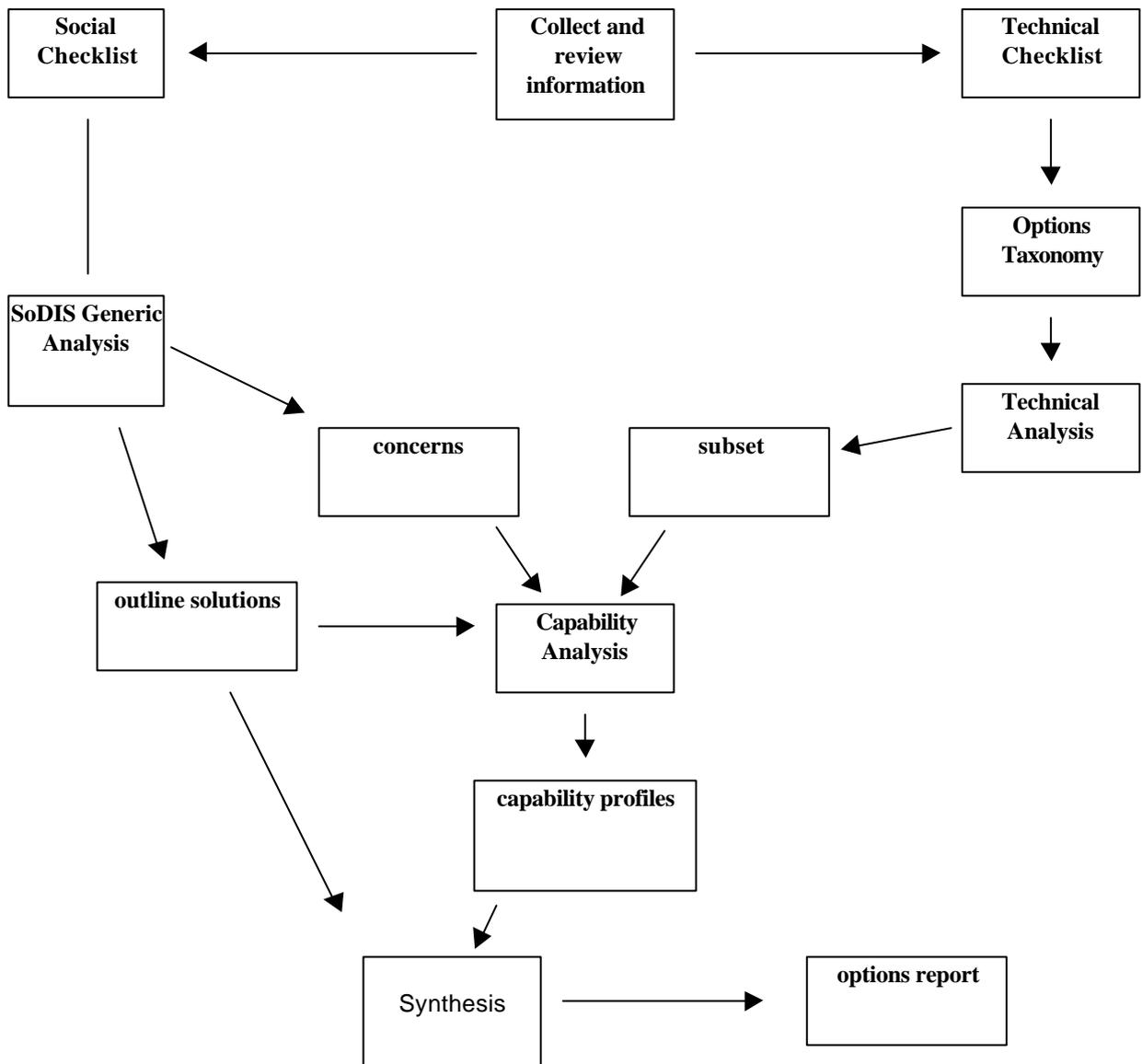# Technical Options Report

Dr N Ben Fairweather & Professor Simon Rogerson
Centre for Computing and Social Responsibility
School of Computing
De Montfort University, Leicester
email ccsr@dmu.ac.uk

This report describes the work undertaken to examine the technical options available for electronic voting. The task commenced with establishing a taxonomy of technical options and interrelationships. This was used to identify the most plausible and issue laden combinations. Each combination was evaluated against a detailed requirements specification which has been developed specifically for this purpose. The outcome of this detailed analysis comprises two main elements. First is a detailed account of the many issues that need to be resolved before any type of electronic voting can be implemented. The second main element is a detailed account of the most plausible options based on current and near-future technological developments.

Methodology

The approach adopted is illustrated in the diagram below. The first step was to review existing information and seek expert opinion. This enabled both the technical and social issues to be clarified. Consideration of the technical issues led to the formation of the options taxonomy. This taxonomy was subjected to a technical analysis in order to identify a subset of options that were worthy of further in-depth analysis. The social issues led to the development of the generic requirements and the identification of the stakeholders. These two elements were the inputs used for the SoDIS generic analysis which is described in detail later in this report. The outcome of this SoDIS analysis was a detailed list of concerns together with recommended solutions. The options subset and the list of concerns were then brought together in the capability analysis, which led to capability profiles for each option in the subset. These profiles together with the suggested solutions to the identified concerns form the overall findings of this work.

Methodology adopted

```
┌──────────┐          ┌──────────┐          ┌──────────┐
│  Social  │◄─────────│Collect and│────────►│ Technical│
│ Checklist│          │  review  │          │ Checklist│
│          │          │information│          │          │
└────┬─────┘          └──────────┘          └────┬─────┘
     │                                           │
     │                                           ▼
┌────┴─────┐                              ┌──────────┐
│SoDIS Generic│                           │ Options  │
│ Analysis │                              │ Taxonomy │
└──┬────┬──┘                              └────┬─────┘
   │    │                                      │
   │    └──────►┌──────────┐  ┌──────────┐     ▼
   │            │ concerns │  │  subset  │◄─┌──────────┐
   │            └────┬─────┘  └────┬─────┘  │ Technical│
   ▼                 │             │        │ Analysis │
┌──────────┐         │             │        └──────────┘
│outline solutions│  ▼             ▼
└──┬────────┬─┘  ┌──────────┐
   │        └───►│Capability│
   │            │ Analysis │
   │            └────┬─────┘
   │                 ▼
   │            ┌──────────┐
   │            │capability profiles│
   ▼            └────┬─────┘
┌──────────┐        ▼
│ Synthesis│────────►┌──────────┐
└──────────┘        │options report│
                    └──────────┘
```

Context

There have been a small number of attempts at public elections using the internet, with mixed success: perhaps the most prominent, the Arizona Democratic primary[1] 2000 seems to have passed without incident, while others, such as a referendum in the Netherlands, have had to abandon internet voting due to fraud (Nu.nl, 2001).

Throughout, our analysis has been working on the assumption that polling will, for the indefinite future, take place through multiple means, including use of (possibly modified) polling stations. If modified polling stations are used, extra staff will need to be present at those polling stations to help guide voters through any changed procedures. If electronic voting is introduced, there would be a temptation to reduce the number of polling stations since there would be a reduced number of people voting in person, and thus an opportunity to save money. But if any such reduction in the number of polling stations resulted in polling stations being further from home, people who don't vote electronically for whatever reason and who otherwise might have voted might be dissuaded from voting by the extra effort needed: resulting in reduced turnout, rather than the hoped for slight increase/reduction in the rate of decline in turnout. Further, if there is disruption to the electronic election, it may be necessary for polling stations to issue 'tendered papers' rather than ordinary votes. As this process is likely to take longer than the issue of a normal ballot paper does at present, a systematic attack on the election could swamp conventional polling stations too, even if the number of polling stations were not reduced.

While voting over several days may help ease some of the security problems, there is a severe danger that a proportion of voters will be unwilling to try again later if they experience trouble. If there is a preparedness for electronic voting to be accompanied by lower turnout, this need be no concern. If turnout is of crucial importance, voting over several days will not ease security concerns (although it might prove beneficial to turnout if security concerns prove to not be a problem).

We have been asked to work on a timescale of 'the General Election after next'. Given that the length of Parliaments is not fixed, twentieth century precedent tells us that the next general election could be perhaps in 2005, or maybe 2006, but the length of time until the following election could be anything between five years and about 8 months. Technology may develop quickly, but given that adequate time for testing and piloting *of the actual system that will be used* is required, there is little time for such developments to take place, if they are to be incorporated into an electronic voting system. The longer term prospects for particular technologies may be better.
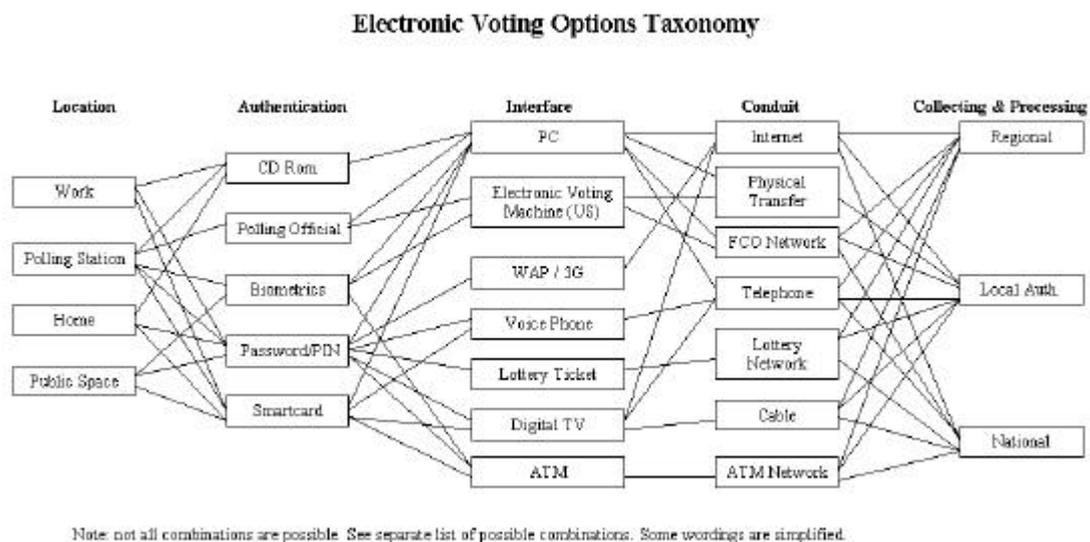
Technical options taxonomy

There are five elements of the technology enablers for electronic voting which are largely but not entirely independent of each other. These are the location, the authentication type, the interface, the conduit and the collector/processor. The location determines the degree of control over the voting process and the security of the interface. The authentication type describes something of the technical means for confirming voter identity: for all forms, the crucial part is the input into the computer system of some data which is taken as being

---

[1] According to some definitions the primary was not a public election, however, the role of the public in the election was essentially identical to the role of the public in a public election: for our purposes it makes most sense to consider it a public election.

sufficient to authentically identify an individual. The types refer to the different means for introducing this data into the system. The interface enables citizens to access the electronic voting system. The collector/processor cumulates, counts and reports the voting outcome.

Various combinations of the enablers within the five elements are possible: all possible combinations are illustrated by the diagram, but since the five elements are not entirely independent of each other, some combinations appear possible on the diagram which are not in fact possible.

Electronic Voting Options Taxonomy

Note: not all combinations are possible. See separate list of possible combinations. Some wordings are simplified.

SoDIS Project Auditor Requirement Analysis – Input Parameters

Any project goes through three distinct phases; an initial phase where the feasibility of the project is examined, a requirements phase that lays out the overall structure and function of the project and a detailed phase that lays out the plans for building the software.

Each of these phases has its peculiar risks. The purpose of the SoDIS (Software Development Impact Statement) Project Auditor (SPA) is to identify these risks in a pre-audit of each phase. It helps to keep track of a variety of concerns that may affect the development and the eventual impacts of a project. Once identified, action can be taken to avoid or resolve these risks before they negatively impact the project or those who will use the software. In the worst case it will help to identify infeasible projects before major expenditure has occurred.

The SoDIS process encourages the developer to think of people, groups, or organisations related to the project and its products or deliverables (stakeholders in the project), and identifies the potential risks for these stakeholders.

For the technical options analysis the requirements analysis function of SPA was used. The input parameters were established which would drive the SoDIS analysis. These comprised two main sets: stakeholders and general requirements. Stakeholders were subdivided by role and within each role there were individually named stakeholders. The list of stakeholders was as follows.

Stakeholders

Role	Name
Customer	Central Government
	Local Government
	Those seeking election
Community	Minority groups: those overseas, those with disabilities, those with linguistic constraints, those from minority ethnic groups, those belonging to fringe political parties, those with restricted movement for example on remand or in hospital long term, those living in rural areas
User	Citizens as voters
Vendor	Suppliers of technological elements
Developer	Systems developer

It was decided to focus primarily on stakeholders with the Community and User roles. This was because the purpose of the analysis was to ascertain the issues that might hamper the implementation of a particular technical option. Emphasis was placed on satisfying the needs and rights of the general public (represented in this analysis by Community and User roles).

Generic Requirements

Ten generic requirements have been identified against which all technical options should be judged. These are now described in detailed.

1 Security

Adversaries

Since the voting system is security sensitive, any sensible analysis of technologies must include a threat analysis at an early stage.

Hackers/Publicity Seekers

It should be assumed that there is 100% probability that hackers/publicity seekers would see a UK general election conducted largely by electronic means as a target. Attacks on prominent websites are routine. The first major democracy to use extensive electronic voting is liable to be attacked simply because it is the first. Moreover, even if electronic voting had already become routine, a successful attack on a UK general election could be expected to generate considerable publicity for the attackers. To generate such extensive publicity, serious doubt would have to be cast on the validity of the results in several parliamentary constituencies, at least, or inconvenience or annoyance caused to tens of thousands of voters. Attacks that can generate limited publicity, at most, can also be expected, including from those whose interest is the technical challenge, rather than publicity. However, the greater the disruption that it is possible to cause, the greater the publicity that could be gained, and thus the more likely an attack, *ceteris paribus*. Such attackers are unlikely to be prepared to take significant personal risks or use their own financial resources to a significant extent, which limits the extent of the threat from these adversaries.

Hostile Regimes

Regimes such as China, Russia and Pakistan are likely to have significant technical ability, facilities and resources at their disposal, should they *choose* to attempt to disrupt a UK election. While the probability of such attacks is lower than for attacks from hackers/publicity seekers, the resources at the disposal of such regimes are much greater, so they would be able to mount a very wide range of attacks. If (but only if) there is a possibility of causing substantial embarrassment to the UK regime or affecting the result of a UK general election in a way that is more favourable to the hostile regime, the probability and sophistication of such attacks is sufficiently high that any system should be able to withstand an attack equivalent to the most extensive that the UK security services could mount against such a system. If a system could be disrupted by the use of facilities available to our security services, the vulnerability to disruption from foreign regimes can be expected to be unacceptably high.

Partisans

There is a low probability of an attack from an existing mainstream political party in Britain of a sort that would not be otherwise defended against. However, given the potential rewards for controlling or influencing the government of the UK, and the sums of money that are currently spent attempting to gain influence and gain election, there is some risk that any system would face attempts at disruption that was intended to affect the result of an election. A significant part of this threat could be made up of the actions of activists and external sympathisers of parties who use techniques that the party would not approve of to secure its election. Equally, the possibility that some party not currently involved in UK politics would attempt to achieve election as the government through corrupt means cannot be completely excluded. Finally, the evidence suggests that some non-mainstream parties, such as the British National Party, may resort to illegal means to influence the election of sorts which would otherwise not be a significant concern.

Terrorists and dissident groups

With the state of the Northern Ireland peace process at the time of writing, the likelihood of threats that use techniques available to such groups but not available to hackers/publicity seekers in general is low. However, given the still fragile nature of the NI peace process, it would be unwise to design a system on the assumption that such threats will remain unlikely. The possibility that other dissident groups within the UK will acquire the capability for such attacks is also low, but cannot be discounted altogether. If such groups do attack a UK general election, it seems most unlikely that they will be able to successfully attack more than a handful of targets without prior intelligence enabling attacks to be thwarted. An electoral system that is not vulnerable to single (or small numbers of) points of failure should be able to resist attacks from these adversaries.

Opportunists within the system

Experience elsewhere in computer security suggests that systems are significantly vulnerable to insider attacks, with perhaps 70% of attacks coming from insiders (eg http://bob.nap.edu/html/trust/trust-4.htm, p112). Unusually for an application of computer security, financial gain cannot be achieved by corrupt insiders without external backers. Simple opportunism within the system is less likely than with many other systems. While

many with insider access are likely to have political views they might seek to promote, fewer will be prepared to risk their jobs and break the law to exploit opportunities that arise. By contrast, the likelihood of attacks using insider access is significant if such attacks are backed by financial inducements from a hostile regime, partisans, terrorists or dissident groups. Thus while insider opportunism doesn't increase the probability of an attack to any great extent, it could increase the severity.

Another possible attack is for technically competent attackers to seek to gain employment within organisations upon which the election depends.

Thus it cannot be assumed that insiders will be trustworthy.

This could particularly be a problem if the same insider or small group of insiders have "direct access to individual ballots, vote totals, population statistics, registration information, and preexisting voting patterns. It is possible for employees of election companies who provide full service operations to have access to all of these databases simultaneously. This information could then be applied in order to shift tallies in swing precincts in subtle ways that would be hard to detect. This is extremely powerful, since many elections are won by small percentages" (Mercuri, 2001, pp96-7).

Disruption by strikes, commercial contract disputes and failures

Any electronic voting system is inevitably much more dependent on the commercial world than the current system is. Most alternatives would depend on a single supplier (of telecommunications, for example) for some part of the process for a highly significant number of voters. Both trades unions and commercial contractors may attempt to exploit the leverage this gives them to pursue their own ends. There is a significant risk of contracts being breached, or there being credible threats to disrupt the election by breaching contracts. Given that time is of the essence, careful attention will be needed when legislation is drafted to ensure that the threat of such breaches of contract is nullified.

Conventional legal remedies may not be enough if suppliers are limited liability companies: "Given the recent rise and fall … in dotcoms, one should also be skeptical of doing business with voting system vendors who may not have the ability nor the intention to service their products or customers for the long haul." (Mercuri, 2001, pp37-8).

Geographical location

If voting is conducted using the internet in a substantial way it probably will be possible for an attack on the polling system to be launched from anywhere in the world, including places beyond the reach of British extradition. Another possibility is that the attackers could cover their tracks, using technical means to hide their true IP address. Other networks generally allow much stronger defence against attacks from outside the UK (although voting by satellite Digital TV may be vulnerable to electromagnetic attacks on the satellite from almost anywhere).

Conclusions on Adversaries

Systems must be able to withstand attacks from hackers and publicity seekers. Attacks from hackers and publicity seekers are going to happen. Better researched attacks might not happen, but cannot be ruled out. The more extensive the use of any system, the greater the probability of serious attack, *ceteris paribus*. Any system introduced for mainstream use

needs to be tested by UK security services and capable of withstanding any attack they could mount.

Vulnerabilities

Denial of Service Attacks

Denial of service attacks are a favourite technique of hackers/publicity seekers, often attacking websites. Other adversaries may also choose to use these techniques, "yet this potential problem has not been sufficiently addressed by the manufacturers and purchasers of electronic vote tabulation systems" (Mercuri, 2001, p98).

DoS attacks could target a wide range of parts of the system. Some possible targets are discussed below.

DoS attacks are a particular problem because elections are unusually time-critical (see also below under Reliability from Failures). An election held on a different day could well have a different result. If polling is spread over several days, a DoS attack after a piece of prominent positive publicity for one party (perhaps a party election broadcast, or a key speech reported on the news) could easily affect the election result. "The time-critical nature … makes this form of attack particularly likely" (Mercuri, 2001, p98).

Virus and malware

"not only is there no reasonable way to trust a client-side program in real usage, but there's no possible way to ever achieve that level of protection" (Schneier, 2000, p310). For our purposes this problem is moderated in that attackers have little or nothing to gain from subverting their own instantiations of the client-side program (assuming designs do not make the fundamental mistake of relying on the client-side program to prevent multiple voting, for example). However, they may be able to disrupt the election by subverting the instantiations on other voters' computers. Hackers and publicity seekers may well seek to exploit this route of attack by distributing a computer virus/worm/trojan horse infection that enables them to subvert the client-side programs for casting votes.

Any system that is dependent on pre-existing mainstream (MS) software such as web-browsers and operating systems is also vulnerable to attack from within the suppliers of such software. Despite the largest such company, Microsoft, having a record of rigging online polls (Judge, 2002), the probability of such attacks *is* low. However, it cannot be automatically assumed that all of 1) the software house(s) responsible for such software, 2) the distributors of that software, and 3) the relevant personnel within those organisations, will be benevolently neutral about the political situation in the United Kingdom. Because of the intimate relationship between such software and the computer on which it resides, such software, if so designed or manipulated, could interfere so that the apparent operation of the computer is normal, while, for some proportion of voters at least, votes are changed. While the probability of such attacks may be low, this is not the problem. It is not enough simply to not be attacked. There needs to be some way of **verifying** that such attacks will not affect the election, yet "verification that an arbitrary piece of software (…) performs a certain task, is known to be intractable". (Mercuri, 2001, p44). More must be known about all relevant software than is known about arbitrary software. Since the source code of mainstream software houses is not open to inspection, the only way to verify that an

election has not been subverted by attackers within mainstream software houses is to insulate it from their software.

The same problems of verifying the integrity of software apply whenever source code is not available for inspection, and thus also apply to all proprietary electronic voting machines that we are aware of. A further reason for being wary of off-the-shelf systems is that historically, in the United States (the world's largest market for automated voting systems) "Election system vendors are … forced by competitive bidding pressures to offer … the cheapest possible systems, and the products they offer do not maximize fraud protection." (Burnham, 1985).

Hacking of servers

A wide range of adversaries (including publicity seekers, hostile regimes, partisans and dissident groups) may make use of hacking techniques to attack servers.

Physical Disruption

The greatest risk of physical attacks could well be counting centres, which thus need to be defended against such attacks at least as well as the practical defences of current counting centres.

While the likelihood of attack is low, there is also some possibility of localised disruption to power and telephone networks. For individual voters, the best that can be done in the face of such disruptions may well be to go to polling stations/places as at present, however, such polling places will themselves need to be invulnerable to such disruptions, with computers able to use battery or generator power and insulation from failures with the fixed telephone network, perhaps through the availability of suitable equipment to use any mobile telephone networks for telecommunications.

Attacks on Privacy

Many attacks on privacy will essentially involve viruses or other malware, however, there are extra particular concerns.

A standard worry about privacy in elections is to ensure that the state will not be able to identify which way individual voters have voted. This is dealt with as a separate criterion, below; however, it is not just the state that might have an interest in such data. The full range of those who seek to influence the outcome of an election (including parties, family members and employers) may have a non-legitimate interest in identifying which way individual voters have voted.

Confidence Attacks

Whatever system is used, there is a serious danger that attempts will be made to cast doubt on the integrity and security of the system, regardless of whether integrity and security have actually be compromised.

2 Simplicity of the Voting Process

There are a number of types of reason for making the voting process simple.

Time

One would normally expect that the more complex a process is, the longer it will take. Given that one of the key anticipated advantages of electronic voting over traditional polling-station voting is time-saving, this may provide an argument for promoting simplicity in the voting process (in so far as is reasonably compatible with other requirements).

Even if a process which is complex is at the same time quick, prior awareness of the complexity may lead voters to wrongly suspect that it will be time-consuming, and thus dissuade them from attempting to vote electronically.

Cost

Cost is also of concern as an aspect of equity of access. However, even if there are no equity of access issues at stake, cost may be an argument for a simpler voting process. Costs which may be associated with a complex voting process could include: costs of production and distribution of more, and more expensive materials to voters; costs of educating voters; additional charges for connection time (where it is chargeable); and possibly charges for additional hardware and software for the voter or the provider of their computer/ICT.

If everything else is equal, cost savings should be promoted.

Likelihood of using

For all except the tiny minority of voters with a passion for problem-solving, complexity will be off-putting. If voters perceive that a system is complex, it is to be expected that they will use it in smaller numbers than if they perceive it to be simple to use.

Likelihood of making mistakes

Any voting technology should be a mechanism for accurately (*inter alia*) transmitting the wishes of the voter. It is possible to design a more complex system that *uses* the complexity to reduce the number of mistakes (for example, introducing error-handling procedures increases the complexity of a system). However, aspects of complexity that are not specifically designed to reduce the number of mistakes can normally be expected to introduce possibilities for making mistakes where none existed before.

Mistakes that do not affect the accurate transmission of the wishes of the voter are also a matter of concern. They can be expected to increase the time (and possibly cost) to use the system.

Likelihood of abandoning

A particular worry would be that voters would abandon an online voting session part-way through. Complexity could cause this either because the time taken (and possibly connection charges) was greater than anticipated, or because the voter (erroneously) lost confidence that the time taken would be as anticipated, or alternatively because the voter did not want to expend the mental effort to master the complexity.

The effects of abandoned voting sessions could be severely problematic. If voters attempt to vote by another means (such as going to a polling station) they could result in much higher demands on the system than anticipated, with some risk of overload that would have to be protected against. At an individual level, abandoned sessions could conceivably be taken

over by a subsequent user of the interface, resulting in effective personation (see below) with all of its effects.

Equity of Access

Simplicity will also have a role to play in ensuring equity of access for those who are less familiar with technology, or who have limited intellectual ability. The problems of complexity do not fall equally on all voters.

3 Reliability from Failures

Among information systems, the extent of the need for reliability in voting systems is unusual. It is not possible to suitably insure against financial losses caused by failures in the way that it would be with a business information system. Other considerations mean that it is impossible to reconstruct voting transactions from receipts.

Further, voting is a time-sensitive process: a significant proportion of voters may change the way they vote between the original polling day and any attempted rearranged polling day (for example in Winchester in 1997, when the general election result for the constituency was declared void, there was a 20% swing between the same two leading candidates when the byelection was held 7 months later). This is particularly likely if either there is political controversy accompanying the failure of the voting system or other results have become known. Thus if the entire election is postponed because of systems failures, the accompanying political controversy will change the way people vote; and if at a General Election, only the election in certain constituencies is postponed, the knowledge of the results in other constituencies will change the way people vote.

Smaller failures may not be quite so problematic, but there is a severe danger that a proportion of voters will be unwilling to try to vote again later, or by other means, if they experience trouble with an electronic voting system. If there is a preparedness for electronic voting to be accompanied by lower turnout, this need be no concern. If turnout is of crucial importance, levels of reliability that are exceptional for information systems need to be assured.

In Great Britain, the voting system is not directly safety-critical, but levels of reliability that are exceptionally high for non safety-critical systems need to be maintained.

One particular type of failure that *will* happen is communications failure during individual voting transactions. Any system must be able to cope with such failures without breaching the other requirements of the system. To achieve this, the recording of the fact that a voter has voted needs to take place when a (completed) vote is received from them rather than (for example) when a 'ballot paper' is issued to them. To meet this need, we anticipate a four stage process. First, the voter uses the voting software to transmit an identification message to the computer which records who has already voted. If no vote has yet been received for that voter, this is communicated back to the voting software local to the voter, which allows the voter to make their choice of who to vote for, and then sends that vote, along with identification data, to the computer which *then* records that they have voted. A confirmation of receipt of a vote is then returned to the voter (the issue of whether this should include confirmation of how the voter has voted is dealt with elsewhere). If no confirmation of receipt of a vote is received, the voter can attempt to vote again: if communication was lost before their vote arrived, they will not be recorded as having voted, and will be able to send a vote again; on the other hand, if the vote did arrive at the first

attempt, a message that they have already voted would be sent back, and they would be prevented from casting their vote again.

4 Anonymity of the Voter from the Regime

Legal research as part of this project emphasises the importance of a "secret ballot" in international treaties, in legislation and in international standards. Similarly, the stakeholder analysis as part of this project identifies it as a major concern for voters. For the purpose of analysis of the technological options, we have divided this into two aspects: anonymity of the voter from the regime (where the content of the vote must be revealed to be counted), and secrecy of the content of the vote from those who have no legitimate interest in it.

This division is important in the analysis of technological options because the separation of the vote from the identity of the voter largely requires different techniques, and takes place at a different time, from the shielding of the content of the vote from observers.

It is important that levels of anonymity are at least as good as the practical levels of anonymity in the current system[2], and ideally any new voting system would give higher practical levels of anonymity. With electronic counting of votes (whether or not accompanied by electronic voting) automated searching of votes becomes possible, and thus practical levels of anonymity may be reduced *without any change* in the observance of the principles at stake.

There is some evidence that anonymity from the regime is a live concern with current electoral practice in the UK, with a proportion of the electorate desiring greater anonymity than is offered (eg Bolton MBC, 2000, p2).

It is technically possible for a unique identifier to be generated for a particular election for each voter from which it would be impossible to return to the identity of the voter. To do so would make it possible for a voter to later claim that they did not have an opportunity to vote when they had in fact voted (Mercuri, 2001, p77), and would make it impossible to ask the voter as they entered the voting program if they were the particular voter whose identifier they were using.

Our model for the transmission of votes and identification data at the same time (see previous sub-section), can give an appropriate level of anonymity of the voter from the regime, but this requires that it is virtually impossible to associate how a particular individual has voted with their identity. This requires that even when the identity is checked against the register of electors and a record is made that the voter has voted, the content of the vote is (still) very securely encrypted, and that it is only decrypted once it has been passed on (by secure and reliable means) to another agency.

Thus this generic requirement requires that votes are very securely encrypted separately from any encryption of identification data. Given that regimes may have a non-legitimate interest in political affiliations held many years previously (remember the McCarthy question "are you now *or have you ever been*"), encryption may have to remain secure for many years. Yet increases in processor speeds and distributed cracking of encryption have repeatedly made encryption standards insecure, and can be expected to continue to do so (Mercuri, 2001, pp62-3). To guard against this, voters should be randomly allocated an identification number that could not later be associated with the voter, and the list correlating

---

[2] It is currently technically possible to make an association between identity and content of the vote by bringing together ballot papers and counterfoils. This association requires legal action, and extensive, time consuming, sorting of ballot papers.

numbers issued with names should be kept on a separate computer, under intense security separate from other parts of the voting system and the list should never be made publicly available until destroyed[3]. Given that automated sorting of ballots is possible, the security surrounding such a list should be greater than that surrounding the counterfoils for ballot papers under the current system. Thus we anticipate separate computers under the control of separate agencies fulfilling each of three separate tasks at each count centre: computer(s) A receive voting communications, decrypt them at the first level and then send the identifier to the computer(s) B that correlate the identifier with the electoral roll: if the identifier is valid and no vote has already been recorded, B records that a vote has now been received for that voter, and sends a message to A, which on receipt of that message sends the (still encrypted) vote to computer(s) C.

This is not a complete solution, but an important part of any solution.

5 Secrecy of Ballot

The full range of those who seek to influence the outcome of an election (including parties, family members and employers) may have a non-legitimate interest in identifying which way individual voters have voted.

As mentioned in the previous section, legal research as part of this project conveys the importance of secrecy of the ballot in treaties, legislation and international standards.

There can be little doubt that for a proportion of the electorate, even when voting for a mainstream party, being able to keep how one has voted secret is important, even when there is no reason to suspect that the information will be misused (Butler and Kavanagh, 1992, p142). Thus the stakeholder analysis as part of this project identifies secrecy as a major concern for voters. Similarly, in the public attitudes work for this project, the secrecy of the ballot was felt to be critical to the electoral process.

In circumstances where there is suspicion that the information may be misused, including those such as occurred in Oldham at the 2001 General Election, the importance of secrecy can be expected to increase.

Some have claimed that in order to reduce the intensity of the need for secrecy, voters should be able to change their votes: thus those who violate secrecy would have no way of knowing whether it was the genuine (final) vote that they violated the secrecy of. This is deeply problematic, in part because it may be possible for a hacker or other person to intercept the communication, or forage in waste bins and thus gain identifiers and any PINs, and after a voter has voted for what they thought was their final time, change their vote without their knowledge. The intense need for secrecy remains.

Marking the Ballot

Direct observation

A major concern is the possibility of others observing the screen (or listening to a spoken voting transaction). Technological solutions that make it more difficult for others to observe the screen are to be preferred, *ceteris paribus*. Where a solution cannot prevent others

---

[3] Perhaps at the end of the parliament for which the election was held: the point at which a challenge to the result can no longer have a practical effect.

from observing the screen, careful consideration will be needed about whether, on its own, this factor makes the solution unacceptable.

Remote monitoring of the screen

The primary risk of remote monitoring of the screen is where the computer is part of a workplace or similar network[4], which has been set up to allow remote support, administration and monitoring of activities. Such networks are increasingly common, as products to enable such remote support and administration become more common.
A second risk is where the computer has been compromised by a virus/worm/trojan horse or other malware that detects inputs and sends reports of them to the person wishing to violate the secrecy of the ballot (eg F-Secure, 2001).
There is also a smaller risk that van Eck radiation will be exploited to violate privacy: using such a technique "with the right equipment you can read someone else's computer screen from down the block - … everything leaks to some degree" (Schneier, 2000, p220). The costs of mounting such attacks, are however, likely at present to be sufficiently great to make them unlikely (estimates vary from $300 (Infinity, 1995) to £10,000's per receiver (Popkin, 1999)). If the cost of such technology drops dramatically this may come to be a significant concern, but it appears to not be at present.

Transmission

For virtually all forms of electronic voting, there will be a long, long way between the 'booth' where you mark the 'cross' and the 'ballot box' where votes are collected for a high proportion of voters: because there is such a long way, and the vote will pass through many 'hands', there is a particular problem with secrecy. Ensuring a system can be reliable in the face of communications failures (see above) requires that identification data is sent at the same time as the vote. Any electronic voting message sent unencrypted would be the equivalent of sending votes on postcards which have been marked in pencil, but with the difference that they will pass through the hands of commercial providers rather than the Royal Mail (and indeed could well go via overseas locations for convenience), and where the voter is identified by the postcard.
Secrecy in transmission is particularly important when the employer's telephone or data network is used. The public attitudes work for this project has shown that secrecy from employers was of particular concern. Employers may have all of access to relevant communications, the desire to influence votes and the ability to exert undue influence. Suitably secure encryption can provide secrecy of the ballot in transmission, as well as providing security from alteration in transmission. It is thus a requirement of all systems that they enable such encryption.

6 Integrity of vote tallying

Legal research as part of this project makes clear the importance of integrity in the tallying of votes.
In the United States "no one is making any attempt to hide the fact that vote tabulation is a business, that elections can be rigged, and that votes can be bought." (Mercuri, 2001, p92). There can be no question that this would be unacceptable in the United Kingdom.

---

[4] Other notable examples would be cyber-cafes and students using University networks.

Whatever system is employed in the United Kingdom, it should be impossible for corruption within a single supplier to affect the number of votes recorded.

For each counting centre, there should, thus, be at least two sets of servers, running separately developed programs. In the case of different results, in all cases an investigation should be launched to detect the origin of the difference, with previously determined procedures.

Even with parallel systems, collusion between those involved in the parallel systems is a possibility. The only real defence against attempts to cause biased software to be used requires ensuring that more is known about that software than arbitrary software, by making the source code of programs used openly available, with a legal requirement that authoritative results could not arise without open source code[5].

The only way to have software at the voter's end that is free from hacking and viruses is for it to be tested by enabling the security community as well as the hackers to attempt to find the problems. Open source software allows the expertise of the wider security community to be leveraged (Schneier, 2000, p344): such leveraging of the security community should enable more thorough testing than any which, in reality, could be bought by hiring the services of a relatively small number of security experts, although testing by paid experts is also needed, since making software open source does not guarantee any testing in itself.

7 Audit

It is not sufficient for us to believe that the election results are accurate: as under present electoral arrangements, there need to be procedures to both *check* that the results are accurate and that they have been arrived at by the correct procedures.

The audit should also be designed to reveal problems that are not necessarily related to the integrity of vote tallying, such as problems with connections, and thwarted attempts to abuse the system.

Once again, we must not repeat the experience of the United States "As audit controls for access and use of vote tabulation systems have typically been lax or nonexistent, the attack can be done in a straightforward manner, often with minimal technical skills or knowledge." (Mercuri, 2001, p98)

8 Prevention of Multiple Voting

It is a fundamental of contemporary UK elections that each voter has the same number of votes (i.e. one, for all elections where a single office is to be filled). There are currently procedures in place to ensure that voters are not able to obtain multiple (sets of) ballot papers, even if they both apply for a postal vote and attempt to vote in person, or if they enter the polling station more than once to ask for their ballot paper(s)[6].

Formally, prevention of multiple voting could be defined as the prevention of a person voting more times in their own right than the rules of the election permit.

---

[5] 'Open source' in this document means that the source code (and that of any compilers) would have to be open to inspection. It seems most likely that professional software development would be needed for specialised programs, rather than the ad-hoc collaboration associated with the 'open source' software movement. See also http://www.govtalk.gov.uk/rfc/rfc_document.asp?docnum=429

[6] Proxy voting, of course, enables someone to legitimately obtain two (or more) (sets of) ballot papers, but if done according to proper procedures, only by getting the permission of another voter (or voters), who is (are) then prevented from voting in person.

Any acceptable electoral system must prevent people from successfully voting more than once for a single office (and more than the permitted number of times where more than one office is to be filled), even if they attempt to vote electronically by any combination of the available means and in person at any combination of places where they are able to vote in person.

If an election uses parallel methods for voting, some technical method needs to be in place to ensure that a vote by one method will prevent a successful vote being registered by another: thus the electronic system described above (under reliability from failures) needs to be consulted and activated for all methods of voting in an election where electronic voting is enabled. This includes the circumstance of a paper ballot being issued by a polling official at a polling station. This requires real-time marking of online registers to record who is voting, and there is no reason for them to be anything other than nationally accessible.

9 Prevention of Personation

In Northern Ireland politics there is an oft quoted saying 'vote early, vote often'. This voting often is not achieved by simple multiple voting, so much as personation. Personation can be defined as taking someone else's opportunity to vote and using it yourself as if you were that person (without the use of a legally valid proxy vote) (with the possible further consequence that the person who has been personated will be denied the opportunity to vote).

In Great Britain, the prevention of personation at polling stations is usually dependent on the polling staff, and the exercise of their judgement about the circumstances under which those seeking to vote might be challenged.

Where electronic voting takes place in unsupervised locations technical measures are needed to prevent personation.

It is not sufficient for the techniques to prevent personation to work as a doorkeeping procedure. One particular possibility that needs to be protected against is 'electronic personation' where communications are intercepted, and the relationship of identification data to a vote is changed. Without such protection, it might be possible to copy the vote part of your own voting transaction (encrypted to meet requirements 4 and 5) and affix it to the identification data of intercepted votes in place of the votes currently affixed. This 'electronic personation' by intercepting communications is one example of how those who attempt personation can be expected to try to find ways round any doorkeeping procedure: procedures are needed to ensure that successfully bypassing the doorkeeping procedures is impossible. The particular possibility of attempts swap the vote part of electronic communications can be thwarted by securely encrypting the whole package of vote and identifier as a single encryption, once the vote has been encrypted. Other attempts at electronic personation will require other technical preventative measures.

10 Equity of Access

Current electoral arrangements uphold the principle that there should be no systematic discrimination of a sort that would make it more difficult for some eligible voters to vote than it is for others. This has been reinforced by moves to enable independent access to polling stations by more disabled people and the introduction of postal voting on demand for all voters.

There is currently some inevitable inequality of access because it is not possible for all voters to live equally close to polling stations, but this is moderated by having large numbers of

polling stations, the availability of postal voting, and its importance is moderated by the similarity of the demography of those living further from polling stations to the demography of those living closer to polling stations. If polling stations were only in city and town centres, and there had been an American-style flight to the suburbs of all who could afford to move, there might be cause for concern about the equity of present arrangements: as things are though, both the leafy suburbs and the sink estates will usually have a polling station within walking distance.

Electronic voting should, at worst, not increase inequalities in access to voting. Particular attention needs to be paid to ensure that systematic discrimination is not introduced, even if only in the form of systematically giving a proportion of the electorate easier access to voting than at present while another demographically recognisable proportion of the electorate do not have that opportunity.

On this basis, technologies that are more commonly used by some identifiable segment of the population than by other segments of the population should, *ceteris paribus*, be looked on less favourably than technologies that are more evenly distributed among the population.

Cost of Voting

A particular question of equity arises if voting is accompanied by financial costs of a sort that do not currently accompany voting. Demography clearly distinguishes between people according to their ability to make payments.

Factors that may be of relevance here could include the cost of any computer or other capital equipment that needs to be provided by the voter, costs of having a connection and other subscriptions (for example to the telephone system, and/or the internet), costs associated with a particular communication (such as telephone call costs), and other required costs (such as the cost of a TV License if voting is by digital TV).

Generic Requirements In Brief

A - Security from disruption by partisans and or opponents of the regime, and or terrorism.
B - Simplicity of voting process
C -Reliability from failures
D - Anonymity of voter from regime.
E - Secrecy of ballot.
F - Integrity of vote tallying
G - Audit
H - Prevention of multiple voting
I - Prevention of personation
J - Equity of access

These letters are used in the cluster tables below.

SoDIS Analysis

For this work only the requirements analysis phase was undertaken.

It was decided to focus the generic requirements analysis on Citizens as Voters and Minority Groups. The latter was used to identify any specific issues related to minority groups in general and specific groups in particular. In addition the 10 generic requirements were consider in the context of evoting in general.

The analysis has identified 103 concerns. These have been grouped into five clusters of issues as follows:

1. Individual
    1.1. Safety
    1.2. Privacy
    1.3. Cost
    1.4. Anonymity
2. System
    2.1. Usability
    2.2. Access
    2.3. Performance
3. Outcome
    3.1. Misuse
    3.2. Audit
4. Data
    4.1. Integrity
    4.2. Security
5. Context
    5.1. Environment
    5.2. Attitude

The tables below list the concerns identified for each issue. The letter identifying the generic requirement from which the issue emanated is shown in the first column. The concerns which suggested strategies for addressing them provide an agenda for government policy and legislation as well as terms of reference for developers.

Cluster: Individual

Safety

Req	ID	Concern	Possible Resolution	cluster
E	042	Lack of secrecy could cause danger to voters	voting at ATMs with added security	11
			voting software to include checks for surveillance software in operation - only partial solution	
			Encrypt votes during transmission so those with access to the network might not be able to see the voting outcome of individual voters	
			voting from public telephone boxes	
			voting at polling stations	
			voting under the supervision of a	

Req	ID	Concern	Possible Resolution	cluster
I	078	individuals might be at risk through the physical stealing of authentication instruments.	polling official secure and discrete delivery of instruments to individuals	11
I	088	A system that involves authentication instruments that can be physically stolen may result in voters being at risk.	Secure and discrete delivery of instruments to individuals. Avoid using voting interfaces that place voters at risk at the time of voting. If the risk of personation is high then the risk of harm may be high and therefore preclude some electronic voting.	11
I	093	If biometrics form part of the preventative measure there may be privacy, and health and safety issues relating to individual voters.	Design must include a full risk analysis of biometrics in this application, if they are used.	11

Privacy

Req	ID	Concern	Possible Resolution	cluster
C	025	Certain types of system failure might reduce the security infrastructure such that access to voter data might be accessible to unauthorised parties.	Treat security aspects of design with similar importance as is "safety critical" systems and adopt similar solutions.	12
D	034	Failure to achieve a sufficient degree of anonymity may result in an unacceptable violation of privacy.	Insufficient safeguards for anonymity may result in system rejection.	12
D	040	The likelihood of identification disclosure increases as costs of searching through ballots decreases. This is a particular concern for political minorities	Separate identity from vote cast as soon as possible and before the vote is decrypted. Encryption keys must be kept separate and adequate impartial protection of such keys in place for extended time spans.	12
E	043	Employers have a legitimate interest in computer and network activity which may conflict with secrecy of voting at work.	Factor in an effective ring fence around voting activity at work.	12
E	044	RIPA obligations may conflict with voter secrecy	If this is the case then a change in the law may be required	12
E	049	Privacy violations may result from inadequate or inappropriate protection of secrecy.	Ensure appropriate levels of secrecy, taking into account context, are included in the system design. Instigate public debate and expert opinion gathering leading to a political decision as to a definition of an acceptable level of privacy.	12
E	054	Most minority groups have an increased risk of privacy violation where specialist interfaces are in use.	Within the public debate and expert opinion gathering leading to a political decision as to a definition of an acceptable level of privacy, there should be an explicit consideration of this particular concern.	12
E	055	Those with linguistic constraints may need support from others if interfaces or authorisation tokens do not support any language they are fluent in which may cause privacy violations	Ensure the design includes multilingual support for a sufficient range of languages	12

G	064	The audit process may capture details of voter profiles	Take into account secrecy (including of the ballot) to ensure voter privacy when defining and implementing an appropriate audit trail during system development as well as in implementing operational audit procedures.	12
G	065	In order to have effective audit of technologies used by disabled voters, voter identity may be revealed.	The tension between audit and secrecy needs political, social and technical analysis.	12
H	074	Measures to prevent multiple voting may result in a loss of privacy.	Ensure design of the voter checking function takes into account the privacy rights of individual voters.	12
I	087	Measures to prevent personation may result in a loss of privacy. For example the procedure may require additional identification to be presented or input at the point of voting.	Design appropriate authentication functions at the point of voting to achieve an acceptable balance between personation prevention and voter privacy.	12

Cost

Req	ID	Concern	Possible Resolution	cluster
B	008	The minimum accessing system requirement may be greater than the specification of the system available to a voter	Optimisation of the system design is essential, as is the provision of access to minimum systems to those who do not otherwise have such access	13
B	009	Loading of the voting software might result in a voter incurring costs either financial or time or both	Optimisation of the system design and use of delivery technologies to minimise cost	13
B	010	Some authentication methods may result in an extra time cost since pre registration might be required	Minimise the time cost involved for example by going to the voter rather than the voter going to some central place to pre register	13
C	024	Loading of the voting software might result in a voter incurring costs either financial or time or both.	Optimisation of the system design and use of delivery technologies to minimise cost	13
D	032	The minimum accessing system requirement may be greater than the specification of the system available to a voter	Optimisation of the system design is essential, as is the provision of access to minimum systems to those who do not otherwise have such access	13
D	033	Loading of the voting software might result in a voter incurring costs either financial or time or both	Optimisation of the system design and use of delivery technologies to minimise cost	13
E	046	The minimum accessing system requirement may be greater than the specification of the system available to a voter	Optimisation of the system design is essential, as is the provision of access to minimum systems to those who do not otherwise have such access	13
E	047	Loading of the voting software might result in a voter incurring costs either financial or time or both	Optimisation of the system design and use of delivery technologies to minimise cost	13
F	058	The minimum accessing system requirement may be greater than the specification of the system available to a voter	Optimisation of the system design is essential, as is the provision of access to minimum systems to those who do not otherwise have such access	13
F	059	Loading of the voting software might result in a voter incurring costs either	Optimisation of the system design and use of delivery technologies to	13

Req	ID	Concern	Possible Resolution	cluster
		financial or time or both	minimise cost	
G	062	The minimum accessing system requirement may be greater than the specification of the system available to a voter	Optimisation of the system design is essential, as is the provision of access to minimum systems to those who do not otherwise have such access	13
G	063	Loading of the voting software might result in a voter incurring costs either financial or time or both	Optimisation of the system design and use of delivery technologies to minimise cost	13
H	071	The minimum accessing system requirement may be greater than the specification of the system available to a voter	Optimisation of the system design is essential, as is the provision of access to minimum systems to those who do not otherwise have such access	13
H	072	Loading of the voting software might result in a voter incurring costs either financial or time or both	Optimisation of the system design and use of delivery technologies to minimise cost	13
I	083	The minimum accessing system requirement may be greater than the specification of the system available to a voter	Optimisation of the system design is essential, as is the provision of access to minimum systems to those who do not otherwise have such access	13
I	084	Loading of the voting software might result in a voter incurring costs either financial or time or both	Optimisation of the system design and use of delivery technologies to minimise cost	13
I	085	Some authentication methods may result in an extra time cost since pre registration might be required	Minimise the time cost involved for example by going to the voter rather than the voter going to some central place to pre register	13
J	096	The minimum accessing system requirement may be greater than the specification of the system available to a voter	Optimisation of the system design is essential, as is the provision of access to minimum systems to those who do not otherwise have such access. Need to have convenient alternative methods of access (such as at a polling station) that do not require any additional resource requirement for the citizen.	13
J	097	Loading of the voting software might result in a voter incurring costs either financial or time or both	Optimisation of the system design and use of delivery technologies to minimise cost	13

Anonymity

Req	ID	Concern	Possible Resolution	cluster
D	031	Anonymity may not be attainable and automation removes or changes some of the practical solutions to anonymity attainment.	Consider alongside other issues during systems development and recognise that insufficient safeguards for anonymity may result in system rejection.	14
D	035	Identifying which votes have been cast using interfaces designed specifically for a special need could result in small groups of voters being identified implicitly or through an amalgamation of data.	System design must ensure that the interface used is decoupled from the vote cast as soon as possible.	14
D	039	Those at the intersection of several minority groups might be easily identifiable.	System design must ensure that the interface used is decoupled from the vote cast as soon as possible.	14

Req	ID	Concern	Possible Resolution	cluster
D	041	Voting through specialised interfaces may result in small subsets making identification of individuals possible implicitly or through an amalgamation of data.	System design must ensure that the interface used is decoupled from the vote cast as soon as possible.	14
E	045	Secrecy may not be attainable particularly when solely dependant on technology	During systems development secrecy needs to be considered in the wider perspective which may lead to technically feasible solutions being rejected	14
E	050	Voting not under the direct supervision of a polling official cannot guarantee secrecy of ballot.	Instigate an appropriate public awareness programme which acknowledges the limitations.	14
E	053	For some minority groups the family culture may make it difficult to vote in secret within the home environment.	Within the public debate and expert opinion gathering leading to a political decision as to a definition of an acceptable level of privacy, there should be an explicit consideration of this particular concern.	14

Cluster: System

Usability

Req	ID	Concern	Possible Resolution	cluster
B	006	Technologically assisted voting is inevitably less simple than traditional methods	The development should make the voting processes as simple to use as possible without compromising other essential requirements	21
B	007	Existing system specifications may be altered to aid simplicity of the voting procedure, for example turning off typematic	Design must ensure existing settings are restored on terminating the voting system	21
B	011	Over simplification may reduce choice, for example, having the ability to spoil a ballot paper.	Include such consideration in the system design.	21
B	012	Over complication of the system may prevent those, for example, with learning difficulties, voting independently	Undertake a thorough special needs assessment of interface technologies. Where necessary provide acceptable alternative interfaces.	21
B	016	Providing multilingual interfaces is costly and could increase the complexity of the interface.	A balanced approach to design must be adopted in order to support linguistic constraints whilst minimising complexity.	21
C	018	Design could lead to added complexity in the voter interface in order to realise the desired level of reliability	Ensure this tension is adequately addressed in the system development	21
H	073	Effective prevention of multiple voting may increase complexity unacceptably.	Need to achieve a balance between usability and prevention measures. This being informed by risk assessment and human interface assessment.	21
H	075	Biometric identification as a means of prevention may be inappropriate for some voters. For example, retinal scanning cannot be used by voters	Biometric identification can only be used if alternative means of identification are available to voters who need them and such alternatives	21

				21
		with some visual impairment.	do not lead to disadvantage.	
I	086	Effective prevention of personation may increase complexity unacceptably	Need to achieve a balance between usability and personation prevention. This being informed by risk assessment and human interface assessment.	21
I	089	Biometric identification as a means of prevention may be inappropriate for some voters. For example, retinal scanning cannot be used by voters with some visual impairment.	Biometric identification can only be used if alternative means of identification are available to voters who need them and such alternatives do not lead to disadvantage.	21
J	101	Provision of alternative interfaces might result in extra stages in accessing the voting process	The front end HCI design should reduce perceived complexity and time to access the voting process	21

Access

Req	ID	Concern	Possible Resolution	cluster
A	005	For those with access to voting solely through the Internet (eg overseas) disruption during the polling period will eliminate their ability to vote.	Provide alternative points of access as part of contingency planning.	22
B	014	Over complication of the system may prevent those, for example, with learning difficulties, voting independently.	Undertake a thorough special needs assessment of interface technologies. Where necessary provide acceptable alternative interfaces.	22
C	022	The minimum accessing system requirement may be greater than the specification of the system available to a voter	Optimisation of the system design is essential, as is the provision of access to minimum systems to those who do not otherwise have such access	22
C	029	Some minority groups require specialist interfaces of some description, therefore failure of such interfaces could lead to discrimination.	Factor in a high level of fault tolerance and reliability into specialist interfaces. Such interfaces require exceptionally stringent testing before any election.	22
E	048	By requiring a high level of secrecy in the voting process, some more popular evoting options may be excluded. This may mean that many, if not all, will fail to benefit from the evoting process.	Instigate public debate and expert opinion gathering leading to a political decision as to a definition of an acceptable level of secrecy.	22
I	080	Personation by family members	Education and warnings of legality on interfaces	22
I	082	Voters could lose their opportunity to vote through personation	The design of the system must include a voter authentication procedure that results in an authentication outcome that is at least as good as at present	22
I	094	The need to have an unofficial proxy for those with linguistic constraints may be curtailed through anti-personation measures.	Undertake a thorough analysis of this potential conflict to ensure this minority group need can still be satisfied, if by other means.	22
J	098	Lack of access to appropriate interfaces could lead to some forms of discrimination.	It should be Government policy to ensure adequate provision. This should include no reduction in the number of locations of existing polling stations. Ensuring the system requirements are minimised regarding interface hardware.	22
J	099	Particular interface technologies may exclude groups of disabled voters. For example, the telephone interface	Undertake a thorough special needs assessment of interface technologies. Where necessary provide acceptable	22

Req	ID	Concern	Possible Resolution	cluster
		excludes those with hearing impairments and ATMs could exclude those with mobility difficulties.	alternative interfaces. Legislation in place to ensure voting system caters for the needs of all voters	
J	102	Lack of equity of access may disenfranchise some voters.	Ensure all voters have adequate access to appropriate voting facilities.	22
J	104	Some minority groups, eg rural and socio-economic, have less access to appropriate technologies.	Need to have convenient alternative methods of access (such as at a polling station). In rural areas for example the use of post buses as electronic polling stations could be the alternative.	22
J	105	Members of minority groups with low rates of uptake of relevant technologies who are also disabled will not be able benefit from accessibility features built into the voting system.	Access to some minimum system sufficient to enable voting should be provided to those who would not otherwise have access to the technology. Have electronic voting facilities at polling stations equipped with a variety of accessibility tools.	22

Performance

Req	ID	Concern	Possible Resolution	cluster
C	019	Complete reliability is probably unattainable or an over emphasis on reliability reduces effort in other equally important aspects	Consider balance of approach at onset of system development	23
C	028	Inclusion of safeguards in system design may result in degradation of system performance	Optimise the system to achieve the necessary balance between addressing the issue and system response	23
D	038	Inclusion of safeguards in system design may result in degradation of system performance	Optimise the system to achieve the necessary balance between addressing the issue and system response	23
E	052	Inclusion of safeguards in system design may result in degradation of system performance	Optimise the system to achieve the necessary balance between addressing the issue and system response	23
H	077	Inclusion of safeguards in system design may result in degradation of system performance	Optimise the system to achieve the necessary balance between addressing the issue and system response	23
I	092	Inclusion of safeguards in system design may result in degradation of system performance	Optimise the system to achieve the necessary balance between addressing the issue and system response	23
J	095	Promotion of equality of access may result in computer system problems due to the "extra" resource requirement	Careful design of these functions must take place taking into account the minimum specification of accessing technologies used in the voting system	23

Cluster: Outcome

Misuse

Req	ID	Concern	Possible Resolution	cluster
A	001	These people may seek to alter votes in order to change the outcome of an election	Encrypt votes as soon as possible once entered to prevent and or detect an attempt to alter votes	31
A	002	These people may seek to alter votes in order to change the outcome of an election	Encrypt votes as soon as possible once entered to prevent and or detect an attempt to alter votes	31

| H | 069 | Failure to prevent or detect multiple voting may result in incorrect election results leading to danger to public. | Check who is voting against an electoral register, check voting status at both interface and collector/processor. checks must be separated from the actual vote as soon as possible as well as the vote being securely encrypted. | 31 |
| I | 079 | Result of election might be effected by successful personation | Develop an approach which identifies and prevents multiple electronic personation attempts without preventing legitimate concurrent attempts to cast a vote. Use of traffic trends through interfaces to trigger investigation might be an approach | 31 |

Audit

Req	ID	Concern	Possible Resolution	cluster
G	061	Audit must only consider the efficacy of the process and not capture any details of voter profiles - a precise definition of audit needs to be developed - It is an issue about the nature of the audit and associated trail.	Define and implement an appropriate audit trail during system development and ensure operational audit procedures do not conflict with secrecy of the ballot	32
G	067	Audit must only consider the efficacy of the process and not capture any details of voter profiles - a precise definition of audit needs to be developed - it is an issue about the nature of the audit and associated trail.	Define and implement an appropriate audit trail during system development and ensure operational audit procedures do not conflict with secrecy of the ballot	32
G	068	The conflict of interest between audit and citizens as voters is aggravated for certain minority groups.	Define and implement an appropriate audit trail during system development and ensure operational audit procedures do not conflict with secrecy of the ballot	32

Cluster: Data

Integrity

Req	ID	Concern	Possible Resolution	cluster
C	020	Voters could lose their ability to vote or their votes once cast	Ensure rigorous testing and implement effective disaster recovery operational procedures. Lessons could be learnt from measures adopted in safety critical systems	41
C	021	Software defects could cause the loss of data files	Effective testing procedures adopted	41
F	056	Tallying defects could result in errors in who is elected, the impact of which could be significant	Encryption of votes during transmission to prevent and or detect unauthorised and or accidental alteration of individual votes Appropriate effort during systems development to ensure integrity - it is essential to embark on a rigorous testing regime. Account needs to be taken of open source.	41
F	057	If proprietary software is used (directly or indirectly) as any part of the voting system it is extremely difficult to guarantee it free from vote tallying defects (black box concept)	Err on not using proprietary software unless open to inspection. Devise a strategy which leads to a system independent of such software	41
H	070	Some methods used to prevent multiple voting may result in the inappropriate modification of data files	Use other methods	41

Security

Req	ID	Concern	Possible Resolution	cluster
A	003	Tension between open source and the need to safeguard software from disruption whatever the threat	Solved by adopting open source policy and addressing security via other means	42
A	004	Issue of technical limitation and being able to anticipate the potential threat	Clarification of the issue by detailed discussion with technical experts may lead to a respecification of scope of evoting. Invoke potential problem analysis techniques to develop disaster scenarios, deterrents and preventative measures Consider the introduction of alternative concurrent forms of voting	42

Cluster: Context

Environment

Req	ID	Concern	Possible Resolution	cluster
C	017	Safeguards against will require redundancy to be built into the system which may result in additional environmental damage.	Undertake environmental audit as part of system development activity	51
I	081	Distribution of authentication instruments may have an adverse environmental impact	Produce and recycle instruments in sympathy with the environment	51

Attitude

Req	ID	Concern	Possible Resolution	cluster
B	013	An ease of development focus may result in simplicity of voting process at the expense of the demotion of equally important considerations	A balanced approach to design must be adopted to ensure the breadth of stakeholder needs is adequately catered for.	52
B	015	Inadequate concern regarding simplicity of voting	Ensure design and implementation addresses simplicity of voting effectively.	52
C	026	There is a temptation to suggest the system is more reliable and secure than it really is.	Design and test processes such that levels of reliability and security are genuinely sufficient to alleviate public concern. Ensure transparency regarding communication to the public both at the time of design and implementation and ongoing as difficulties may be discovered through live usage.	52
C	027	Inadequate concern regarding reliability	Ensure design, testing and implementation addresses such issues effectively.	52
D	036	Public ignorance of anonymity limitations could be perpetuated in electronic voting.	Instigate an appropriate public awareness programme.	52

D	037	Inadequate concern regarding anonymity	Ensure design, testing and implementation addresses such issues effectively.	52
E	051	Inadequate concern regarding secrecy of ballot	Ensure design, testing and implementation addresses such issues effectively.	52
F	060	Inadequate concern regarding vote tallying	Ensure design, testing and implementation addresses such issues effectively.	52
G	066	Inadequate concern or inappropriate implementation regarding audit	Ensure design, testing and implementation addresses such issues effectively.	52
H	076	Inappropriate levels of concern regarding multiple voting	Ensure design, testing and implementation addresses such issues effectively.	52
I	090	Some systems may be unable to achieve a level of security against personation which satisfies public expectation.	Instigate an appropriate public awareness programme which acknowledges the limitations.	52
I	091	Inappropriate levels of concern regarding personation	Ensure design, testing and implementation addresses such issues effectively.	52
J	100	Inadequate concern regarding equity of access	Ensure design addresses equity of access effectively.	52
J	106	There may be a tendency to focus on the needs of the unexceptional citizen at the expense of those in the minorities.	Ensure that the needs of all types of voters are taken into account and catered for in the system design. Resource limitations should not lead to those in minority groups being disproportionately excluded.	52

Key Actions

- For technical solutions where it is not possible to prevent others from observing the screen, instigate a public debate leading to a political decision as to a definition of an acceptable level of privacy and secrecy, including explicit consideration of issues relevant to minority groups who may be using specialist interfaces, and where family pressures make secret voting in the home difficult. There is a crucial disanalogy between electronic voting using normal display screens and postal voting because screens are normally larger and less portable than paper and pencil, less easily hidden from view and less easily taken to another venue where privacy could be more easily attained.
- System design methodologies must embrace social impact: 'off the shelf' commercial design methodologies as implemented by major contractors can be expected to be inappropriate. For example, in this application of an information system, it is wholly and grossly inappropriate for the design to consider: that a certain proportion of disabled people need not be catered for; that errors are just another design factor that can be simply factored against financial considerations; or that secrecy can surround the design and the choices made as part of the design.
- Development of a voter friendly system should be based upon the concept of inclusive design. That is based on providing facilities for all that cater for the needs of all voters including those with disability, linguistic constraints and restricted literacy.

The use of adaptive interfaces will be important so that the view of the system is sympathetic to the needs of the individual voter. There needs to be legislation in place to ensure that the voting system as a whole caters for the needs of all voters.

- Provision for audit should be incorporated into system development from the outset. The audit should not capture details of voter profiles, and should maintain secrecy of the ballot. Further political, social and technical analysis of the tension between audit and secrecy is needed, including explicit consideration of interfaces used by minorities (whether disabled voters or geographical or linguistic minorities). Thorough procedures for audit need to be developed that provide assurance that integrity of vote tallying is achieved, and that reveal any other problems with the system (that have not affected the integrity of vote tallying), such as dropped connections, problems with any specialist interfaces, and attempts to abuse the system, all without jeopardising the anonymity of individual voters.

- Achieve cross-party acceptance not just that undue influence from businesses has not taken place, but also that it is impossible. A system that relies to a significant extent on the use of the facilities of a major business (such as News International, the banks, or BT) is in danger of being accused of being unduly influenced by that business. Systems that cannot achieve cross-party acceptance should be rejected as being too susceptible to confidence attacks.

- To stand any chance of maintaining privacy and prevent votes being altered in transmission, votes need to be put in an 'envelope' of encryption, and there need to be mechanisms to prevent "bypass, deception, trapdoor or other malicious circumvention of an entire crypto system" (Mercuri, 2001, p61). For voting using standard computers running their normal operating systems, "Since the environments (operating systems, compilers, etc.) upon which the crypto systems rely are inherently weak, vast security holes persist" (Mercuri, 2001, p61). The solution to this problem for standard computers is to bypass the software on already on the computer, providing a specialised operating system of known quality.

- Encryption keys must be kept separate and adequate impartial protection of such keys in place for extended time spans.

- Voters should be randomly allocated an identification number that could not later be associated with the voter, and the list correlating numbers issued with names should be kept on a separate computer, under intense security separate from other parts of the voting system and the list should never be made publicly available until destroyed.

- De-couple voter identification data (explicit and implicit) from the vote as soon as possible after the vote is received.

- All identification information must be separated from the vote while the vote is still securely encrypted. To achieve this, the identification communication needs to be encrypted separately from the encryption of the vote, so that the authorities who decrypt the identification data and check it against the register of electors to ensure the voter is eligible and has not already voted, cannot discover how that voter has voted. In practice this requires two levels of encryption, and thus the distribution of encryption software that is capable of encryption, separately secure, of the two elements.

- Equity of access requires that if a significant proportion of voters can use hardware they posses (whether PC, digital TV, or some telephone technology) to vote, and there is demographic inequality in the distribution of such technology, access to some minimum system sufficient to enable voting should be provided to those who would not otherwise have access to the technology.

A Comparison with Other Secure Transactions

It is useful to compare voting with other online transactions for which security is needed. The most obvious comparison is with banking. Attacking an electronic voting system is unlikely to bring the immediate financial rewards that a successful attack on the banking system would, and thus some types of well-resourced attack are less likely. However, the likelihood of well-resourced attacks is still sufficiently high to be problematic.

The consequences of a successful attack are very different with electronic voting, than with banking, though. Banks can, and do, take a financial analysis of how much loss they can stand and insure against such losses. It may be that a political decision could be taken that the loss of a certain percentage of votes is acceptable, but in the absence of such a decision, security appropriate for banking cannot be considered sufficient for electronic voting. Banks have also maintained confidence in the face of repeated losses through computer crime by covering up the cause of those losses. It is inconceivable that, in the event of a successful attack on electronic voting, such a cover-up would be acceptable to the electorate if subsequently disclosed. In a similar vein, individuals can be, and are, compensated for financial losses due to disruption/failures/hacking of online banking. It is not easy to see how there could be equivalent compensation for disruption/failures/hacking of an individuals vote, even if somehow it was discovered which individuals were affected (which might not be possible with some sorts of disruption).

Another issue is anonymity: electronic voting "differs from the aforementioned applications due to the fact that, in addition to the requirements for accuracy and privacy, there is the mandated necessity to provide ... anonymity. In other words, banking … applications can (in fact must) allow tracking back to the user of the system, but the [electronic voting system] must ensure that such tracking is impossible." (Mercuri, 2001, pp8-9).

Electronic voting also differs from financial transactions in that the risk that an election delayed by a few days will have a different result is unacceptably high. By contrast substantial financial transactions between two willing partners usually can be conducted a few days later if there are problems with ecommerce applications, since such transactions are rarely conducted on a whim.

The Options

PCs

Personal Computers of all types, and whatever software is loaded, are a technology that makes it difficult to prevent others from observing the screen, unless they are used in a supervised location.

The risk of virus/malware attack will be greatest if general purpose computers are used by individual voters. Such computers will, almost universally, be vulnerable to attack by novel viruses/malware, since virtually all 'virus protection' facilities rely on a library of known viruses/malware. In the case of home computers, few currently have any 'virus protection'

and even fewer have regularly updated libraries of known viruses/malware. Any virus widely distributed in the months before the election could be expected to be present on a high proportion of *home* computers, if such a virus did not make its presence felt to the individual user concerned in advance of the election. Viruses are already in widespread circulation that can detect anything typed on the keyboard (eg F-Secure, 2001). It would be relatively easy for a virus writer to write a virus that did nothing (except propagate itself[7]) until a web browser was directed to "election.gov.uk" or a similar address, but which then was capable of changing the individual's vote, or preventing the individual from voting, or sending a copy of their vote to some other destination (violating the secrecy of the ballot). It might be thought that this problem could be overcome by distributing 'virus protection'. At present with low levels of broadband takeup, if such a distribution was conducted 'down the wire' as part of the voting process, the downloading of the software onto the user's computer could be prohibitively time-consuming. A theoretical alternative might be to distribute 'virus protection' facilities on disk, however to be successful, the library of viruses included would have to be very contemporary. Considerations elsewhere suggest that the contents of such a disk would have to be open source and open to scrutiny by experts appointed by the Parties for a specified period prior to the election. With disk production and distribution time as well, there would be a danger of viruses being propagated between when the contents of the disk were finalised and the election. This could be mitigated by including an internet address to check for updates, but such sites (a large number to reduce denial of service dangers) would equally have to be running open source code, available to scrutiny by the Parties, and even if no updates were needed, the extra time taken for the voting process to go through this extra stage would be problematic.

A better solution is to bypass the software on which such viruses/malware depend, providing a specialised operating system and set of drivers of known quality and without the basic security vulnerabilities of mainstream (MS) software on the disk (California Internet Voting Task Force, 2000, p4). The process of loading such an operating system and drivers would detract from the convenience some hope for from PC-based voting.

It will be exceptionally difficult for the specialised drivers to include drivers for the full range of specialised interfaces that make PCs compatible with the needs of groups of disabled people.

If general purpose computers are used, with software being loaded for the purposes of the election, there is a serious danger that any failure of the system that coincides with the general time of voting will be blamed on the voting system. It is quite plausible that attempts will be made to claim recompense for damage that far exceed any damage that the voting system may have caused. This is equally a problem for all solutions that use general purpose computers.

Voting from Work

Voting from work opens particular challenges: employers claim a right to monitor activity in the workplace, and it would be virtually impossible to exclude voting from such monitoring

---

[7] For home users who do not have 'virus protection' with a regularly updated library, a virus that propagates itself slowly is probably more of a threat, since such a virus is less likely to get media attention, and thus less likely to come to the attention of the individual. If such a virus also restricted itself to ISPs who serve the home user, the chances of detection would be considerably reduced.

and maintain secrecy in the voting process, unless workers are in individual offices, and certain technical measures to monitor are disabled.

Voting by PC from **suitable** workplaces might be a possibility, apart from technical constraints. Security issues preclude the use of PCs and general purpose computers unless the installed operating system is bypassed. Many work computers will have been, wisely, set up to prevent this. Further, work computers will generally connect to the outside world through a local network that will be practically impossible for the specialised operating system and drivers to navigate.

If votes are encrypted and not capable of decryption by the corporate firewall, they may be prevented from reaching their destination by the firewall, while if they are not encrypted they voters would be in very grave danger of having their employer know how they vote, and able to unduly influence this, and there would be no security to ensure that the vote was not changed, whether by the employer or somebody else on the network.

Issues with telephone voting are dealt with elsewhere.

Supervised Polling Place

We believe the worry about other software installed on the machine (Coleman et al, 2002, p69) is not sufficient to justify election-dedicated equipment to be required, provided that when used in an election, all software that can be used by the computer is of known quality, and in particular that a specialised operating system and drivers are provided and that any pre-existing general purpose operating system and hard-drive is completely prevented from interfering with the election software.

Within the environment of supervised polling place either electronic voting machines or general purpose computers will provide an adequate technical solution provided the software (and especially in the case of electronic voting machines, the hardware) is known to be trustworthy. Low-specification, reconditioned, general purpose computers would be adequate, and thus probably a cheaper solution; while electronic voting machines may include screening to hide the voter, or offer touch-screens (which may be useful for a proportion of voters), or some other advantage. Existing electronic voting machines should not be accepted unmodified since "hooks and backdoors, particularly those within compilers and operating systems, exist and have already been proliferated invisibly throughout the industry. Under this view, software rigging is assumed to have already happened, rather than just a speculative possibility." (Mercuri, 2001, p49).

Transfer of the votes to a counting and processing location could be accomplished adequately by physical transfer, or, encrypted over the telephone network to a modem on a dedicated (secret) telephone number. Encrypted votes could also be sent from supervised polling places in Embassies, High Commissions and Consulates overseas using the FCO network. If such conduits were not available, encrypted votes could be sent over the internet with less problems than would accompany sending votes from home computers, since the polling official can ensure that the polling place computer is virus free, and can ensure that a connection has genuinely been made with the correct server (bypassing DNS if necessary).

When used in a polling station environment, we would recommend that a paper ballot is printed for voters to examine (but which they are prevented from removing) to provide a paper audit trail (see Mercuri, 2001, pp54-5).

Voting at Home

With all sorts of voting from home, the voting system cannot, with current technology, prevent others from observing the screen (or listening to a voice telephone call) while the voting transaction is taking place. Voting from home should not be introduced without a public debate about acceptable levels of privacy and secrecy.

One of the major barriers we see to internet voting is that there appears, at present, to be little prospect that internet access (including home and workplace access) will reach 90% of the voting population, except through interactive digital TV (and if voting is to be conducted using iDTV, it would be better to use direct connections rather than routing through the internet). The Government, by contrast, is committed to achieving such high levels of penetration of digital TV, prior to the planned ending of analogue TV broadcasts.

Digital TV

Software to vote by DTV needs to be designed to ensure that DTV suppliers cannot detect who has voted. Considerations about the openness of all source code, both for the voting software itself, and for operating systems, apply as much to DTV as to voting using devices conventionally recognised as computers: it will thus be necessary to negotiate with the suppliers of DTV hardware to achieve access to their source code, as well as to negotiate access to the DTV broadcasts to enable distribution of voting software.

Digital Television does not offer the range of specialised interfaces that PCs do, and thus may be *more* difficult to make compatible with the needs of groups of disabled people. Terrestrial and satellite digital TV rely on the use of telephone lines for the 'return path'. There may be problems for some voters whose televisions are not close to a telephone point. While this will present a problem for a proportion of voters, it is anticipated that these voters will, in general, not be demographically distinctive.

For DTV to be suitable for electronic voting, any DTV equipment distributed to those without DTV in preparation for the switch-off of analogue transmissions will have to be equipped with the capability for a return path. At present it is unclear whether such equipment will be suitably equipped: the suitability of DTV for use in electronic voting hangs on that decision, since it can be expected that there will be issues of equity of access of a demographically distinct minority who have not previously purchased DTV (perhaps due to lack of funds).

Satellite Digital Television may be susceptible to disruption to the satellite (either failure or attack from a hostile regime). Any digital TV-based electronic voting system would have to be resilient against such disruption.

Given that Digital TV is, globally, not in widespread use (the UK is more than 25% of the world market (e-Envoy 2000)), it has not had the degree of security testing that internet systems have (although that it is still a better bet than the internet for time being because internet systems repeatedly fail those tests). Future developments need to be monitored carefully.

Lottery

Lottery terminals are geographically distributed in a manner which is broadly comparable with the distribution of current polling stations, except with a greater presence in town and city centres.

Lottery terminals offer the advantages of publicly available points at which votes could be input to a secure network.

Security from tampering with lottery terminals is assured, in part at least, by the presence of the lottery vendor.

Supervision by the lottery vendor could provide some deterrent to intimidation of voters.

The cards used to input selections to the lottery terminal would need to be securely retained at or by the terminal to prevent them violating the secrecy of the ballot after the vote has been input.

Accurate marking of the cards used to input selections to the lottery terminal could be problematic for a minority of disabled voters.

A decision was made in the contract process for the current lottery contract to exclude a voting function.

The current lottery security model, with transactions mediated by a vendor, would preclude the introduction of lottery terminals that could support voting even minimally secret from the vendor. This is a fatal flaw with current technology. If at some time in the future there was a change to a security model compatible with secret voting, it would almost certainly be accompanied by unsupervised terminals, which would allow problems of intimidation and tampering with terminals which provide key advantages to the use of lottery terminals on present arrangements.

ATM

Bank Automated Teller Machines provide a distinctive advantage over all other kinds of unsupervised electronic voting, in that they have been designed to offer transaction secrecy from those in the vicinity. Thus they may offer greater potential for secrecy of the ballot.

The security of the banking ATM network also lends itself well to use in electronic voting.

Geographical distribution may be a problem with ATMs, since they are much less frequent in residential areas than polling stations currently are. Perhaps worse for equity of access, they tend to be less common in less affluent areas, and thus a demographically distinct population may have less favourable access to electronic voting, if it were conducted by ATM.

It seems unlikely that ATM operators would be willing to allow open source operating systems to be run on ATMs, for fear of introducing security vulnerabilities, if only by the process of changing operating system.

Focus group research as part of this project makes it clear that there is a significant fear of intimidation at unsupervised ATMs.

Telephone Voting

Telephones offer one massive advantage over other technologies: ubiquity.

Voters will have to listen to a list of candidates. Given that it is not unusual for elections to have more than 5 candidates, this could be a lengthy process, and there will be a temptation to vote for candidates who are announced first, especially if you are allowed to vote before the list is completed. To avoid biasing by the order the candidates were 'read out', I suspect that the order would have to be different for each voter, but this would prevent parties saying "vote for candidate 5", and force all phone voters to listen to the whole list. The big advantage, of course, would be for visually impaired voters.

For most telephone voting, authentication of voter identity will not be easy. Focus group research as part of this project suggests the input of a PIN (of sufficient length to uniquely identify the voter and prevent successful guessing) will prove too difficult for many voters. At present voice telephone voting is only possible with operators to note down the votes – there must be zero secrecy from them, and no guarantee they will not attempt to rig elections unless there are further violations of secrecy of the ballot. There would be no way to make sure that others monitoring a call (such as employers) can't find out how the vote is being cast.

The user interface problems with touch-tone voting are massive. There are problems with defences against violations of secrecy of the ballot and preventing calls being hijacked part way through, threatening the integrity of the ballot.

Focus group research as part of this project suggested public interest in dialling separate numbers according to the party of one's choice, a procedure that is familiar from popular television voting. To prevent multiple voting identification data will be needed, inevitably violating the requirement for anonymity from the regime. Secrecy of the ballot from the immediate telecomms supplier (including the employer, if the call is made from a work 'phone) will not be possible, and any handset with last number redial further risks violating secrecy. The integrity of the election could further be threatened by calls to particular numbers being caused fail (particularly by employers).

It is currently impossible to encrypt votes using WAP or 3rd generation (3G) mobile telephones, meaning that secrecy and inalterability of the vote are both impossible. There is a possibility of smartcard readers in the future for 3G phones, which might enable cryptographic potential. Current levels of penetration are insufficient to suggest whether this technology will ever be sufficiently widespread to be practical, and it appears unlikely that the voting function will be sufficient to ensure it is widespread.

The only form in which telephone voting appears acceptable is if voter identification data and the vote can be encrypted automatically prior to input into the telephone. A smartcard-like device with sound generator could do this.

Authentication

Biometric authentication may seem to allow the most reliable authentication of identity, however, the data associated with the biometric can be stolen, giving the thief access to an identification data that the person associated with that biometric cannot repudiate as a valid identifier. Further, biometric identification may be inappropriate for some voters (for example retinal scanning cannot be used by some voters with visual impairments), meaning that another system will have to be available that does not disadvantage the voter using the other system. Moreover, the collection of biometric identification data will be expensive, probably involving door-to-door collection. It will require the state to hold data on citizens of a sort that currently would be seen as being an unacceptable invasion of privacy.

Considerations of anonymity of the voter from the regime (above) preclude any authentication that uses identifiers that are valid over time, including all of biometric authentication, the use of identity and entitlement cards, and the use of long term "elector cards" as recommended by Coleman et al (2002, p13).

The model for anonymity that we recommend would require identifiers to be generated by the computer that holds the electoral register that will be 'marked' when votes are received. We would anticipate that they would then be sealed into envelopes addressed by the same

computer. The receipt of such an identifier that has been accurately delivered (whether by the Royal Mail or by some other agency) will provide a level of authentication of identity for many voters not far removed from that achieved by current arrangements. The combination with some other data, such as a date of birth, may provide levels of authentication greater than current arrangements.

A significant issue with authentication is ease of use. Focus group research as part of this project suggests the input of a PIN (of sufficient length to uniquely identify the voter and prevent successful guessing) will prove too difficult for many voters. Where appropriate hardware exists on the voting system, ease of use suggests that the randomly allocated identifier should be recorded onto a CD-Rom or Smartcard, so that the introduction of that computer-readable material into the voting system would be the first part of the authentication procedure. The choice of CD-Rom or Smartcard would depend on convenience and the availability of suitable readers.

Whether a manually input PIN or an identifier on CD-Rom or Smartcard, the first stage of the voting process would be to send the (encrypted) identification data to the computer that will eventually receive the encrypted combination of identifier and vote. The identification data will then be sent on to the computer that holds the electoral register and the confidential list correlating numbers issued with names. If the identification data is in order, and no vote has been recorded for that voter, this computer will send a message back to the voting software at the voter's end, to ask the voter to confirm (on pain of legal penalty) that they are the voter whose identification data was sent, before they proceed to the selection of the candidates of their choice. As outlined (above) in the consideration of reliability from failures, the identification data will be sent again (in encrypted form) with the vote before the register will record that the voter has voted.

One particular danger, is that if internet voting was enabled, procedures to thwart automated attempts to guess identification data may well prevent real voting, especially if the attack were mounted from distributed compromised machines.

For voting in supervised polling places, individuals could identify themselves to the system using a CD ROM, a smartcard or a password/PIN combination, ideally partially moderated by the polling official, since polling officials can make use of judgements of the demeanour and appearance of the voter to judge whether to suspect personation, whereas use of automated techniques alone would inhibit that process. It should also be possible for a voter to identify themself using name and address, as at present. To make this operationally possible, computers would need to be (securely) available to polling staff that could securely enquire of the computer that holds the electoral register and the confidential list of identification numbers for that election what the identification number was for that particular voter. To maintain the confidentiality of the list of identifiers, answers should be returned only for those who have not yet voted, and statistical techniques employed to ensure the system was not abused.

Conduits

The law on treating voters currently requires a clear separation of voting from commercial activities. Transferring this into the electronic sphere creates difficulties for a variety of conduits.

Many internet service providers provide a default page of web content. Others "also ship unsolicited advertising along with the requested Web pages" (Mercuri, 2001, p34). It is

clear that any service provider that enables electronic voting (whether internet, digital TV, lottery or ATM) will need to be required to separate the voting function from their normal service. This might be done by a legal requirement that they keep content (news, commentary and advertising) well separated from any electronic voting interface, and perhaps even a requirement that such content is suspended for the polling day(s). The acceptability of this to service providers is unclear.

The Lottery Network and the ATM Network are dealt with through consideration of the lottery and ATMs as voting interfaces. Where voting takes place at supervised polling places overseas, the FCO network should be used if at all possible.

Physical Transfer

While it is anticipated that even at supervised polling places, voting should be conducted with votes transmitted at the time of casting to the counting location, supervised polling places do, uniquely, enable the physical transfer of votes at the end of polling, if communications are lost.

Cable

For voters who receive digital TV by cable there is the possibility of sending votes by the cable network, this appears to be a relatively secure first-choice network that should be used when available.

Telephone

Telephone communications will be available to internet-capable PCs and interactive digital television as well as telephone-based voting.

Unlike the internet, the telephone system has significant defences against overload. Despite these defences, in theory it might be possible for a distributed Denial of Service attack to be mounted that abuses very many compromised user systems to dial and attempt to overload the telephone system. Using different telephone numbers for different local collection and processing centres may help with this. Similarly, keeping such telephone numbers confidential for as long as possible could hamper the mounting of a distributed DoS attack, and aid detection. If telephone numbers are only distributed implicitly by software that automatically dials the relevant number, it may be that by the time attackers have obtained the numbers they cannot mount any effective attack. If a system that uses direct dial in access to local processing centres *is* disrupted in this manner, if it is appropriately designed, it may be possible for it automatically use the internet as an alternative method of communication (provided the local processing centre internet connection does not come through the disrupted part of the telephone network: locations which can enable this separate routing should be chosen).

Systems based on mobile telephony could be susceptible to localised disruption through radio interference.

Mobile telephones automatically release information about their location, which could to some extent be a problem for maintaining privacy for voting by mobile telephone.

Internet based solutions

Where the internet is used as a substantial transmission route, general disruption of the internet (such as when the email 'ILOVEYOU' worm was propagating) could be a

significant threat. At present there is no effective defence against such disruption. Until and unless such defences are introduced, the internet *cannot* be relied upon as a substantial transmission route for electronic voting. The most likely way of ensuring effective defence would be for there to be substantial Government regulation of internet service providers to ensure they monitor for and act against the propagation of viruses/malware of sorts that could cause this disruption. We see no sign that Government is prepared to regulate internet service providers in this way. In theory technical means may be developed to defend against such development in the absence of Government regulation.

If mainstream electronic voting does not use the internet, the 'number of eggs' in the basket of an internet connection for the server might be sufficiently small to enable internet voting where the mainstream electronic voting option is impractical or impossible (overseas, for disabled voters who need specialised interfaces, etc.). It appears that internet voting used on a small scale to enable voting from overseas and other exceptional cases would be incomparably less problematic than large scale internet voting.

If general purpose computers are used for electronic voting away from supervised settings, it is necessary to protect them from viruses and to ensure that they are *verifiably* free from attacks within mainstream software houses. There may be a number of possible ways of achieving this.

1) If by the date of the relevant election a significant majority of home computers use genuinely open source operating systems[8] which have been analysed and are known to be suitable for use in elections, the election software may be able to verify the integrity of the operating system and ensure that computers are virus free.

2) If most general purpose computers still have operating systems that are not suitable for election use, they might still be used in an election if some technique can be devised to ensure the election software communicates directly with input devices (mouse and keyboard, for example) and screen, without interference from the operating system, browser software or viruses, and if virus protection either is widespread on such computers or can be distributed by broadband connections.

3) If most general purpose computers still have operating systems that are not suitable for election use, and no technique as described in 2) has been developed, there is no real alternative to bypassing the installed operating system, and supplying an operating system and sufficient drivers of known quality that are known to be free of viruses and are insulated from any viruses/malware that are already on the general purpose computer. At present such an operating system would have to be supplied on CD-Rom with a floppy disk to boot the computer using the special operating system rather than the normal operating system. While such installation is compatible with internet voting, for virtually all voters, at present the advantages of internet voting over voting by interactive Digital TV will be lost in the process, and the result would be identical to a system that sent votes by telephone without using the internet.

Even if other problems could be solved "One company that audits Web sites for application-level bugs … has never found a Web site they could not hack. That's 100 percent vulnerability." (Schneier, 2000 p175) If websites are used as part of an internet election, the software and server configurations for such websites must be extensively tested

---

[8] That is operating systems where all the elements are open source, rather than commercial versions of, say, Linux, where proprietary closed source software might modify the operation of open source elements.

both by Government security agencies and by at least one internationally recognised security consultancy, and also be available for testing by the political parties, and experts in their employ to ensure that they cannot be hacked.

At present the distribution via the internet of encryption software suitable for voting is not practical for the bulk of home users without broadband access, and for whom the time to download would seem unnecessary and excessive. It is possible that broadband access will become the norm for home users, and thus this problem will disappear, however, if not such software will need to be distributed by post. This need not be a barrier to internet voting, although advantages of internet voting would be lost.

A further concern with networks is that it may be possible to identify the individual who is casting a vote (presumably encrypted, and thus the precise content of the vote is not discernible, although spoilt ballots may be discernible). This is particularly a risk if individuals are voting from work, where it is not uncommon for the name of the computer to be employeename.employername.co.uk.

Network

The internet domain name system is at present not sufficiently secure against attack to enable it to be used in the election process in any substantial way. A system that asks significant numbers of voters to access a particular web domain (for example, www.election.gov.uk), risks having that web traffic hijacked (in the short term, which is long enough to cause unacceptable problems for the election). As security consultant Bruce Schneier puts it: "there's no security in the DNS system. So when a computer sends a query to a DNS server and gets a reply, it assumes that the reply is accurate and that the DNS server is honest. In fact, the DNS server does not have to be honest; it could have been hacked. And the reply that the computer gets from the DNS server might not have even come from the DNS server; it could have been a faked reply from somewhere else." (Schneier, 2000, p180)

The US National Science Foundation similarly warn: "Remote voting systems will … have to contend with an attack known as spoofing—luring unwitting voters to connect to an imposter site instead of the actual election server. While technologies such as secure socket layer (SSL) and digital certificates are capable of distinguishing legitimate servers from malicious ones, it is infeasible to assume that all voters will have these protections functioning properly on their home or work computers, and, in any event, they cannot fully defend against all such attacks. Successful spoofing can result in the undetected loss of a vote should the user send his ballot to a fake voting site. …. In short, this type of attack poses the same risk as a Trojan horse infiltration, and is much easier to carry out." (Internet Policy Institute, 2001 p16).

While DNS problems could only disrupt a given election for a short time, it could well be that individual voters have no idea if they have 'voted' on a spoofed site rather than the real one, so that when the correct IP address is replaced on the DNS, the affected voters do not know that they need to vote again. Spreading the election over several days will not help with this problem, so much as give a longer window during which the DNS system can be disrupted.

The current DNS protocol contains many elements that can, in principle, be used to secure DNS, and these are implemented in current versions. These are in use, but not widely. The real problem with this is the resolver library that the client uses to perform a query. At

present this is a barrier to the current implementation of internet voting, however it need not remain so. If 95% of home computers used to access the internet have web browsers with a library that supports secure DNS and secure DNS is at least as widely implemented by nameservers, DNS attacks need no longer be seen as a barrier to internet voting (although other barriers may remain).

There is currently a vulnerability to attacks on network traffic routers using Simple Network Management Protocol (SNMP) (Lemos, 2002b). If SNMP version 3 (or above) comes to be used by at least 90% of installed routers in the UK, and no serious vulnerabilities are discovered with SNMP version 3, SNMP attacks on routers need no longer be seen as a barrier to internet voting (although other barriers may remain).

Even if much of the network can be made in principle secure, it seems that client end problems will still be a potential problem for SOME voters for many years.

Conclusions on Internet based solutions

In the eyes of some experienced commentators "interfacing to the Internet could be, in itself, considered to constitute a security breach, in that wide attack and monitoring opportunities are provided that would not be possible with individual DRE [voting machine] kiosks, or in a closed network setting" (Mercuri, 2001, p34)

Despite this, it is logically possible for internet voting to be made suitably secure for use as the mainstream means of voting in a UK general election. However, the cost of achieving such security (including the time costs to voters), suggests that other options are much more likely to be fruitful as the mainstream method of electronic voting for the next few general elections. It may be worthwhile continuing to investigate internet voting for the longer term future.

Collecting and Processing Centres

In order to be resilient in the face of attempted denial of service attacks (DoS), the electronic voting system needs to avoid being vulnerable to single points of failure. Similarly, reducing the 'number of eggs in one basket' would reduce the attractiveness of any single target: thus the collection and processing of votes should take place at very many centres for a general election. Each of these centres will need to be defended against DoS attacks.

However, given that the number of trustworthy people with sufficient technical capabilities is limited, the need for security from internal attacks may place limits on the numbers of counting centres.

Whether connected to the internet or not, to protect against attempts to hack into servers (as well as denial of service attacks) each counting centre needs a good, well configured and well maintained firewall with effective detection and reaction capabilities in addition to the protection capabilities that are normally associated with firewalls[9]. If servers that collect votes and pass them on for processing have *any* connection to the internet (as seems most likely), firewalls will also have to ensure that DoS attacks on the internet connection do not tie up system resources and cause a denial of service for other connections.

---

[9] Unlike many applications of firewalls, the configuration should err on the side of false alarms, since the election period will be short, and the costs of a security breach cannot easily be offset by financial measures.

The number of counting centres may be limited by the availability of staff capable of competently operating such security systems and servers, however, in no circumstances should more than 10 parliamentary constituencies be dealt with at a single counting centre (and if as many as 10 are dealt with in one centre, the constituencies should be politically mixed, since the chance of the overall result of the election being affected could affect the likelihood of an attack).

A further consideration that strongly suggests that the number of counting centres should be large is the risk of physical disruption. At present to cause significant disruption to a general election would require physical disruption to many counting centres, thus the election is fairly well defended against attacks using physical disruption. The smaller the number of counting centres, the greater the defences of each would need to be.

Shortlist

Thus our shortlist for further study as part of our project was

1) Polling Location-Polling Official-PC
2) Home - CDRom and Floppy-PC
3) Home - Smartcard -DTV
4) Public Space -Smartcard -ATM
5) Anywhere - Smartcard with sound generator-Voice Phone

All would connect to local authority collecting and processing facilities to provide security against hacking.

1-3 would use telephone to communicate but with the potential to use the internet if that route is blocked.

3 can, for households where DTV is Digital Cable, use cable as first choice communications network, using internet as a back-up route.

4 uses the ATM network.

5 uses the phone network with no backup. The smartcard with sound generator would have to be issued to each voter and with the current state of play would be significantly expensive.

Capability Analysis

Cluster	Issue	1 Polling Place	2 Home PC	3 Home DTV	4 ATM	5 Phone with sound generator
Individual	Safety	Adequate	Adequate	Adequate	Worst	Adequate
	Privacy	Best	Better on protecting minorities from identification. Worse on workplace monitoring (esp SME), and at protecting from pressure within the home	Worse at protecting from pressure within the home	Adequate	Adequate
	Cost	Travel cost only	Worst	Best excluding TV licence cost	Travel cost only	Best if smartcard provided free.
	Anonymity	Adequate	Adequate	Adequate	Adequate	Adequate
System	Usability	Best, because multiple interfaces available, complexity handled by official	Worst for mainstream voters (complex), but could enable multiple interfaces	Good: some various interfaces available, complexity handled by software	Fair: good for mainstream voters, but little choice of interface.	Worst for mainstream voters (no visible interface)
	Access	Distance, Stops personation by family	May not have PC with phone access in the home	1 Best but may not have TV/ nearby telephone socket	Distance (not as good as supervised polling location)	2 More than adequate
	Performance	Best: can specify good enough	Worst: has to run on ageing machines	Adequate	Adequate	Poor: Risk that technology may be too innovative
Outcome	Misuse	Better defence against personation	Adequate	Adequate	Adequate	Adequate
	Audit	Best	Adequate	Adequate	Good	Adequate
Data	Integrity	Back up procedure for system failures	Adequate	Adequate	Adequate	Adequate
	Security	Best	Adequate	Adequate	Best	Adequate
Context	Environment	1 Best	3 Fair	4 Adequate	2 Good	5 Worst
	Attitude	Issues may differ if use 'off the shelf' solutions, also need to ensure adequate	Ensure adequate	Ensure adequate	Ensure adequate	Ensure adequate
Notes		Improves on current polling station in that can vote from any polling station, multiple interfaces available. May be possible to have more polling stations than at present, including abroad.	DTV preferred for cost, usability, access, performance.	Preferred solution for voting at home.	Safety concern may be sufficient to exclude.	Usability of the interface and innovative technology suggest other solutions should be preferred.

Conclusions

Account should be taken of the key actions outlined above.

Voting from unsupervised locations should not be introduced without a public debate informed by the gathering and dissemination of expert opinion about acceptable levels of privacy and secrecy.

It is quite plausible that whatever is done to protect the election from attacks on software distributed to voters or to prevent such attacks, the first election at which such programs are widely distributed will suffer some disruption: the best that can be hoped for is that relatively few people will be voting electronically, and thus that the problems caused will be minor.

Servers

Defending against attempts to cause biased software to be used requires the source code of programs used to be openly available. There should be a legal requirement that authoritative results cannot arise without open source code. There is an element of tension here with the desire to prevent hacking and viruses, in that openly available source code would be more vulnerable to such attacks than equally well tested bespoke source code that remained confidential. However, attempts to widely distribute programs while keeping them sufficiently confidential to prevent hacking repeatedly fail as 'tamper-proof' devices are tampered with and programs are reverse engineered by hackers.

Thorough testing of software by paid experts is essential, although open source software should additionally allow leveraging the expertise of the wider security community.

Openly available source code for programs run on servers would, despite advantages in other respects, be more vulnerable to hacking attacks than equally well tested bespoke source code that remained confidential (unlike voter-end software, there is a reasonable chance that server software could remain confidential). For each counting centre, there should, thus, be at least two sets of servers, one running open source code and the other running separately developed programs with confidential code. If the results differ, an investigation should be made into the origin of the difference. If there was evidence of hacking of the system with open source code, before the system with confidential code could be accepted as giving a result that overrode the result from the open source system, the source code of the previously confidential system should be opened to inspection[10].

To minimise the risk of physical attacks on counting centres, parallel systems should be in separate locations for each (logical) counting centre.

There will be a need for those charged with the operation of servers to have a thorough concern for security: if they are operated by local authorities, there may be a need for a programme of security education for relevant local authority staff.

---

[10] With a sufficient minimum time for inspection being specified by law, so that a result could not be declared until there had been sufficient opportunity to ensure that the previously confidential code was fair and accurate.

43

Supply

There is also a need for substantial procedures to ensure that the programs actually run on servers and distributed to voters or polling places are unmodified instantiations of these open source programs, where "The compiler used to generate the object code must be available, and all hardware specifications must be revealed, down to the chip level" (Mercuri, 2001, p48).

There will be a need to ensure that there is adequate security within those suppliers who are charged with enabling the delivery of software and identifiers to voters (whether transmitting software to the voting point or producing physical carriers of the identifiers, and if applicable, software for delivery), and servers. There is also a need for testing to verify that no undetected changes of the software have been made: a sample of voter-side software and all server software should be tested in this way.

System design methodologies must embrace social impact: 'off the shelf' commercial design methodologies as implemented by major contractors can be expected to be inappropriate.

Technologies

The two technological solutions that give the greatest promise in the timescales under consideration are

A) Voting using PCs supervised by polling officials, probably in a wider range of polling places than current polling stations, and where voters can vote from any such polling place in the UK (or overseas, where they are set up). Such polling places would use telephones[11] to communicate but with the potential to use the internet if that route is blocked.

B) If the public debate about privacy and secrecy in voting from unsupervised locations concludes that such a technological solution is acceptable, voting from home using digital television, with primary identification being by inserting a smartcard produced for that particular election. For households where DTV is digital cable, the cable network should be used as the first choice communications network, using the internet as a back-up route. For other DTV systems the telephone system would be the means to conduct the voting transaction, but with the potential to use the internet if that route is blocked at a point distant from the house.

In the longer term the internet may show potential, but a number of key hurdles outlined in the report need to be overcome.

Whatever technology is used to send electronic votes, they would connect to local collecting and processing facilities to provide security for the overall election.

Generally, the only way to be sure that a system is secure is that many people have tried a wide range of attacks against it, and it has withstood them. Electronic voting should thus be introduced gradually.

---

[11] Land line where available, or mobile telephones, with handsets for alternative mobile telephone networks available as a back-up for the local connection.

As a further safeguard, we would recommend that electronic voting initially only be introduced in constituencies where the consent of all the parties that have stood in either the last two general elections has been obtained.

References:

Bolton MBC, 2000 "Evaluation of Pilot Election Schemes" online at http://www.elections.dtlr.gov.uk/pilot/pdf/evalbolt.pdf, accessed 26.02.2002.

Burnham, David, 1985 "Vote by Computer: Some See Problems" in *New York Times* 21.08.1985, as quoted in Mercuri, 2001, p92.

Butler, David and Kavanagh, Dennis, 1992 *The British General Election of 1992* (Basingstoke: Macmillan)

California Internet Voting Task Force, 2000 *A Report on the Feasibility of Internet Voting* (Sacramento, CA: Secretary of State, State of California) online at http://www.ss.ca.gov/executive/ivote/final_report.htm, accessed 31.01.2002

Coleman, Stephen et al 2002 *Elections in the 21st Century: from paper ballot to e-voting* Report of the Independent Commission on Alternative Voting Methods (London: Electoral Reform Society)

F-Secure, 2001 "F-Secure Virus Descriptions: BadTrans.B" at http://www.europe.f-secure.com/v-descs/badtrs_b.shtml accessed 24.01.2002

Graham, Paul, 2002 "Online defences" pp8-9 in *Local Government Chronicle Special Supplement on Electronic Government* January 2002

Internet Policy Institute, 2001 *Report of the National Workshop on Internet Voting: Issues and Research Agenda* online at http://www.netvoting.org/Resources/InternetVotingReport.pdf, accessed 31.1.2002

Judge, Peter, 2002 ".Net vote rigging illustrates importance of Web services" online at http://news.zdnet.co.uk/story/0,,t269-s2102244,00.html, accessed 01.02.2002

Lemos, Robert, 2002a "Data on Internet threats still out cold" online at http://news.com.com/2100-1001-819521.html, accessed 28.01.2002.

Lemos, Robert, 2002b "Flaws in common software threaten Net" online at http://news.com.com/2100-1001-835602.html accessed 13.02.2002.

Mercuri, Rebecca, 2001 *Electronic Vote Tabulation: Checks and Balances* PhD thesis, University of Pennsylvania.

Mohen, Joe, 2000 (CEO, election.com) as quoted in *Wall Street Journal* "Election.com Aims to Revolutionize The Voting Process With Online Ballots" 08.05.2000

Nu.nl, 2001 "Internetstemmen voor gemeentenaam stopt na fraude" online at http://nu.nl/document?n=44479&___cookie2__=S1012231513707873 accessed 28.01.2002

O'Neill, Tip, with Novak, William 1987 *Man of the House* (Random House) as Quoted in Mercuri, 2001, p91.

Schneider, Fred,B (ed) 1999, *Trust in Cyberspace* (Washington, DC: National Academy of Sciences) online at http://bob.nap.edu/html/trust/trust-4.htm, accessed 31.1.2001

Schneier, Bruce, 2000 *Secrets and Lies* (Wiley)

Appendix - Electronic Voting Options Taxonomy: full listing

LOCATION	AUTHENTICATION	INTERFACE	CONDUIT
work	cd rom and floppy disk	pc	internet
work	cd rom and floppy disk	pc	telephone
work	password/pin	pc	internet
work	password/pin	pc	telephone
work	password/pin	wap/3G	internet
work	password/pin	voice phone	telephone
work	smartcard with sound generator	voice phone	telephone
polling station / supervised polling place	cd rom	pc	internet
polling station / supervised polling place	cd rom	pc	physical transfer
polling station / supervised polling place	cd rom	pc	telephone
polling station / supervised polling place	cd rom	pc	FCO network (from overseas)
polling station / supervised polling place	polling official	pc	internet
polling station / supervised polling place	polling official	pc	physical transfer
polling station / supervised polling place	polling official	pc	telephone
polling station / supervised polling place	polling official	pc	FCO network (from overseas)
polling station / supervised polling place	polling official	electronic voting machine	physical transfer
polling station / supervised polling place	polling official	electronic voting machine	FCO network (from overseas)
polling station / supervised polling place	biometrics	pc	internet
polling station / supervised polling place	biometrics	pc	physical transfer
polling station / supervised polling place	biometrics	pc	telephone
polling station / supervised polling place	biometrics	pc	FCO network (from overseas)
polling station / supervised polling place	biometrics	electronic voting machine	physical transfer
polling station / supervised polling place	biometrics	electronic voting machine	FCO network (from overseas)
polling station / supervised polling place	password/pin	pc	internet
polling station / supervised polling place	password/pin	pc	physical transfer
polling station / supervised polling place	password/pin	pc	telephone
polling station / supervised polling place	password/pin	pc	FCO network (from overseas)
polling station / supervised polling place	smartcard	pc	internet
polling station / supervised polling place	smartcard	pc	physical transfer

polling station / supervised polling place	smartcard	pc	telephone
polling station / supervised polling place	smartcard	pc	FCO network (from overseas)
home	cd rom and floppy disk	pc	internet
home	cd rom and floppy disk	pc	telephone
home	password/pin	pc	internet
home	password/pin	pc	telephone
home	password/pin	wap/3G	internet
home	password/pin	voice phone	telephone
home	smartcard with sound generator	voice phone	telephone
home	password/pin	digital TV	internet
home	password/pin	digital TV	telephone
home	password/pin	digital TV	cable
home	smartcard	digital TV	internet
home	smartcard	digital TV	telephone
home	smartcard	digital TV	cable
public space	biometrics	ATM	ATM network
public space	password/pin	voice phone	telephone
public space	smartcard with sound generator	voice phone	telephone
public space	password/pin	ATM	ATM network
public space	smartcard	ATM	ATM network
public space	password/pin	lottery ticket	lottery network

All could be connected to national, regional, or local, collection and processing facilities
(except that physical transfer would have to be to local facilities)
This leads to 136 combinations (approx), some of which may be used by some voters in the same election as other voters use other combinations.