Survey & Analysis of E-Voting Solutions

Master in Computer Science
Trinity College Dublin

Mark O'Meara
Supervisor: Dr. Mike Brady

Submitted to the University of Dublin, Trinity College,
May, 2013

Declaration

I, Mark O'Meara, declare that the following dissertation, except where otherwise stated, is entirely my own work; that it has not previously been submitted as an exercise for a degree, either in Trinity College Dublin, or in any other University; and that the library may lend or copy it or any part thereof on request.

Signature : —

Date : —

Summary

In order to contribute to the continuing debate around the use of electronic voting machines, it is important to consider the track record countries have had with the use of the technology. A lot of arguments have focused on a small number of cases of failure or success. This research, in contrast, aims to provide insight into the uses of e-voting worldwide by surveying a large number of the countries and states that have made significant use of technology in their election systems.

To begin, the various properties of what constitutes an adequate voting system are examined. These properties are: authentication, auditability, privacy, speed, mission critical, security and availability. This dissertation then discusses, one by one, the stories of a number of countries. These include the best known case studies on electronic voting, but also less frequently cited cases. Where possible, each case includes a description of the technologies used, the reasons for implementing electronic voting, and any major problems encountered.

Following the survey, an analysis is performed on the cases with a number of conclusions drawn. This research concludes that governments throughout the world have varying reasons for introducing electronic voting. These reasons include the need to eliminate vote rigging, to reduce financial costs, to improve voter accessibility, or to simply modernise the process. It also concludes that while electronic voting does involve risk, this risk must be compared to the risk some governments would experience by remaining with a paper-based voting system; therefore, the adoption of risky e-voting may be justifiable in some cases but not justifiable in others. Further conclusions include the need to consider the social effects of voting technology, and the need for a formal approach to be taken towards the development of such systems.

Acknowledgements

Many thanks to my supervisor, Dr. Mike Brady, for all his time and invaluable help.

Contents

Chapter 1

Introduction

The use of electronic voting began decades ago; yet, there still exists a lot of debate around its use throughout the world. While some groups and experts have been actively lobbying against the adoption of certain technologies in the election process [23] [14], many governments have continued to increase the role technology plays in their democracy. Throughout the debate, a lot of discussion has been based on the theoretical risks related to certain technologies, with the same small number of cases being regularly cited. In contrast, this research is a real world survey of a large number of different implementations of electronic voting. In order to make a measured assessment of the controversy behind the use of electronic voting, it is necessary to examine what the experience of e-voting has been throughout the world. This includes examining why governments have adopted its use in the first place, what considerations may have been involved, and what controversies, if any, have been experienced since its adoption.

Firstly, it is important to distinguish the different types of e-voting technologies. The term ‘e-voting’ is usually associated with a Direct Recording Electronic (DRE) system. This refers to a machine that a voter casts their vote on, and on which the vote is then digitally. When using a DRE system, the voter’s role consists of simply approaching the machine and casting their vote on it. This is in contrast to variation of this, whereby a voter uses a machine to cast their ballot, but once the ballot is cast the machine then simply prints the ballot, at which point the vote is treated the same way any paper vote would be treated. A third type of system is known as an Automated Election System (AES), or also an Optical Mark Recognition (OMR) system. This often involves the use of voter-marked paper ballots, but instead of the ballots being put into a ballot box and then hand-counted, the ballots are instead put through machines that count the ballots automatically, usually by scanning and analysing the ballots in order to determine the voter's intention.

There are also two types of internet voting systems. The first is a kiosk-based system. This is where the casting of the vote takes place over an internet connection, but must be done from a machine at one of a number of specified locations; for example, a polling station. The second type of internet voting, known as remote internet voting, is where a voter can cast their vote from any location they choose, and on a machine not necessarily provided by the country's election commission. For example, voting from a home computer. The differences between these two internet voting systems are significant in terms of the considerations and risks involved.

In practice, e-voting implementations often consist of a mixture of the different types of systems defined above.

Before surveying different implementations, it is important to consider what an adequate voting system looks like. Over time, a number of properties have been outlined for what a voting system should consist of [33][9]. While some of these properties may clash, it is generally seen that these are ideals that a system should, as best as possible, obey. Each of these properties will be examined one by one.

1.1 Authentication

One of the key properties of an adequate voting system is the ability to ensure that only those who are eligible to vote are actually able to vote. To do this, we need to be able to authenticate each voter. Under a normal voting system, where voters vote at polling stations, this is generally done by giving polling station officials the power to request photographic ID from a voter. For remote voting systems, where a voter does not need to present themselves at a polling station, this becomes a problem. A number of different methods have been used to implement authentication in internet voting systems. One such way has been to simply send out voter credentials in the post, which a voter then uses to log in to the voting system in order to cast their vote. More creative methods have been used, for example in Estonia [13], which will be discussed later.

Authentication under a normal paper voting system, of course, does not completely guarantee against fraud. In many countries, including Ireland, requests for identification are arbitrary. This leads us to question whether completely fool-proof authentication should be necessary for an online voting system, given that such a requirement is not necessary needed to be fool-proof in paper-based voting systems. However, a direct comparison between paper-voting authentication and online voting authentication cannot be drawn due to the fact that a vulnerability in an online voting system could allow for advantage to be taken of the vulnerability on a huge scale, whereas taking advantage of a vulnerability in the authentication in a paper-based voting system would be rather difficult to do on a large scale. Exploiting a vulnerability in polling-place authentication would allow a single person to vote multiple times, but the scale at which this could be done would be limited by this person's ability to move between polling stations and avoid recognition by polling officials he or she has already encountered. In contrast, a vulnerability in authentication in an internet voting system could allow the same person to cast multiple votes very quickly, limited only by the speed of his or her computer.

1.2 Auditability

The property of auditability covers the idea that any proposed system must be able to produce a tamper-resistant, independent record or audit trail in order to ensure the result announced was actually the correct result. Under a paper-based voting system, the paper votes themselves act as this audit trail, as if there is a dispute over the result then the paper votes can simply be recounted.

DRE voting systems do not have a natural method of being auditable. A suggestion made for e-voting systems, such as the one proposed in Ireland[61], was that each DRE machine should also produce a paper record of each vote in order to ensure these can be checked if the declared result is called into question. The suggestions also includes the idea that a significant number of paper votes should also be counted to see if the result corresponds to the result declared by the e-voting machines. However, it could clearly be argued that if such a feature was to be implemented in an electronic voting system, then this would effectively render the use of an e-voting system pointless, since paper is still playing a major role in the process. As well as that, while a paper-based audit trail may be possible with an e-voting system, such an audit trail would not be possible with a remote internet voting system.

While it may be preferable to have a paper-based audit trail of some kind, it should be considered whether, alternatively, enough trust can be placed in an electronic system to digitally store tamper-proof logs securely, which could be accessed to verify outputted results.

1.3 Privacy

The privacy property is one that is very easily catered for with a paper-based or electronic voting system, but is actually very difficult to implement in a remote internet voting system without encroaching on the auditability property. Ensuring votes are cast in private is important for many reasons; not only does it ensure no one can see how you voted, but by extension it also ensures no one can coerce you into voting a certain way since a coercer will have no way of verifying how you actually voted. This comes into conflict with the auditability property in an online system because the best way to ensure auditability is to keep a very detailed record of every action that is carried out in the system; however, if privacy is to be ensured then there may be difficulty with the idea of the voting system storing records containing any information that may allow a voter's information to be matched to their vote. While some may argue that if we can do our banking online then we should be able to do our voting online, the difference between the two concepts is clearest when you consider the necessity of actions being kept anonymous on an e-voting system. In online banking systems, detailed records of each user's actions can be kept to ensure nothing malicious is occurring. Not only is the privacy of a vote put at risk by storing records allowing for the matching of a vote with a voter, but it is also put at risk due to the possibility of a coercer watching a voter cast their vote, and thereby ensuring that the vote is cast as wished.

A consideration should be made as to necessity of the privacy property. It needs to be considered that a paper-based system does not guarantee complete privacy in practice; for example, it's not unlikely that one adult may accompany another adult while they cast their vote. An absence of privacy when casting a vote online may allow for coercion on a greater scale; however, it could be argued that this slightly increased vulnerability would not render an entire voting system useless or unsafe to use in democratic elections.

1.4 Speed

Another principle is that election results must be available in a timely manner. Of course, the definition of “timely” is up for debate and other properties would generally be given priority over this. However, there are examples where voting systems have been modified in order to ensure this property is better met.

One side-effect that may need to be considered with this property is if there is such a thing as “too fast”. Would politicians be satisfied, for example, to be told suddenly without any build-up or expectation that their campaigns had failed and they had not been re-elected?

1.5 Mission Critical

Elections must be held on a fixed day or days. This means it is not acceptable for systems to fail for a period of time when they’re in use. A typical approach to software development, therefore, may not be acceptable for an electronic or internet voting system. Software development often involves patching bugs when they become noticed, and prioritising fixes; however, if a bug or issue arises during the use of an electronic voting system then it’s very likely this will have an impact on the result. Voting machines are therefore mission critical.

1.6 Security

Security is an essential component to an electronic voting system. It ensures other properties hold even in the case of a limited conspiracy of election officials, programmers, third-parties and voters to undermine the election. The use of the word ‘limited’ is important, because ultimately no system can be completely tamper-proof if there are enough people in enough positions who are working together to manipulate an election for their own advantage.

1.7 Availability

The principle of availability is the idea that the system must be up and able to accept ballots for the whole voting period. This means that it is not acceptable for a DDoS attack to be able to temporarily take down a voting system. The idea that an internet voting system must have complete availability is questionable. After all, is the ability to vote severely hampered if the voting system is down for just a few minutes, or even just an hour or two, in a voting period several days long? This property is similar to the 'Mission Critical' property already described, but refers to the idea that the voting system is available for use, whereby the 'Mission Critical' property refers to the idea that the system must operate as expected without the occurrence of bugs or the need for patches.

Chapter 2

Americas

2.1 Argentina

Each of Argentina's 24 provinces is responsible for its own electoral system, including designing its own rules [42]. Since 2003, test pilots have taken place across the country to examine the possible use of electronic voting [62].

One such province is Salta, in which approximately 1,200,000 people live, 850,000 of whom are registered to vote [42]. The province of Salta represents a significant case study for the country because of its rural geography and rough terrain, as well as the fact that many places in the province still lack electricity. Salta had a number of motivations to move towards electronic voting. These motivations included increasing voters' confidence in the voting system, increasing the speed of the counting, and improving the ease of voting. A law was passed in 2008 with provisions for the introduction of electronic voting. The law gave the Electoral Court authority over the control of the system, but did not specify how it should be audited. Trials have been conducted in the province since 2009, and are to conclude in 2013 when it is expected that 100% of the province's population will vote electronically [42][58]. Until then, those who were not provided with electronic voting facilities were required to cast their ballots by paper.

The machines used in Salta are not Direct Recording Electronic (DRE) machines; they do not store any votes. When a voter wishes to vote, they proceed to a machine with an e-ballot provided by a poll station worker. The ballot, which is similar to a paper ballot but also contains a RFID-chip, is then inserted into a slot in the touch-screen machine. The voter then makes their selection on the machine's touch-screen, and once finished the machine then physically writes the vote onto the ballot, as well as storing it on the ballot's chip. The voter then places this ballot into a ballot box, just like they would with a normal vote. If they wish, the voter has the option to verify the contents of the digital vote are as expected. [42]

Once voting in Salta has concluded on election day, the machines used by voters to cast their vote can now be used by polling officials to count the votes. The poll workers do this by opening the ballot boxes and, one by one, passing each vote through the reader of the machine. A beep is heard whenever a vote is read by the machine, and the machine's display also provides feedback. For example, if an attempt is made to scan the same vote more than once, the machine will display a "repeated vote" error. Once the tallying process has completed, relevant information, including the result from that polling station, will be printed and also transmitted to a central computer centre. [42]

The implementation in Salta achieved many of its goals. Within three hours of polls closing, the results of nearly all votes cast electronically had been received by the Electoral Tribunal. In contrast, by this stage few of the results from areas using the traditional paper method had been received. It wasn't until nearly 8 hours after polls closed that results of all votes cast by paper had been received. A survey taken during the system's initial pilot test indicated the solution did ensure ease of voting. Of the 410 voters who took the survey, 93% said they found the system easy or very easy to use. 70% said they could rely on the new system to a greater extent than the traditional system. [42]

2.2 Brazil

Brazil's use of electronic voting first began in 1996 with tests carried out in the state of Santa Catarina.

All of Brazil's voters cast their votes using the same model of voting machine. The voting machines are small, weighing less than 9 pounds, and consist of a display screen and number pad. Interestingly, the votes are transmitted via satellite transmission to the central processing centre and are also capable of operating on battery power for around 9 hours, making them suitable for use in Brazil's most rural areas. The results are determined by the central processing centre within hours of polls closing in the country. [53]

The move to electronic voting took place following frustration with the country's manual voting system, which often took several weeks to return the results of an election. This was because of the country's rural areas, meaning ballots needed to be transported to the depths of the Amazon and back again, a journey which could take weeks. The results returned under the paper system were also often considered unreliable, with a lot of errors occurring during the process. The machines, manufactured by a subsidiary of the Ohio-based company Diebold Inc., were first introduced in 1999 with a third of precincts using them. Since 2000, 100% of votes in Brazilian elections have been cast using the voting machines. [53]

The newest models come with a fingerprint scanner and a number pad, as well as a display screen. See Figure 2.1.

The machines carry out all three vital functions of a voting system: voter identification, vote casting, and vote tallying. The fingerprint scanner is used to verify the identity of the voter, and the number pad used to allow the voter make their selections. The primary benefit of the machines is the ability to transport them to, and operate them in, the country's most rural areas, such as the Amazon rainforest. The transportation of them to some areas can take a number of weeks, but because of their use of satellite technology, the

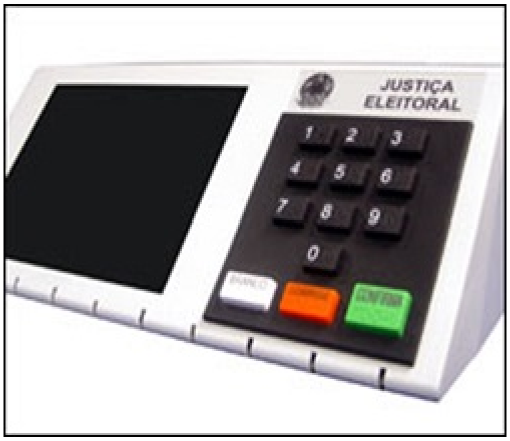

Figure 2.1: Brazil Voting Machine [44]

results of elections are now available within hours of the closure of voting [53].

While the use of electronic voting in Brazil is popular and has brought increased efficiencies and trust in the electoral process, the system itself has also been scrutinised by hackers to attempt to find faults [53]. Nine teams, consisting of 38 experts in total, were challenged to try overcome the election system's security features and to find serious security holes [25]. Although none were found, the source code is still proprietary closed-source, and therefore the lack of public scrutiny or knowledge of how its operations are carried out still leaves a lot of room for faults to go undetected.

2.3 Canada

Although there is not yet any electronic voting on a federal level in Canada, there has been a wide range of technologies put to use at provincial and municipal level. Six provinces have passed legislation to give municipalities the chance to pursue alternative voting methods, including electronic voting. These six provinces are Alberta, British Columbia, New Brunswick, Nova Scotia, Ontario and Saskatchewan [27] [37].

Touch-screen voting machines are used in some municipalities in Alberta and Ontario. Some Ontario municipalities additionally deploy optical scanning technology. Optical scanning has also been used in municipalities in New Brunswick. Quebec did, previously, allow for the use of electronic voting machines in the 2005 municipal elections; however, their use in the province has since been discontinued due to a number of reasons. Among the reasons were an absence of technical specifications, norms and standards [37].

Remote internet voting has been trialled in a number of government jurisdictions over the last decade, including its implementation in more than 45 municipalities [37]. The municipalities include Halifax, Nova Scotia and 44 municipalities in Ontario. In all cases, internet voting has remained as an option for voters to choose rather than being forced upon them [37].

The first implementation of electronic voting in Canada was in 2003 through various trials in municipalities throughout the country. One of these municipalities was Markham. Markham's motivation for introducing electronic voting included wanting to increase turnout and improve accessibility. The town offered internet voting during the 5-day long advance polls, as well as optical scan vote tabulators in the polling stations on election day itself. To avail of internet voting, voters were required to pre-register. Upon registration, they were required to create a unique security question and were subsequently mailed a unique PIN. Once registration had completed for the advance polls, the voter was then manually taken off the list of electors eligible to vote in person on election day. To vote on the online system, a voter must provide their PIN and the answer to their security question. Despite the turnout in other municipalities in the province falling that year, turnout remained the same in Markham with a 300% increase in the amount of people voting in the advance polls. [27]

Following Markham's success, Peterborough sought to introduce a similar system in order to reduce the need of proxy votes and to improve accessibility. This was done in 2006, and similarly to Markham they provided internet voting during a 5-day advance polling period and also introduced optical scan tabulators at polling stations. All electors received a registration card with information including a unique elector identifier (EID). Voters could access the online voting system by simply entering the EID and passing a CAPTCHA challenge. They could then register on the system by supplying their address (as it appeared on the registration card) and their year of birth. A PIN would then be sent to them either by mail or email, depending on what the voter chose. Once registration had completed for the advance polls, the voter was then manually taken off the list of electors eligible to vote in person on election day. To log in to the system to vote, the voter would need to enter both the EID and the PIN. [27]

Halifax Regional Municipality (HRM) introduced internet voting in 2008. The motivation for them was to determine the viability of electronic voting. The choice of internet voting was also offered alongside telephone voting to the electors during advance polls, which took place during a three-day period two weeks before election day. The trial was available to 276,000 voters. Unlike the two previously mentioned implementations, no registration was required to make use of the technologies available during the advance polls. This meant that voters were not taken off the election day list of voters manually once they had registered, but rather they were taken off automatically once their vote had been cast using an alternative method. This applied to the two technologies in use also: internet and telephone voting. Once a vote had been cast using one method, the voter then automatically became ineligible to cast a vote using the other method. A feature of the Halifax system was the ability to switch voting channels. This meant that, for example, an elector could commence their voting on their cell phone and finish their voting through via the Internet on their home computer, or vice versa. The online voting system required the use of a PIN and the voter's date of birth to confirm their identity. The system also made use of a number of security tests. A 'penetration test' was performed by hiring an IT firm to try break through the system and to therefore evaluate existing security mechanisms. A second check consisted of an analysis of the encryption system in place for the communication between computer servers. A third check involved an external audit of the entire voting process by Ernst & Young. The final check was an analysis of the overall network, its security, and its ability to prevent attacks. [27]

2.4 Philippines

The Philippines first began considering the adoption of electronic voting in 1993 due to fears of corruption in the electoral system. Public confidence in the system was low, a problem which wasn't helped by the fact that it could take longer than a month after an election for the results to be announced. An Automated Election System (AES) was first used during the May 2010 elections. [12]

The journey towards its use was far from smooth. Following a pilot of the technology in the country's 2001 nationwide legislative elections, the election commission (COMELEC) procured a physical automated election system for use in the 2004 elections. However, due to problems with logistics and security, the machines were never used and the election was carried out manually. A similar problem occurred in the 2007 elections, for which the use of electronic voting was mandated, but because there was insufficient time given for its implementation the election, again, had to be carried out manually. [12]

A pilot project did take place in 2008 in the Autonomous Region in Muslim Mindanao. This pilot used a combination of Direct Recording Electronic (DRE) and Optical Mark Recognition (OMR) technologies. The success of this pilot allowed for a national implementation of electronic voting in the 2010 elections. However, due to a lack of public trust in DRE systems, and concerns about costs and reliability, DRE technology was not used in the

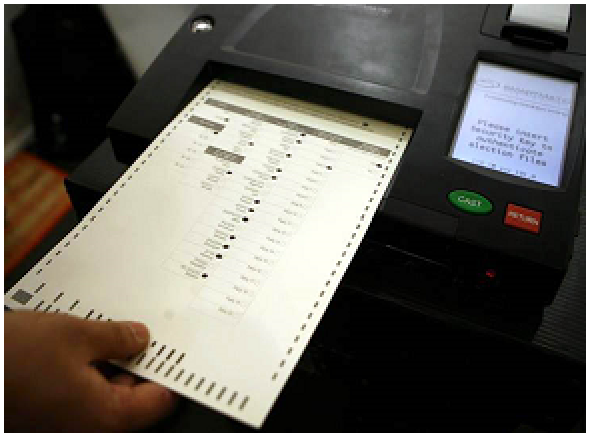

Figure 2.2: Philippines Voting Machine [3]

2010 election; only Optical Mark Recognition technology was used.

The machine ultimately used, developed by Smartmatic, was an Optical Mark Recognition system, which scans both sides of a double-sided paper ballot. The ballots, which can be up to two feet long, should be marked by the voters with a felt-tip pen. The machine then analyses the ballot and determines the voter's choices, storing the data onto a compact flash card inside the machine. See Figure 2.2.

The machine also puts the paper ballot itself into an attached secure ballot box. Images of each ballot are also stored in the machine as TIFF files. Information stored by the machine is stored on a compact flash drive.

Each of the 76,347 polling stations in the country received just one machine. Each machine's features included a touch-enabled screen, a "cast" and "return" button, an iButton key slot, and two compact flash cards (one backup). Each was also designed to be able to operate for at least 12 hours on battery power [12].

The legal framework for electronic voting, adopted in 2007, does not specify a specific technology, but rather it specifies the minimum requirements of any voting system in the country. These requirements include:

- security against unauthorised system access
- accuracy and efficiency in recording
- data retention
- a voter-verified paper audit trail
- ability for a voter to verify their choice has been registered

Notable is the fact that the system used in 2010 did not obey all the specified requirements. Specifically, on election day voters were not provided with a way to verify their choice had been correctly registered. The machines, however, did provide a feature for this, but this feature was disabled. The machines were equipped with screens that would display how a voter's ballot had been read by the software. The reasons given for disabling this feature included the idea that it would slow down the voting process, and that there was also a potential for vote buying, as people may use camera phones to take a picture of the screen as proof of them voting a certain way.

A Technical Evaluation Committee was set up and assigned the responsibility of obtaining certification of the machines, and therefore determining whether they were operating as designed and expected. The certification must include documented successful reviews of, among other things, an audit of the software, a source code review, and confirmation that the source code review was conducted on the actual source code used in the system. The audit and code review were carried out by a third-party software and source code testing and auditing firm. [12]

A number of phases of testing took place. These phases were post-bid testing, acceptance testing and field testing. As well as that, during an election poll workers are required to complete a short testing of the machines seven to three days before election day. In the 2010 elections, these final tests found serious errors which threw the election into chaos. During the testing, it was found that the machines were not producing the right results based on the ballots they had processed. This, it turned out, was due to a printing error on the ballots. One side of the ballots had, correctly, been printed in single spacing. However, the other side of the ballots had been designed in double spacing. This caused the machines to be unable to read the ballots and therefore could not correctly determine the voters' intentions. This problem was discovered just 7 days before election day. Because there would not be enough time to re-print the 50 million ballot papers, the decision was made to recall all 76,000 CF cards, and to distribute different CF cards with updated configurations to allow machines to be able to read the ballots. This was done in time, but caused serious worry over the country's election preparations and contingency plans, and highlighted the possibility of problems existing in how the machines were tested in the first place. The problems were further highlighted by the fact that before the election, many of the presidential candidates had demanded manual voting to take place in parallel to the electronic voting, only for their demands to be dismissed by authorities. [7]

Each ballot paper contained an ultraviolet (UV) mark in order to allow the machine to validate its authenticity. However, due to another printing error, the machines were unable to read the UV marks on the ballots. This led to polling stations being issued with hand-held UV lamps so that poll workers could verify the ballots manually.

Once the voting had concluded, results from each polling station were transmitted to the relevant servers. This transmission was most commonly done through general packet radio service/cellular, but other methods included over broadband global area network (BGAN) or over very small aperture terminal (VSAT) satellite. Physical transportation of the compact flash cards to their respective results locations was available as a contingency.

Despite the problems throughout the election process, the election was seen as relatively successful. Fewer than 400 machines (from more than 76,000) needed replacement on election day, and by 24 hours after polls had closed 92 percent of polling stations had officially declared their results.

This is in contrast to previous elections where it could take up to 40 days for precinct results to be announced. The project cost the country $160 million. [7]

2.5 United States of America

In the USA, each state is responsible for the administration and funding of elections in their state. During the 2000 elections in the state of Florida, a number of severe problems were experienced with the voting system. In particular, problems were experienced with the use of a ‘puncher’, which was a mechanical system used to punch a hole in a ballot paper to correspond to a voter’s selection. In a huge amount of cases, however, the holes were not correctly punched and it was left up to counting staff to determine the voter’s intent. This determination needed to be informed by the counting rules, which had regularly changed and were sometimes contradictory. Poorly designed ballots, too, contributed to problems with the election. 113,820 ballots had too many candidates marked, and a comprehensive examination determined that nearly 25,000 of these were the result of confusing, poorly designed ballots. Ultimately, the controversy surrounding the Florida count ended up in the Supreme Court of the United States, with them declaring that the recount should end. [6]

Following on from this, a number of moves were made to change the way elections were run. Most significantly, the Help America Vote Act (HAVA) was passed by the US federal government, appropriating $4 billion for states to update their election processes and another $325 million to update voting technologies. This money led to states abandoning the outdated mechanical voting systems in favour of electronic voting systems, with the number of e-voting vendors and service providers substantially growing. However, many well-publicised errors have occurred since the mass adoption of electronic voting technologies. In the 2004 presidential election, for example, the machines in one precinct in Ohio recorded 4,258 votes for George W. Bush and 260 for John Kerry, despite the fact that only 638 votes were cast in the precinct that day. During the same election, another serious problem was experienced in a North Carolina county. The county was told by their e-voting machine vendor that the machines could hold 10,500 votes; however, the machines could only hold 3005 votes, which led to 4500 votes being completely lost. [6]

Controversies continued in the most recent General Election in 2012. A touch-screen machine in Pennsylvania was recorded on camera not allowing a voter cast a vote for Barack Obama. Instead, when a voter pressed the area around Barack Obama's name, Mitt Romney's name was instead selected. In fact, no matter where the voter touched on the screen, he was unable to select Barack Obama's name [55]. A lawsuit in Ohio preceding the same election contested that some of the electronic voting machines in use in the state had not been tested or certified [57].

Although many states' technology is in need of an upgrade, due to the lack of financial resources at their disposal many are not in a position to change their systems [51].

The Secure Electronic Registration and Voting Experiment (SERVE) was an experimental internet voting system [32] implemented by the Pentagon to be used by troops abroad to vote in elections. Initially the system would serve overseas troops from seven states: Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington; with the eventual goal being to support the entire population of overseas voters, including military troops and their dependants. The initial deployment of the system was planned to take place in time for the 2004 primary and general elections. Following a critical report from the Security Peer Review Group (SPRG), a group of experts assembled to evaluate the SERVE system, the project was scrapped. The critical report stated that the system should not go ahead due to the fundamental architectural weaknesses that exist in the Internet, and therefore

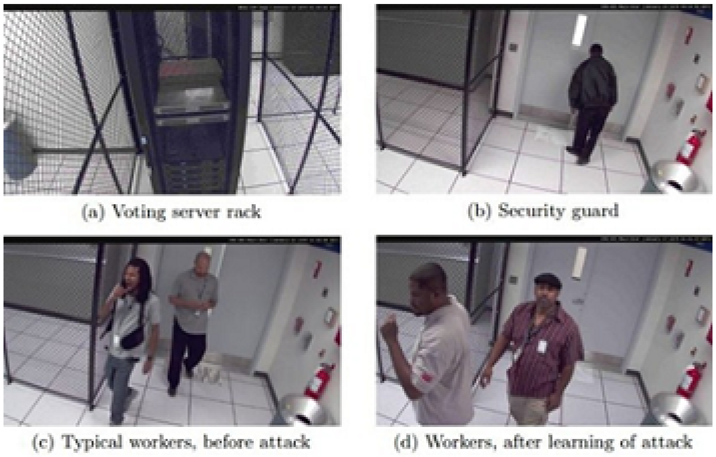
(a) Voting server rack
(b) Security guard
(c) Typical workers, before attack
(d) Workers, after learning of attack

Figure 2.3: Group's access to the Washington DC CCTV system [66]

a redesign of the SERVE system itself would not be adequate in dealing with their concerns.

Following the failed SERVE system, Washington D.C. in 2010 developed their own internet voting pilot [66]. The goal of the project was similar to the goal of the scrapped SERVE project: to allow overseas absentee voters to vote in elections through the Internet. One month before its planned use in the 2010 general election, a public trial was held. For this trial, a mock election took place on the system. The purpose of the trial was to test the system's security. Within 48 hours of the trial commencing, a group of experts had hacked into the system and had it under their full control. To demonstrate their level of control, they changed every vote and revealed nearly all secret ballots, as well as determining which user had cast each ballot. The group also gained access to the server room's CCTV cameras, allowing them to see the movements of election officials. See Figure 2.3.

As if to emphasise the scale of the failure experienced, election officials did not even realise there had been a breach in the system's security until two days after the hackers had taken full control; and this realisation only came soon after the hackers left a message on the ballot confirmation page, which came in the form of a song that played after a 15 second delay. This proposed system was immediately scrapped, just weeks before it had been scheduled to go live. [66]

Chapter 3

Asia

3.1 India

Electronic voting was introduced in India largely to resolve a number of specific issues.

The first issue was the logistics of accommodating such a large country.

The second issue was the problem of having such a large illiterate population, and the effect that has on the electoral process. In every election since the country's independence in 1947, for example, the number of invalid votes has been more than the winning margin between candidates. The amount of invalid votes is linked to the country's illiteracy rate, which was at 66% in 2007. [65]

The third issue which India sought to solve was the rampant vote rigging taking place in the country. This was a huge problem in the country, and consisted of incidents such as voters turning up to a polling station to find that they had already been recorded as having voted, to the hijacking of trucks carrying ballot boxes, to criminals stuffing ballot boxes and removing voters from polling stations. [29]

Electronic voting was first used in 1982 to solve these problems. Initially, they were placed in only 50 polling stations. Since then, their use gradually

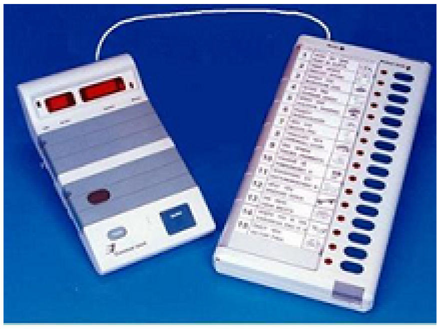

Figure 3.1: India Voting Machine [4]

grew up until the 2004 General Election when they were used nationally for the first time. In the 2009 General Election, nearly 1.4 million voting machines were used [29] [65] and an average of 302 votes were cast per machine. The electronic voting machines are very simplistic, and consist of two distinct parts: a ballot unit and a control unit. The machines are also relatively cheap, at just $200 each, which is far less than machines in the U.S. which can cost several thousand dollars each [65]. Because voting sometimes takes place in rural areas, or areas with intermittent electricity supply, the machines are completely battery operated. The ballot unit, which is placed in the polling booth, has a list of candidate names and respective party symbols on it, with a button beside each one. When voting, the voter, simply presses the button beside the candidate they wish to vote for. The ballot unit is connected by a 5 metre wire to a control unit, which is in the possession of a poll worker. To allow a voter to cast their vote, a poll worker must press the 'ballot' button on the control unit. A maximum of 5 votes a minute can be recorded on a machine in order to avoid ballot stuffing [29]. See Figure 3.1.

The control unit also has two LED number displays. These are used to display the results of the election once it has concluded. To conclude a voting period, a poll worker simply presses the 'Close' button, which is concealed on the control unit. When counting occurs, which could be weeks later, the control units are brought to the count centre and an election official presses the ‘Results 1’ button. The LED display on the left displays the candidate number, and the display on the right displays the number of votes that candidate received. The official can then go through each candidate to see how many votes the candidate received. [65]

In 2010, a critical security analysis was done on India’s voting machines which exposed a large number of vulnerabilities existing within India’s machines. The report highlighted a number of possible attacks that could be carried out by a malicious third party. These attacks included replacing the display with a ‘dishonest’ display that reads back a different result, or using a clip-on memory manipulator that could change the stored results in just a few seconds [65]. The report made a number of possible recommendations, which included either implementing a paper audit trail, making use of an optical-scan system, or simply returning back to a paper-based system [65]. In July 2011, following on from court cases and public scrutiny, a new system with a paper audit trail was piloted in 200 polling stations [29]. It is expected that these will be launched fully in the near future, in time for the 2014 general election [52] [17].

3.2 Japan

E-voting in Japan has been in existence for just over a decade. A law was passed in 2002 to permit its use, and in the same year the country’s first e-voting election was held in Niimi city of Okayama prefecture [28]. The use of e-voting machines is currently allowed only for local elections, and not for national elections. At least 10 local governments, out of 1800, have made use of voting machines since 2002 [30]. The biggest e-voting election took place in Yokkaichi city of Mie prefecture, where the turnout was approximately 95,000 people [28].

In order to vote, a voter must present themselves at a designated polling station. Once a voter has been validated, they receive a voting card from a poll worker. They must then insert this voting card into the voting machines. The touch screen of the machine is used to select vote choices, and to cast the vote. Once the vote has been cast, the voter returns their voting card to a poll worker. These cards are continuously reused by other voters throughout the day. Once polling has concluded, a poll worker, under the supervision of auditors, removes the storage media containing the votes from the polling station and transports it to the counting station [28]. By law, the voting machines cannot be connected to an electronic communication line, such as the Internet, for security reasons [30].

The types of e-voting machines in use in Japan vary slightly in the way they store the votes cast. Most machines use a standalone storage method, whereby each machine has its own storage media for remembering the votes. This method is in contrast to the client-server method, where there would be just a single recording medium per polling station. Under this method, all votes would be stored in a single polling station storage rather than a machine's own storage [30]. The latter proves to be a disadvantage if the central storage fails, which would render all machines in the station faulty. This is in contrast to a single storage unit failing in a machine, which would render just that machine faulty. In fact, a problem similar to that posed by the client-server method in 2003 led to a lawsuit in Kani City. This lawsuit resulted in that local government's election being declared invalid. [30]

Because of some issues in the use of e-voting, the Ministry of Interior Affairs in November 2005 set up the Research Committee on E-voting Systems. A report released by the committee in March 2006 suggested the introduction of a certification system, in order to ensure compliance of voting machines with their technical requirements. Before this, confirmation of compliance only involved manufacturers performing their own inspections and a joint inspection with an election committee. As a result of the report, from December 2006 an inspection to confirm compliance was carried out by a private inspection agency on behalf of the Ministry, with the result of such inspections being made public. [30]

Although e-voting is only allowed in local government elections, moves had been made in 2007 to introduce it on a national level. This came about after agreement from Japan's ruling parties at the time. Although a bill was put together, which passed the House of Representatives, it was never passed in the House of Councillors due to a number of unresolved issues and the limited amount of time they had to resolve them. [30]

3.3 Kazakhstan

Kazakhstan first made use of electronic voting in their 2004 elections [19]. The technology and system they use, known as the Sailau e-system, is somewhat unique, with the term 'in-Direct Recording Electronic voting system' used to describe it [35].

The electronic voting system in a polling centre consists of a number of parts. Firstly, there's the electronic registration. This involves a voter having their national ID card scanned to verify their identity and to record the fact that they've voted. Once the voter has registered, they receive a smart card, similar in size to a credit card. They then proceed to the voting booth and enter the card into the voting machine. Once the card is entered, they make their vote choice on the touch screen in front of them. This process is, for the voter at least, similar to the process experienced in many other countries. In other countries, as mentioned in this report, voters are given an authorisation card to enable the voting machine, which, upon placing it in the machine, allows them to cast their vote. There's a significant difference between that system and the Kazakh system, however. Under the Kazakh system, the card is not an authorisation card; in fact, the card holds the ballot itself. When the voter is given the card, they are given a card with the ballot and election information on it. Upon entering the card into the voting machine, the machine simply reads the information on the card and allows the voters to cast their vote accordingly. The cast vote is stored on the card. This system means that the voting machines themselves do not need to be modified in between elections, since they simply read the information on the cards and allow the voter to cast their vote accordingly. Once the vote has been cast and has been written to the card, the voter then takes the card and places it in a smart card reader at the registration table. The reader records the ballot. The card is then available for reuse by other voters. Due to the complexity of the system, there is one technician placed in every polling station in which electronic voting is in place. [35]

A verification process is offered to the voter during this process. Once they have cast their vote, but before their vote has been written to the card, voters who wish to partake in the verification process will be issued a random 4-digit control number. When voting has finished, reports are generated by the election officials. One such report contains a list of all the 4-digit numbers given to voters, with each number beside the candidate for which the vote was cast. A voter is entitled to return to the polling station after voting has closed to verify that their number is assigned to the candidate they voted for. Obviously problems exist with this, however, such as the fact that the machines could be programmed to only alter the votes of those voters who did not request verification. Another problem is that this type of verification infringes on the right to a private vote, since any voter who was willing, or forced, to sell their vote could provide proof of their vote through this process. [35]

The whole national voting system on election day is overseen in a centralised location, electronically, to which each polling station's system is connected and to which each polling station regularly sends updates. The centralised structure allows for a number of benefits. The first benefit is that it ensures those overseeing the election in the central location can tell immediately whether problems exist in any polling station by being able to see which polling stations have started and finished the voting processes successfully.

The second benefit is that it allows for the detection of voters who have voted in more than one polling station. This is done through the electronic registration system. However, detection of voters who have voted more than once cannot be done until after polls close. Additionally, a centralised structure means all relevant data can be quickly transmitted to the central location where it is needed. [35]

Notable with this system is that electronic data was, by law, given preference over any information on paper. Also notable is that there was no method for which a recount could take place. [35]

Due to a significant lack of public confidence in the system, however, voters at polling stations equipped with the electronic voting machines were given the opportunity to cast their vote by paper ballot instead. It was not originally intended for the paper and electronic voting systems to operate in parallel, yet this process remained in place throughout all elections for which electronic voting was available [35]. The lack of trust in electronic voting by the public was clear from its usage. In 2005, less than 14% of those who had a choice between voting electronically or by paper chose to vote electronically [20]. In 2007, approximately 33% of the electorate had the option to vote electronically; however, just 6% of those who had the option chose to vote using the e-voting machines [21]. These figures were likely influenced by the fact that opposition parties encouraged voters to vote by paper [39]. Ultimately, due to the lack of public confidence and a need to update the system at a cost, 2007 was the last election in which the e-voting technology was used [22] [46].

3.4 United Arab Emirates

The United Arab Emirates (UAE), established in 1971, held its first national elections in 2005. Following this election, the UAE National Election Commission decided to introduce an electronic voting system for the 2011 elections. The project was aimed at improving accessibility, accuracy, auditability, integrity, reliability, and time savings. Also, the system would make use of a paper audit trail. [5]

The authentication of each voter would take place using the country's e-ID card. The UAE itself consists of 7 different emirates. Each voter would be allowed to vote at any polling station within their own emirate. To provide for this, servers were deployed in each emirate, facilitating the conducting of simultaneous elections across the country. The e-ID card played a central role in the system. Once a voter had verified themselves at the station, a flag was set on their card to allow them to vote. Once their vote had been cast, a 'voted' flag would be set on the card. This flag would ensure the voter could not then cast another vote, either at that polling station or elsewhere. The cards also contain digitally stored digital certificates. These certificates allowed the system to encrypt each vote with an anonymous digital certificate. [5]

The encrypted votes would later be decrypted by the private key of the electoral system. This private key consisted of the individual keys of the electoral board members. Importantly, the voting system did not keep any link between the encryption envelope and the contents of the vote, meaning it could not be determined who each vote belonged too. However, temporary data, such as cookies, needed to be destroyed afterwards to guarantee this. [5]

A pilot took place two weeks before election day. No technical issues were discovered in the trial involving more than 600 staff, although a number of minor problems around the issue of usability were flagged. The election itself took place on the 24th of September 2011. To assist with the introduction of the new system, voters were brought to a training area once they had arrived at the voting centre. The training area was used to help familiarise voters with the new process. The identity of the voters was then verified, and once it had been determined the person was a valid voter, they could then proceed to a voting machine. As part of the paper audit trail, once a vote had been cast on the machine a paper record was printed off. Voters were required to place this paper record into a ballot box. [5]

A number of technical issues occurred on election day itself. Firstly, confusion was caused by screen freezes on some machines. Voters were able to get around this by attempting to cast their ballot again, at which stage they would get an error message if a previous ballot had already been processed. Secondly, some of the printers of the paper ballots entered into sleep mode, which caused many paper ballots to not be printed correctly. While this problem was easily ended by staff modifying each printer's default settings, this was a trivial yet important problem that was overlooked. Thirdly, some voters had faulty ID cards in which the chip was not functioning correctly. These voters had to be issued with temporary smart cards, called “white cards”. [5]

The Agile development methodology was used for the design and development of the e-voting system. The software itself was proprietary source code from an international commercial electronic voting solution, which had to be certified by an international body. [5]

Chapter 4

Europe

4.1 Belgium

The use of electronic voting in Belgium first began in 1991 during its federal elections [15], making it one of the first countries in the world to adopt e-voting [63]. Its use then expanded to local, provincial and European elections, with 44% of voters using an e-voting system in the June 2007 elections. There were a number of reasons why Belgium brought in an e-voting system. These included the seeking of quicker results announcements, cost savings, and easier administration [29]. A new, modernised e-voting system is scheduled for use in the country in 2014 [63].

Under the original e-voting system, the voter would select their voting preferences on a machine using a light pen. The vote, rather than being stored in the machine itself, is written on the magnetic strip of a card. The voter then takes this card and places it into an electronic ballot box. The box then reads the magnetic strip of the card and records the vote stored on it. If a recount is required, this is simply done by passing all the magnetic cards through a counting machine again. Once the voting process is finished, the electronic ballot boxes write the results to a floppy disk which is then transported to the cantonal headquarters [15]. Although there is no human-readable information on the magnetic cards, if a voter wants to ensure that the vote stored on the card is the one they cast, they can place the card in another voting terminal to read the ballot and verify it has been recorded correctly [29]. Its use throughout the years has been relatively issue-free. The only major problem occurring was in the 2003 local elections when one candidate got 4096 extra votes due to an error in the flipping of a single bit in memory [29] [15]. To deal with less serious issues, the Government made a series of small changes to the processes involved through the years. The most notable of these changes included the releasing of the source code of the voting software onto a Government website on election day, once the polling stations have closed [63]. Political parties are given an opportunity to view the source code at an earlier stage [15]. Research carried out in 2003 found that 88% of voters had a favourable attitude towards the system [15].

Because the voting system was originally designed in 1991, some of the technology became obsolete over the years, such as the use of floppy disks to load the software and storing the votes. In light of the ageing system, the federal and regional governments in 2006 requested a consortium of seven Belgian universities to perform a comparative study of a number of voting systems and recommend the most appropriate to replace Belgium's existing e-voting system [15]. The study recommended a combination of voting technologies: a touch-based e-voting machine to cast your vote, and an optical scanner for counting the vote. Under this system, once the voter casts their vote on the voting machine, a paper ballot is printed with the voter's choices. The ballot also has a two-dimensional bar-code. This bar-code is a machine readable version of the ballot choices, allowing machines to process the vote. Once the voter has their ballot, they must fold it over so that only the bar-code is visible. The ballot is then deposited into an opaque electronic ballot box, which scans the bar-code and processes the vote. Similar to the country's original e-voting system, the voter also has the opportunity to scan the bar-code on a machine to verify that the bar-code information matches

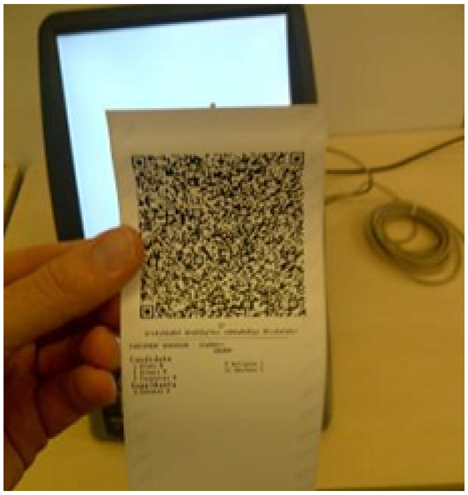

Figure 4.1: Belgium Voter Ballot [18]

the vote which the voter had cast. The electronic ballot box does not allow the same ballot to be scanned more than once, and each ballot box stores each vote cast on two USB sticks. One subtle difference of this new system to the previous one is that the original only stores votes electronically (on the magnetic strips of cards), where the new system stores it electronically and in human-readable form. See Figure 4.1.

This means that, if necessary, the human-readable form of the ballots can be used to verify a vote count. Like the original system, the source code will continue to be made available in a similar fashion. The new system, developed by Venezuelan company Smartmatic, was used for the first time in the country's October 14th local and provincial elections.

4.2 Estonia

Estonia in 2007 became the first country in the world to provide legally binding remote internet voting for national elections [8]. Estonia's internet voting system takes quite a different approach from what has been tried with other systems previously.

Upon the development of their internet voting system, the country had a unique advantage by the fact that a Public Key Infrastructure (PKI) [13] was already in place and being used throughout the country. As part of this system, every Estonian citizen over the age of 15 is required to carry a national ID card. Each ID card stores digitised data relevant to the owner, including cryptographic keys and public key certificates. The card allows a user to digitally sign documents, proving that they themselves are the owners of the documents.

Internet voting was first trialled in municipal elections, where Estonia became the first nation to ever hold legally binding internet elections. Although less than 2% of votes in this election were cast online, the trial was considered a success and the path was paved for further use of the technology. Internet voting has since been available for use in all subsequent local and parliamentary elections in the country, with the percentage of votes in elections cast online constantly increasing. In the 2011 parliamentary elections, 1 in 4 votes were cast online.

Estonia's system makes a very good attempt at overcoming many of the problems associated with internet voting. Among these problems are voter authentication, auditability, and mission criticality.

The problem of voter authentication requires any voting system to be able to ensure that only those who are eligible to vote actually do vote. Under paper-based voting systems, this is often done by giving polling station officials the power to request photo ID from a voter. The lack of in-person verification with online voting systems creates a problem around this area. Estonia attempts to overcome this by using the previously mentioned PKI and national ID cards. The use of these from a home computer requires the user to have a card reader; however, because of the wide-spread use of the ID cards and of digital signatures in the country, many households already possess a card reader for their computer. The system reads the digital information from their card to confirm their identity, and the voter also enters a PIN through the voting website to ensure no one is using someone else's card. [13]

Auditability requires that any voting system can produce tamper-resistant, independent records or audit trails in order to ensure that the result announced was actually the correct result. Under paper-based systems, the paper votes themselves act as this audit trail, as if there is a dispute over the result then the paper votes can simply be recounted. Electronic systems don't tend to have a natural property of auditability. In the Estonian e-voting system, there are a number of audit possibilities. Several logs are created in the system during the various voting stages. LOG1 contains the received votes, with each entry containing the voter's personal identification code and a hash of their encrypted vote. LOG2 contains the cancelled votes, with each entry containing similar information to LOG1 as well as the reason for the cancellation of each vote. LOG3 contains the votes to be counted, with each entry being every entry in LOG1 that isn't in LOG2 (in other words, every vote cast that has not since been cancelled). LOG4 contains all invalid votes, which are all votes that have been cast and not cancelled, but were filled out incorrectly. At this point, the voter ID numbers are no longer matched with votes. The only information stored in log entries in LOG4 are the votes themselves. LOG5 contains all valid votes which have been counted. Again, only the votes are stored in log entries in LOG5, and no voter IDs are stored which avoids the matching of voters with the contents of the votes that they've cast. The use of these logs allows for auditability. This can allow the reviewing of complaints, and the system can also allow a voter to be notified of the status of the vote he or she has cast. The integrity of the logs can also be checked. For example, LOG2 and LOG3 combined must equal LOG1; LOG4 and LOG5 combined must equal the content of LOG3. [13]

Mission criticality is catered for by the fact that internet voting is available to voters in an early voting phase only. Early voting is optional for voters in Estonia, and usually takes place 4-6 days before voting day. On voting day itself, only paper voting is possible. This means that if the Internet voting system did shut down, due to an attack or a bug in the system, voters would still be able to vote in person by paper on polling day. While this would lead to some voter dissatisfaction, and may also mean those who had planned to vote early may not be available to vote on polling day, this solution goes a long way to ensuring that the whole election does not hinge on the Internet voting system needing to be available constantly, and removes the idea of the system being mission critical. If a voter feels uncomfortable with a vote they have cast using the only system, they have a number of options. They can choose to vote again through the online system, which will automatically invalidate their previous vote. If early voting has closed or they do not wish to use the online voting system again, a voter can also choose to vote again on polling day through the paper voting system. Using the paper voting system at any stage will automatically invalidate any previous online votes. This feature of voting multiple times, with only your most recent vote counting, also allows the problem of vote privacy to be catered for. It ensures voters always have the option of voting in private, and ensures a coercer can never be sure of the contents of a person's final vote, for even if they do watch someone vote, they may not be able to stop that person from voting again if they so wish. [13]

While no serious problems have been discovered with the current system, and it's considered by many advocates of internet voting systems as a model that should be adopted by many more countries, it's important to note that there is no fool-proof way of ensuring no problems do exist in the system. This fact is highlighted by the fact that the source code of the system has not been released for public scrutiny. There is simply no way to ensure there are no subtle bugs in the system. Even though it seems as though everything has operated as intended so far, there is no guarantee that it will always do so. [13]

4.3 France

France is still on its journey towards the adoption of electronic voting technologies. In 2003, the Ministry of Internal Affairs introduced a procedure for the certification of voting machines, and listed the various requires a voting machine must abide by. These requirements were [47]:

- voter privacy and secrecy, including for disabled voters
- to allow elections of different types to be held simultaneously
- to guarantee that each voter cast only one vote
- to keep a running total of the number of voters, which can be read during the voting
- to count the votes obtained by each list or candidate, as well as the spoiled votes, which should only be readable after the voting has finished
- to use two different keys in such a way that during the voting process, one remains in possession of the vote office president and the other in possession of a designated member

The country first made use of electronic voting machines the following year, in 2004. The decision to take this step came about largely from the seeking of reducing administration and costs associated with elections [29][47]. While only 18 municipalities (out of 36,680) used electronic voting machines in 2007, this number increased to 60 municipalities during the 2007 French Presidential election. Some areas used the machines as experiments in legally binding elections, while others did not have any legal value. In the lead up to the 2007 elections, all French political parties except the UMP opposed the use of electronic voting [56]. There were no reports of problems with the machines [47]. Three voting machines were allowed for use by the various local authorities. One type was provided by the Spanish company Indra Systems; another by ES&S-iVotronic; and the third type provided by Nedap [56]. None of the approved machines provided a verifiable audit trail, and all stored the cast votes within the machine [29]. About 75% of authorities chose to use the Nedap Powervote machines [47]. These machines are very similar to the machines that were previously used in The Netherlands and the proposed machines in Ireland; however, the Netherlands has recently outlawed their further use due to serious security concerns and Ireland, after careful scrutiny of the proposed machines, abandoned all plans to introduced electronic voting (further details can be found in the 'Netherlands' and 'Ireland' sections).

The introduction of internet voting has also been attempted in France. This was first experimented with for government elections in 2006, when French citizens living abroad were given the option of voting in the Assembly elections over the Internet. To avail of this option, a voter had to inform his consulate of their desire to use this alternative method (as opposed to postal voting) at least six weeks before election day. Three weeks before election day, the voter would receive their voting authentication details.

4.4 Germany

In Germany, local governments are responsible for managing and financing election systems in their area. Cologne was the first to introduce electronic voting when it did so in 1998. Following the successful testing of the machines that year, Cologne used 600 of them in its European Parliament elections the next year [59]. Since then, many more regions followed suit, with 22 municipalities using the same machines in the 2002 elections and 30 constituencies using them for the 2005 Bundestag elections, which consisted of 1831 (out of 80,000) polling stations and more than two million voters (out of 60.5 million) [48]. Only machines authorised by the country's Minister of Interior are permitted to be used in elections, and Nedap's ESD1 and ESD2 machines were overwhelmingly chosen [59] [48]. Nedap is the same company that supplied machines to the Netherlands, which were subsequently abandoned due to vulnerabilities, and which also supplied machines to Ireland for pilot tests but were subsequently not adopted by the country.

It has been observed that a major factor for local governments in deciding whether to adopt electronic voting was the cost savings associated with such a move. In the city of Cologne, for example, it was possible to reduce the number of polling stations from 800 to 540, and reduce the number of workers at each polling station from 7 to 5 [59]. Proponents of their use also cited the speed of the results, the lack of errors in counting, and inherent security as reasons for adopting and continuing the use of electronic voting machines [48].

Although the system was not open source, and there was no paper audit trail feature, the German testing institute, the Physikalisch-Technischen Bundesanstalt (PTB), was confident the machines were adequately tested and that there was no need to change them from the originally tested machines. This followed thorough inspection of the machines, including line-by-line examination of the source code [59].

A research project looking into internet voting took place from 1999 to 2004. This research project was financially supported by the German Government, and included the testing of a system. Supporters of the system cited the possibility of higher voter turnout, lower costs, fewer mistakes in the casting of ballots, and the increased speed at which results can be determined [48].

Following the 2005 Bundestag elections, a number of cases were brought to German courts over the use of the machines. In these cases, a variety of claims were made about the machines, including that they didn't provide enough transparency, only computer experts could verify the system, and the inability to audit the results. Towards the end of 2006, a petition signed by 45,000 people calling for the abolition of voting machines, and criticising their lack of transparency, was submitted to the German Government. One court case taken by political scientist Prof. Joachim Wiesner and his son, software specialist Dr. Ulrich Wiesner, made its way to Germany's Constitutional Court [48]. In 2009, the court ruled on this case, declaring the use of the machines to be unconstitutional. They did not create a constitutional ban on the use of any e-voting machine, but said that any machine must be readily examinable and understandable by anyone without specialist knowledge in the subject. This has in practice ended the use of electronic voting machines in the country [29].

4.5 Ireland

Ireland ran its first e-voting pilot during the 2002 general election in three electoral constituencies, but before the machines could be used country-wide, the e-voting plan was completely abandoned due to concerns over the integrity of the systems following a number of reports into them.

In the proposed system, the hardware consisted of the voting machine itself (a DRE machine), the ballot module, a reading unit and a personal computer. A CD was also necessary to help perform the necessary functions. See Figure 4.2.

Before election day, a PC is used to load the election software from a CD. The software is then configured with the details of the upcoming election, and each ballot module to be used in the constituency is put into a programming/reading unit, where the configuration of the election is loaded onto it, including details of the polling station and centre for which the module will be used. Once they arrive at the polling centre for which they were destined,

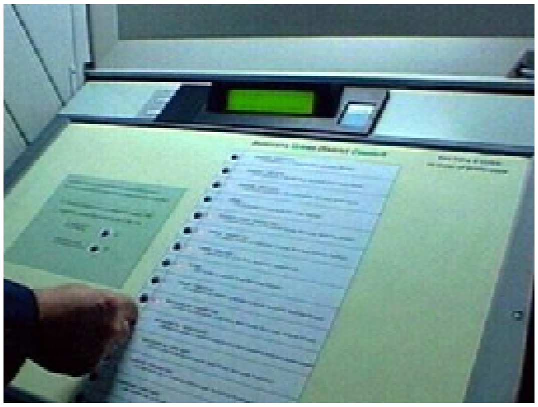

Figure 4.2: Ireland Voting Machine [45]

each ballot module is loaded into a machine.

On election day, the machines are set up as polling booths and a polling clerk activates the machine for each voter who wishes to cast a vote. The activation takes place via the control unit. Votes cast are recorded in the machine's ballot module. Once voting is finished, the ballot modules in each machine are removed and sent to the count centre.

For counting the votes, every ballot module is placed in a programming/reading unit and the votes transferred into the counting software on the PC [60]. The software counts the votes, and the results are announced after each count, as is normal under Ireland's PR-STV voting system.

A Government commission, called The Commission on Electronic Voting, published two reports on a number of issues found with the electronic voting machines and the processes used. The commission declared that it was not satisfied with the trustworthiness of the system. It also found a number of problems, including the fact that the counting algorithm was actually incorrect. Among its suggested considerations was the idea that a paper-audit trail was important for any voting system with integrity, and e-voting systems could develop a paper audit trail by having printed votes appear behind a glass screen for the voter to verify [60].

Following the publishing of this report in 2004, e-voting in Ireland had effectively come to an end. The machines were kept in storage and never used besides the previous trials. Any remaining trust in the machines continued to degrade as a group in the Netherlands demonstrated serious vulnerabilities in similar machines to the ones proposed in Ireland (see the 'Netherlands' section for more). It wasn't until 2009, however, that it was officially declared by the Government that the e-voting project would come to an end and the country's e-voting machines would be scrapped.

4.6 Netherlands

The Netherlands, previously, had fully embraced e-voting technology. The country's municipal elections in 2006, for example, saw nearly 99% of voters cast their votes on a voting machine. This includes the many voters who used internet voting. However, over a number of years, lobbying by action groups and demonstrations of the ease in which the e-voting machines could be tampered with have led to the country completely outlawing the use of e-voting machines. It has since moved its voting system back to the paper-based system [40].

Provision for the use of voting machines was first put into law in the Netherlands in 1965. It was not until the late 1980s until the first electronic voting machines were produced for the country's elections [31].

There were a number of different voting machines put into use in the country, the most popular being supplied by Nedap. Votes cast using the Nedap machines are stored in memory in arbitrary order, and no paper trail is used. Failure by the authorities to publicly release the source code of the machines meant there was no way for the public, or interested third-parties, to assess whether any problems existed within the machines. Nedap has supplied similar voting machines for use in German and French elections, and were also planned to be used in Irish elections [26]. During the e-voting project in Ireland, however, serious concerns were raised over the proposed voting machines (see the 'Ireland' section for more details). The concerns raised were numerous, and included a complaint about the ease in which the EPROM could be replaced: by breaking the paper seal. This is in comparison to the machines used in the Netherlands, where no seals at all were used.

More controversy hit the country's use of electronic voting machines when, in March 2006, a poll worker was accused of election fraud during the Municipal elections. The controversy occurred when it was revealed that one candidate received 181 votes in a single polling stations, when in all other polling stations combined he received just 11 votes. The candidate in question was also a poll worker in the station where he received the large amount of votes, and was responsible for controlling the voting machine [40].

Following this controversy, and the report on similar machines by the Irish Government, the Dutch Government announced in late 2006 that all the Nedap machines will now be sealed before elections. They brushed off other complaints by insisting the Irish studies did not apply to the machines used in the Netherlands [26].

However, more controversy struck the Nedap machines in October 2006, just a month before the country's general election, when a group campaigning against the use of e-voting machines publicly revealed a number of serious vulnerabilities with them. The group wrote a program to overwrite the machine's software and transfer cast votes from one candidate to another. They also wrote over the software to allow a user to use the machine to play chess. See Figure 4.3.

A final vulnerability showed that the secrecy of a person's ballot could easily be violated. The group detected that radiation emitted from the machine's screen could be picked up some distance away, via a tempest attack [31]. After an investigation by the Government, it was found that the most popular machines, by Nedap, did not radiate past 5 metres. However, other machines in use, by Sdu, could be read from over 30 metres [31]. The group

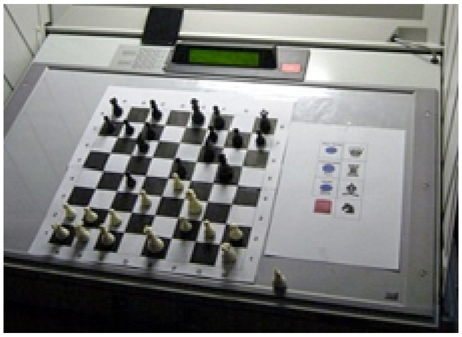

Figure 4.3: Netherlands Voting Machine Modified to Play Chess [41]

publicised these vulnerabilities on October 4th 2006 during a press conference [40]. The Sdu machines were taken out of operation by the Government just three weeks before an election.

A year later, two committees released reports on the electronic voting machines. The second report, 'Voting with Confidence', was released in September 2007. The report cited a lack of technological knowledge within Government departments, and a need for a paper audit trail. On the day of its release, the Government announced its intention to repeal the law allowing for the use of electronic voting machines in elections. In the mean time, the Nedap voting machines would be decertified for use. Because of the decertification of the Sdu machines a year earlier, this meant there were no longer any voting machines in use in the country. The electronic voting law was finally repealed a month later.

Internet voting has also existed in the country. Two internet voting projects were run during the same period; namely the Kiezen op Afstand (KOA) and the Rijland Internet Voting System (RIES). However, due to the controversy surrounding the electronic voting machines, plans for bringing in an internet voting system were put on hold. The source code of the RIES system was also scrutinised by the previously mentioned campaign group. Their scrutiny found a number of serious vulnerabilities existing in the systems which had not been detected previously [16]. Vulnerabilities included cross-scripting and token generation problems, as well as vulnerability towards SQL injection. This led to the use of internet voting in the Netherlands also ending.

4.7 Switzerland

Switzerland is one of the few countries to have provided legally binding internet voting as an option to voters. In 2007, there were approximately 5 million eligible Swiss voters. The country has a decentralised voting system, where each canton is responsible for setting their own election systems. The move towards internet voting, however, did come from the federal level when in 1998 the Federal Council of Switzerland, the country's executive body, adopted a strategy for the movement towards an e-government. This strategy consisted of two projects: to promote the use of the Internet for administrative tasks, such as tax services, and to promote the development of secure internet voting [24]. Two years later, an appeal by the Swiss Confederation was put out to the cantons to discover which were interested in developing an online voting system. Three cantons indicated they would be interested: Geneva, Zurich, and Neuchâtel. Because of the federal government's strategy, these three areas were eligible to receive government funds toward the project until 2004 [50]. Each of these three cantons provided internet voting as an option alongside two others: traditional voting (at polling stations) and postal voting. Postal voting and internet voting were only available in the days before election day [49].

Under the Geneva system, all relevant documents were sent to all eligible voters by mail three weeks before election day. With these documents, each voter would receive a postal ballot, ID and PIN. The ID and PIN allows each voter to vote online if they wish. To start the Internet voting process, the voter simply proceeds to the voting website and enters their identification number. Once they have filled in and confirmed their vote on the website, the voter needs to then confirm their identity by entering their date of birth and a PIN code. The PIN would have been received in the mail by the voter, however it's hidden under a rubber seal on the back of the postal ballot. The voter can reveal this PIN by scratching off the rubber seal. The removal of this seal makes it possible to ensure a voter does not vote by internet and by post, since the lack of seal would be noticed by poll workers processing received postal ballots. Once the vote has been submitted, the voter receives a confirmation [24]. A Java applet checks the integrity of each vote before it can be put into the eBallot box [50].

The Zurich system is very similar, with a few subtle differences. Firstly, they offered the option to vote by SMS during the first few years of their internet voting pilots, up until 2007. As well as sending the same information to voters as is sent under the Geneva system, voters are also sent a "fingerprint" to verify the validity of the browser certificate, as well as a special symbol. Once they have completed their voting, but before they have confirmed their selection, the voter can compare the symbol they received in the mail to the symbol being displayed on the website. This helps protect against voters being directed to incorrect, third-party copy websites. While SMS voting was available, voters received a table of SMS codes in the mail with their other information. If voting by SMS, the user would simply write a SMS message containing their ID, the code of the poll they wish to vote in, and a code based on their desired vote [24]. Once sent, they wait for a response, at which stage they send another SMS with their PIN and date of birth, in order to verify their identity. Encryption is deployed for messages sent between the voter's computer and the servers. A firewall is also used to protect the servers. Encrypted votes are saved in a database and also in a Write Once Read Multiple medium for extra security and redundancy [24].

The federal project itself ended in 2007, but many cantons continued with the technology. In 2008, many Swiss voters living abroad were provided with the opportunity to vote online. Geneva allowed other cantons to host their voter information on Geneva's system, since many did not have the technology available to provide for their own needs. For postal ballots, political parties were provided the opportunity to send controllers to election counts to supervise. For internet voting, these controllers were given the role of generating the encryption keys for electronic ballot boxes. This meant the controllers were the only ones able to open these boxes. In a February 2009 referendum in the canton, 70% of voters voted in favour of approving the introduction of internet voting. This referendum also changed the roles of controllers, instead replacing them and their roles with a permanent electoral commission. Except for Oracle databases, Geneva does not use any proprietary software in its internet voting system. They claim that 85% of the software they use is open source, while the remainder is owned by the state [50].

A number of arguments were used in support of the adoption of internet voting in Switzerland. The first was that it would increase voter turnout. The second was that it would improve the quality of the vote, where the voting website could also contain various impartial pieces of information about the election and the issues. A third argument made was that internet voting is important to be a modern society [49].

Arguments against the technology's introduction centred on the idea that it could lead to social exclusion in the form of a 'digital divide'. Another argument made was that people would end up putting less time into the process of voting, and therefore take it less seriously or could be more willing to vote based on emotion rather than informed choice [49].

Research into whether turnout has been increased due to the introduction of internet voting has been somewhat inconclusive. Because only a small amount of voters have been given the opportunity to use the technology so far, it's proving difficult to create relevant comparisons. However, it seems if the technology has in fact increased turnout, the increase is probably somewhere between 2% and 10%, and those who have voted by internet were primarily voters who would have otherwise voted by postal ballot [49] [24].

4.8 United Kingdom

It has been about ten years since the UK ran a series of e-voting pilots in a number of areas. In 2003 in English local elections, 18 local councils took part in an e-voting pilot, covering 1.5 million people [38]. Besides the usual kiosks that we'd expect to be involved in e-voting, other technologies trialled included voting by text message, internet, and digital TV. Unfortunately, a number of problems, particularly related to ill planning, resulted in a very negative reaction to attempts to bring in electronic voting. Problems included a lack of technical support, limitations to certain technologies (for example, no guarantee that an SMS will be delivered), and also serious breaches in security procedures. One such breach involved the ability for voters to access certain information online on polling day, even though the system's own security model stated this should only be sent through post for security reasons. Another security concern was the fact that many polling stations were not internet enabled. This meant that if a voter voted at a polling station, they could then return home and vote online without being stopped [38]. Pilots on various different technologies continued to take place; however, in 2007 the UK Electoral Commission recommended an end to the the pilots of electronic voting systems until the UK Government establishes a strategy to make the electoral system more secure [54].

Since then, the United Kingdom has adopted a very limited embrace of technology in elections. Paper ballots are still used by voters throughout the country, although some jurisdictions have used electronic optical scanners for the process of counting the votes. Most noticeably, optical scanners are used in the London Mayoral elections.

The use of optical scanning, however, has been far from problem-free.

During the Scottish elections in 2007, for example, voters were presented with redesigned ballot papers, which were necessary for use with the technology. It was found in an independent review that this new design caused great confusion among voters and led to 150,000 spoilt votes [10].

When the process of voting has concluded in London elections, ballot papers are brought to a counting centre in batches. It is not unusual for different elections to be held simultaneously, meaning ballot papers for more than one election may be mixed together. The e-counting technology can recognise and count different ballot papers for different elections in the same batch. It can also read them in any orientation. Each ballot has a printed unique security mark, which ensures the ballot is authentic.

The scanner, when processing the ballots, knows exactly where the votes should appear on the paper and what type of mark should be used, depending on the election type of the ballot. The scanner then applies all the correct election rules to each ballot paper and keeps track of the counts. Where it cannot interpret the voter's intent, it records a digital image of the vote which is sent to the returning officer's team for checks. Ballot papers not scanned successfully can also be manually put through the scanning again. Because of the unique bar-codes on each ballot paper, each ballot will only be counted once no matter how many times it's put through the scanner.

When members of the counting staff are judging a voter's intent where the machine was unable to, this judgement takes place by two counting staff in front of candidates and agents. Any ballots for which the voter's intention cannot be determined by counting staff, or any ballots that are clearly spoilt, are sent to the returning officer's queue. For any ballot paper that is determined to be spoilt by the returning officer, a reason for that judgement is recording on the system [2].

In practice, it seems the error rate for the optical scanning machines is unusually high. The use of the technology has caused a number of well publicised problems in previous London Mayoral elections. The controversy largely arose in 2008, when a report by the Open Rights Group claimed that up to 40,000 votes may have gone uncounted because of faults with the technology [34]. Faults with the actual process itself occurred in 2012 [64] where two whole batches of ballot papers were put into storage without being put through the e-counting machines.

Chapter 5

Oceania

5.1 Australia

In Australia, there are a number of electoral commissions that have jurisdiction over different types of elections. The Australian Electoral Commission manages national elections, whereas state or territory electoral commissions manage elections specific to their state or territory [11]. Electronic voting in Australia was used for the first time in October 2001 in an Australian parliamentary election, in the Australian Capital Territory (ACT) [11]. This followed a close election in 1998 in the territory during which numerous flaws were found in the hand-counting system. Two candidates had initially been separated by only three or four votes but, after recounting the 80,000 votes cast, it was found that about 100 mistakes had been made in the initial count [36]. This led to the adoption of an e-voting system called eVACS, which stands for Electronic Voting and Counting System.

Significantly, the eVACS system is Linux-based and open source [11]. The source code being available to the general public allows for a greater level of trust in the system. In the October 2001 parliamentary election, the first where e-voting was allowed, 8.3% (16,559) of all votes cast were done through the e-voting system [43]. Electronic voting was available in advance for those unable to vote on election day, and also available on election day in 8 polling places [43].

Despite the introduction of e-voting in the ACT territory in 2001, it was a number of years until other states in the country followed suit. There have been local and remote e-voting trials since then throughout the country, both at national level and at state level in the states of New South Wales, Tasmania and Victoria [11]. Most of these states, however, did not follow ACT's lead of ensuring the systems were open source. This is largely because their voting systems were procured from established e-voting vendors, who demand that the technical details of their systems remain secret [11].

In 2006, the Victorian state Electoral Commission (VEC) commissioned a third-party electronic voting system for use in polling places during elections [11]. The system is being developed in-house, and it's planned for use in the 2014 state elections in Victoria. The source code for the system will be released under an open source license [11]. One of the goals of the project is to achieve end-to-end verifiability of votes through the use of a cryptographic voting system. Such a system would allow a voter to verify that their vote has been encoded in the way they intended, with the authorities then providing a mathematical proof to show every that they have decrypted and printed all votes correctly. It should also allow anyone to verify that the overall election result is correct [11].

The state of Victoria is also designing a remote e-voting system solution. This is aimed at voters who have no other way of casting a private vote, and who are unable to travel to a polling place. Therefore, the system will be used only by those who are unable to cast a postal ballot, such as the visually-impaired or motor-impaired [11].

There have been limited attempts to introduce internet voting in the country. The State of New South Wales is one state where internet voting has been used. This came about with the implementation of the iVote system in March 2011, which was provided primarily for blind or visually impaired voters in the state [1]. The iVote system allowed voting by telephone and over the Internet. In order to use the iVote system, a voter was required to register through an application process. Once registered, the voter received a confirmation letter from the Electoral Commission and also an eight digit voting number via email, mail, telephone or text. Once the vote had been cast, the voter received a receipt [1].

Though the iVote system in New South Wales had initially been brought in to cater for blind or visually impaired voters, these voters only made up a small minority of the people who actually used the system. Of the 46,864 voters who used the system, just 2,259 voted by telephone; the rest by internet. Of those who voted by internet, only 1% were visually impaired. Voters who were otherwise disabled made up 2.5% of the votes, voters more than 25km from a polling place made up 3.5% of the vote, and voters who were outside of the state on election day made up the remainder (93%) of the votes. A small number of problems were experienced with the iVote system. One problem was an unexplained 8 minute outage of the system during voting. Another was that the number of votes printed did not match the number of votes contained in the decrypted voting file. This was due to a JavaScript failure that some voters experienced, and affected forty-three ballots. [1]

The federal government of Australia also introduced limited online voting for national elections. A trial took place during the 2007 federal election, which was limited to members of the Australian Defence Force (ADF) who were serving in various locations, including Iraq and Afghanistan. These members also needed access to the Defence Restricted Network (DRN) [1]. For members who had successfully registered to use the system, a PIN and voting instructions were sent to them via mail. To cast a vote, a voter would login on the DRN and enter the relevant information. Voting was then done through a Java applet executing in the voter's browser. A receipt was then issued to the voter, once their votes had been cast successfully. 1,511 voters made used of the Internet voting system in this election. [1]

Chapter 6

Analysis

6.1 Conclusion

A number of conclusions can be drawn from the survey in this report.

Firstly, this research has shown there is a huge array of different reasons why countries have chosen to adopt electronic voting solutions. These reasons include:

- tackling a diverse geography
- improving public confidence in the system by removing any threat, perceived or real, of vote rigging
- cost and efficiency
- improving accessibility for voters
- modernisation of the election process

With each reason comes a different set of criteria for a satisfactory e-voting solution. We saw in countries such as Brazil, which was primarily concerned with tackling a diverse geography, that their requirements could be reduced down to something that was simple, easy to transport, and allowed for a quick reporting of results. Understanding the reasons why governments may move towards electronic voting is vitally important. Much literature around this area, particularly from arguments opposing electronic voting, never considers governments' motivations, and rather simply discusses the risks involved and concludes that therefore governments should remain with voting by paper ballot. This, however, ignores the possibility that a government may be experiencing significant risk with their existing paper voting system. India is a perfect example of this, where their continuation of paper voting would have posed a serious risk to their democracy due to the rampant vote rigging taking place, including the stuffing of ballot boxes and the hijacking of vehicles transporting ballot boxes. While the argument that 'e-voting is risky' could of course be made to them, the fact is continuing with their existing system was not possible and it was determined electronic voting, while it had its risks, posed significantly less risk to them than paper voting.

Besides blatant vote rigging, voter confidence in the electoral system was also low in places like Brazil and the Philippines due to the extremely long waiting period between the conclusion of the voting and the announcement of the results. The waiting period could have been up to a month long in either country. This problem was due to the rural locations that voting equipment needed to be transported to. For example, in Brazil paper ballots needed to be transported to voters deep in the Amazon. Electronic voting, although carrying risks, allowed for the elimination of this significant problem and reduced the waiting period for election results down to just a few hours. These examples, among others, demonstrate the need to weigh the risks of electronic voting with the risks of remaining with a paper ballot system.

Of course, while the risks of remaining with the existing system may outweigh the risks of moving to an electronic voting system in some countries, like the ones just mentioned, it is clear in others that attempts to introduce electronic voting were made without any significant consideration of the risks involved, or the necessity of the technology. For many, e-voting was simply considered as a logical step for a country that wanted to be seen as modern and forward-thinking. Switzerland is one case where, during the debate on internet voting, the argument was made that its adoption is an important step for a modern society. Other countries described in the survey, such as Ireland, clearly had no overwhelming reason to move from paper voting to electronic voting, other than to be seen as a modern society. In these cases, where the risks of moving to e-voting clearly outweigh the risks of remaining with the existing system, the debate over the adoption of e-voting is weighted heavily in favour of those opposed to it.

Financial concerns, while not regularly cited by national governments, may play a larger role in the adoption of e-voting than would appear on the surface. This is because many national governments leave it up to smaller regional and local governments to select and fund their voting system. In particular, this played a significant role in Germany where local governments' primary motivations for introducing electronic voting was the reduction of costs. While this was an explicit motivation in Germany, it is worth considering whether this was an unknown consideration in many other countries. The survey in this report shows that a large number of countries with electronic voting have had e-voting introduced by local governments responsible for voting systems in their jurisdiction. It is possible that local governments with tight budgets, rather than the need to reduce a democratic deficit, have been a significant contribution to the adoption of e-voting throughout the world. This was also explicitly clear in the United States of America, where states moved towards electronic voting when money was made available for them to do so, but may would not later move to more secure systems in later years due to lack of financial resources to do so.

This research has also shown that, despite being around for decades, a consensus has yet to be reached on a number of important issues surrounding e-voting. The varying approaches taken by countries throughout the world shows governments have largely failed to learn lessons from each other on how best to approach the use of technology in elections. Governments have shown to be very hesitant in admitting the possibility of errors in their own systems, even when such possibilities have been clearly demonstrated elsewhere. This was most apparent in the Netherlands, where after several clear demonstrations of the vulnerability of their systems, the Government still refused to accept their systems were insecure. Even after a detailed report showing serious vulnerabilities in the systems was released, it was several years until the country put an indefinite halt to the use, and planned use, of electronic voting in their elections.

Despite this, there are a small number of encouraging signs of willingness by politicians and the public to pay attention to the scrutiny and vulnerabilities of their chosen systems. This was clear in Ireland where, despite the fact that plans had been made, pilots had been run, and e-voting machines had been bought at a considerable expense, the Irish Government ultimately backed down from plans to introduce e-voting nationwide due to the lack of public confidence in the plans. Similarly, some governments followed de facto best practices by ensuring the existence of a Voter-Verified Paper Audit Trail (VVPAT) or by avoiding the use of DRE machines completely. Countries such as India have moved to DRE machines with a paper audit trail from less secure systems.

While there has only been limited experimentation with legally binding internet voting, it is difficult to ignore the uniqueness of Estonia's implementation. Besides the fact that they may have had no real need for internet voting besides wanting to be seen as a modern society, their implementation overcame a number of problems traditionally associated with such a system. By allowing a voter to cast as many votes as they wish, with only the most recent being valid, they dramatically reduced the risk of a voter being coerced into voting a certain way, and also reduced a voter's ability to prove beyond doubt how they voted. This was strengthened by having internet voting available only during the early voting period, with a paper ballot still available on election the day; the use of which guarantees privacy and would override any previous votes cast online during the early voting period. The existence of a PKI system in the country is also crucially importance, and allowed them to get around the problem of securing a vote being transmitted over the Internet, and helped them deal with audit concerns. Of course, a major problem common through many electronic voting systems also exists with the Estonian system: how can the public know the system is doing what it's supposed to be doing? The Estonian Government does not make the source code of its system available for public scrutiny. While they may insist the lack of problems so far shows the system is secure and operating correctly, we have seen in other countries where systems that had been operating correctly for over a decade were later revealed to be highly vulnerable. A problem with Estonia and its use of the PKI system also depends on how much the public trusts its Government. If the Government can't be trusted to keep the vitally important and sensitive cryptographic information secret, then the whole electoral system may be at serious risk. However, any future governments who wish to adopt internet voting should certainly consider Estonia's model. While the introduction of a national PKI system may prove costly, if a government has a legitimate need for implementing an internet voting system, then the financial costs may be worth it.

From here on out, it is clear governments that wish to implement an e-voting solution should learn from the mistakes of others by ensuring sufficient redundancies are included, as well as a paper audit trail. While some governments may argue systems without such provisions have not yet experienced any problems, the survey of countries in this report has shown there have been cases where serious problems have gone unnoticed for a long time.

It's worth noting that e-voting has worked significantly better if used only when necessary, in conjunction with existing systems, rather than as a complete replacement of existing system. Hybrid systems can allow the best of both worlds: the security of paper voting and the speed of electronic voting. This is best demonstrated in Belgium. Important, however, is the need to realise typical development methodologies are not suitable for developing e-voting systems. This, in fact, is what makes e-voting systems so difficult. The 'Mission Critical' property means it is not good enough to wait until bugs have been discovered and expect to patch them once that happens. A methodology suitable for mission critical systems needs to be used. This is notable for cases like the United Arab Emirates, where the Agile methodology was used for the development of their electronic voting system. The use of this methodology probably is not suitable, and could mean problems go undiscovered or unresolved until it's too late. Some work has been done on the formal verification of e-voting solutions, as well as process modelling. Much of this, however, does not seem to have reached a stage where it could be easily used in the real world.

Some discussion has taken place with regard to the social effects e-voting brings, both positive and negative. In particular, a number of interesting social arguments were made against the introduction of electronic voting in Switzerland. One such argument was over the idea of a 'digital divide', where those unable to vote via internet, whether through lack of knowledge, ability, or generational reasons, would feel left out and disenfranchised by the system. Another argument was that voting would turn into a casual activity if it was made too easy, for example by allowing citizens to vote on their home computer. The argument was that voters would be less willing to inform themselves and would be more susceptible to voting based on emotion than research and information. A social argument, which came following Ireland's initial pilot, implied that the immediate declaration of the election result without any lead-up was cruel on the candidates. The previous counting process had consisted of paper ballots being counted manually in front of candidates and observers, with representatives of political parties able to watch the ballots and gradually determine the ultimate success of the candidates in the election based on observing the votes on each ballot. This was in contrast to the counting system in the e-voting pilot, where the final result was simply announced by the returning officer with no previous opportunity for party representatives to analyse the votes and watch the process.

Of course, it has been argued e-voting would bring a number of positive social effects. Many of these arguments were also made in Switzerland, including the idea that many more voters would feel included in the process and that by making the process easier it would encourage more people to participate in it. However, what is clear is that it is vitally important social effects are given real consideration before voting technology is implemented, in order to ensure no interested parties involved in the election system end up feeling excluded from the system.

Bibliography

[1] A Survey of Internet Voting. Technical report, U.S. Election Assistance Comission, September 2011.

[2] London Elects 2012. London Elects Guide to Electronic Counting 2012. `http://www.youtube.com/watch?v=tLAm0OBBZdM`, 2012.

[3] Your One Voice Can Make a Difference. 2010 Elections 101. `http://youronevoicecanmakeadifference.wordpress.com/2010-elections-101/`.

[4] Ahinda. India and Libya Sign MoU on Electoral Cooperation. `http://www.ahinda.com/india-and-libya-sign-mou-on-electoral-cooperation/`, 2012.

[5] Ali M Al-Khouri. E-voting in uae fnc elections: A case study. In *Information and Knowledge Management*, volume 2, pages 25–84, 2012.

[6] Dev Ananda, Amanda Bui, Janet Gonzalez, and Martha Prempeh. The future of e-voting. 2004.

[7] Eric Baculinao. Filipinos go to the (computerized) polls. `http://worldblog.nbcnews.com/_news/2010/05/07/4376624-filipinos-go-to-the-computerized-polls?lite`, May 2010.

[8] Steve Baron. Internet Voting - What New Zealand Can Learn From

International Trials & Errors. Master's thesis, Victoria University of Wellington, 2012.

[9] David Bismark. E-Voting Without Fraud. http://www.ted.com/talks/david_bismark_e_voting_without_fraud.html, July 2010.

[10] Electoral Commission (Great Britain). *Scottish Elections 2007: The Independent Review of the Scottish Parliament and Local Government Elections 3 May 2007.* Electoral Commission, 2007.

[11] R. Buckland and R. Wen. The Future of E-voting in Australia. *Security Privacy, IEEE*, 10(5):25–32, 2012.

[12] Emory University. Carter Center. *Carter Center Limited Mission to the May 2010 Elections in the Philippines: Final Report.* Carter Center, 2010.

[13] The National Election Committee. E-Voting System Overview. Technical report, Tallinn, Estonia, 2005.

[14] We Do Not Trust Voting Computers. http://wijvertrouwenstemcomputersniet.nl/English.

[15] Danny De Cock and Bart Preneel. Electronic voting in Belgium: Past and Future. In *Proceedings of the 1st international conference on E-voting and identity*, VOTE-ID'07, pages 76–87, 2007.

[16] The 'We do not trust voting computers' foundation. RIES - Rijnland Internet Election System; Very Quick Scan of Published Source Code and Documentation, 2008.

[17] The New Indian Express. Make Electronic Voting Machines Above Suspicion. http://newindianexpress.com/editorials/article1489577.ece.

[18] Competence Center for Electronic Voting and Participation. The New Electronic Voting System in Belgium – in use in 2012. http://www.e-voting.cc/en/the-new-electronic-voting-system-in-belgium-in-use-in-2012-archive-1211/.

[19] Organization for Security, Co operation in Europe. Office for Democratic Institutions, and Human Rights. *Republic of Kazakhstan Parliamentary Elections, 19 September and 3 October 2004: OSCE/ODIHR Election Observation Mission Report.* OSCE Office for Democratic Institutions and Human Rights, 2004.

[20] Organization for Security, Co operation in Europe. Office for Democratic Institutions, and Human Rights. *Republic of Kazakhstan Presidential Election, 4 December 2005: OSCE/ODIHR Election Observation Mission Final Report.* OSCE Office for Democratic Institutions and Human Rights, 2006.

[21] Organization for Security, Co operation in Europe. Office for Democratic Institutions, and Human Rights. *Republic of Kazakhstan Parliamentary ElRctions, 18 August 2007: OSCE/ODIHR Election Observation Mission Report.* OSCE Office for Democratic Institutions and Human Rights, 2007.

[22] Organization for Security, Co operation in Europe. Office for Democratic Institutions, and Human Rights. *Republic of Kazakhstan Early Parliamentary Elections 15 January 2012: OSCE/ODIHR Election Observation Mission Report.* OSCE Office for Democratic Institutions and Human Rights, 2012.

[23] Verified Voting Foundation. https://www.verifiedvoting.org/.

[24] Jan Gerlach and Urs Gasser. Three case studies from switzerland: E-voting. *Berkman Center Research Publication No*, 3, 2009.

[25] O Globo. TSE: Urnas eletrônicas resistem a tentativas de fraudes após quatro dias de testes com hackers e especialistas. `http://web.archive.org/web/20091117090258/http://oglobo.globo.com/pais/mat/2009/11/13/tse-urnas-eletronicas-resistem-tentativas-de-fraudes-apos-quatro-dias-de-testes-com-hackers-especialistas-914751763.asp`, 2009.

[26] Rop Gonggrijp and Willem-Jan Hengeveld. Studying the Nedap / Groenendaal ES3B Voting Computer: a Computer Security Perspective. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*, EVT'07, 2007.

[27] Nicole Goodman, Jon H. Pammett, and Joan DeBardeleben. A Comparative Assessment of Electronic Voting. Prepared for Elections Canada by Canada-Europe Transatlantic Dialogue, February 2010.

[28] Hiroki Hisamitsu and Keiji Takeda. The Security Analysis of E-voting in Japan. In *Proceedings of the 1st international conference on E-voting and identity*, VOTE-ID'07, pages 99–110, Berlin, Heidelberg, 2007. Springer-Verlag.

[29] Jordi Barrat i Esteve, Ben Goldsmith, and John Turner. International Experience with E-Voting; Norwegian E-Vote Project. Technical report, International Foundation for Electoral Systems (IFES), June 2012.

[30] Masahiro Iwasaki. E-voting in Japan: 2002-2009. Nihon University.

[31] Bart Jacobs and Wolter Pieters. Electronic Voting in the Netherlands: from early Adoption to early Abolishment, 2009.

[32] Dr. David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, and Dr. David Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). Technical report, Security Peer Review Group, January 2004.

[33] Dr. David Jfefferson. Electronic Internet Voting (The Threat of Internet Voting in Public Elections. Lecture as part of the Google Tech Talks series, December 2010.

[34] Bobbie Johnson. London mayoral election: doubts over 41,000 votes counted by machine. `http://www.guardian.co.uk/technology/2008/jul/02/london.mayor`, 2008.

[35] Douglas W. Jones. The Sailau E-Voting System. In *Direct Democracy: Progress and Pitfalls of Election Technology*, pages 74–95. Sep 2010.

[36] Sanjay Kumar and Ekta Walia. Analysis of Electronic Voting System in Various Countries. *International Journal on Computer Science and Engineering*, 3(5):1825–1830, 2011.

[37] Paul Laronde. Technologies in the Voting Process: An Overview of Emerging Trends and Initiatives. Research note, Elections Canada, May 2012.

[38] John Leydon. UK E-Voting Pilots Deeply Flawed. `http://www.theregister.co.uk/2003/07/31/uk_evoting_pilots_deeply_flawed/`, 2003.

[39] Radio Free Europe Radio Liberty. Kazakhstan's Electronic-Voting System Challenged. `http://www.rferl.org/content/article/1078191.html`, 2007.

[40] Leontine Loeber. E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years. In *Electronic Voting*, pages 21–30, 2008.

[41] Paul Miller. Dutch voting machines hacked to play chess. `http://www.engadget.com/2006/10/06/dutch-voting-machines-hacked-to-play-chess/`.

[42] Guillermo Lopez Mirau, Teresa Ovejero, and Julia Pomares. The Implementation of E-voting in Latin America: The Experience of Salta, Argentina from a Practitioner's Perspective. In Manuel J. Kripp, Melanie Volkamer, and Rüdiger Grimm, editors, *Electronic Voting*, volume 205 of *LNI*, pages 213–224. GI, 2012.

[43] ACE Electoral Knowledge Network. Countries With E-Voting Projects. `http://aceproject.org/ace-en/focus/e-voting/countries`, 2010.

[44] BBC News. Brazil Has Put a 'e' in Vote. `http://news.bbc.co.uk/2/hi/7644751.stm`.

[45] RTE News. Electronic Voting System to be Scrapped. `http://www.rte.ie/news/2009/0423/116606-evoting/`.

[46] Tengri News. Sailau E-system Will Not Be Used at Kazakhstan Parliamentary Elections in 2012. `http://en.tengrinews.kz/politics_sub/Sailau-e-system-will-not-be-used-at-Kazakhstan-parliamentary-elections-in-2012-5678/`, 2011.

[47] Consortium of Belgian Universities. BeVoting Study of Electronic Voting Systems, Study, April 2007.

[48] Consortium of Belgian Universities. BeVoting Study of Electronic Voting Systems, Study, April 2007.

[49] Consortium of Belgian Universities. BeVoting Study of Electronic Voting Systems, Study, April 2007.

[50] State of Geneva. E-voting home. `http://www.ge.ch/evoting/english/`.

[51] Brad Plumer. A quarter of Americans will vote by electronic machine. Is that a problem? `http://www.washingtonpost.com/blogs/wonkblog/`

wp/2012/11/06/thirty-percent-of-americans-will-vote-by-electronic-machine-is-that-a-problem/, 2012.

[52] Millenium Post. Bracing Democracy with Paper Trails. http://www.millenniumpost.in/NewsContent.aspx?NID=25332, 2013.

[53] Intel Free Press. Brazil Offering a Model for U.S. Elections? http://www.intelfreepress.com/news/brazil-offering-a-model-for-us-elections/195, 2012.

[54] European Digital Rights. Enough Internet Voting Trials Says The UK Electoral Commission. http://www.edri.org/edrigram/number5.16/uk-electoral-report, 2007.

[55] Jessica Roy. Voting Machine That Changed Obama Vote to Romney Vote in Viral Video Taken Out of Service. http://betabeat.com/2012/11/pennsylvania-voting-machine-that-changed-obama-vote-to-romney-vote-in-viral-video-taken-out-of-service/, 2012.

[56] Elaine Sciolino. Electronic Voting Has Come to France. http://www.nytimes.com/2007/04/03/business/worldbusiness/03iht-paris.5.5132376.html, 2007.

[57] Erik Sherman. Ohio faces controversy over voting machines. http://www.cbsnews.com/8301-505124_162-57545531/ohio-faces-controversy-over-voting-machines/, 2012.

[58] Smartmatic. Training for Electronic Voting in Salta (Argentina). http://digitalvote.wordpress.com/2011/08/23/the-long-road-of-e-voting-in-argentina/, 2013.

[59] Matthew P. Smith, Kieran Coughlan, Deirdre Lane, Danny O Hare, and Brian Sweeney. First Report on The Secrecy, Accuracy and Testing of

the Chosen Electronic Voting System. Technical report, Commission on Electronic Voting, Department of the Environment, Heritage and Local Government, 2004.

[60] Matthew P. Smith, Kieran Coughlan, Deirdre Lane, Danny O Hare, and Brian Sweeney. First Report on The Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. Technical report, Commission on Electronic Voting, Department of the Environment, Heritage and Local Government, 2004.

[61] Matthew P. Smith, Kieran Coughlan, Deirdre Lane, Danny O Hare, and Brian Sweeney. Second Report on The Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. Technical report, Commission on Electronic Voting, Department of the Environment, Heritage and Local Government, 2004.

[62] Andreína Vargas. The Long Road of E-Voting in Argentina. `http://digitalvote.wordpress.com/2011/08/23/the-long-road-of-e-voting-in-argentina/`, 2011.

[63] Carlos Vegas. The New Belgian E-voting System. In *Electronic Voting*, pages 199–211, 2012.

[64] Robert Winnett. London Mayoral Election 2012: Boris re-elected as London Mayor. `http://www.telegraph.co.uk/news/politics/london-mayor-election/mayor-of-london/9247635/London-Mayoral-Election-2012-Boris-re-elected-as-London-Mayor.html`, 2012.

[65] Scott Wolchok, Eric Wustrow, J Alex Halderman, Hari K Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. Security Analysis of India's Electronic Voting Machines. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 1–14. ACM, 2010.

[66] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman. Attacking the Washington, D.C. Internet Voting System. In *Proc. 16th Conference on Financial Cryptography & Data Security*, February 2012.