opportunities. Resource center online. Available from http://aceproject.org/ace-en/focus/e-voting/e-voting-opportunitie; Accessed on 12 March 2011.