The Institution of
Engineering and Technology

Internet voting in the UK

The issues, challenges and risks around internet voting

theiet.org/internet-voting

Internet voting in the UK is published by the Institution of Engineering and Technology.

Please note that the views expressed in this publication are not necessarily those of the IET. It is not intended to be a guidance note with a specified set of recommendations or actions but rather seeks to add understanding and debate around the topic.

The Institution of
Engineering and Technology

The Institution of Engineering and Technology (IET) is working to engineer a better world. We inspire, inform and influence the global engineering community, supporting technology innovation to meet the needs of society. The Institution of Engineering and Technology is registered as a Charity in England and Wales (no. 211014) and Scotland (no. SC038698).

Contents

About this report

This thought leadership paper discusses the technical and societal issues that will need to be addressed if the UK wishes to move towards an online electoral system in the future.

Written for policy makers and for those concerned with electronic voting (e-voting), it seeks to provide well-informed and authoritative technical advice on the issues, challenges and risks around such systems, with respect to their requirements, design, deployment and operation.

As well as using existing research on the topic, this report brings together key points raised at two roundtable meetings held in June 2019. One was held at IET London: Savoy Place, the other at the National Cyber Security Centre conference for Academic Centres of Excellence in Cyber Security Research in Stratford-upon-Avon. These workshops were attended by individuals with relevant knowledge and expertise in the field, from academics to industry and government representatives, providing an opportunity to share blue-sky thinking and explore how we can help to lead developments in this area.

The roundtables were the first activities delivered by the IET's cross-sector E-voting Working Group, chaired by Professor Steve Schneider, Director of the Surrey Centre for Cyber Security. This group was set up to explore various issues around e-voting, with an initial focus on internet voting.

This report also incorporates input from Dr Ian Levy, Technical Director of the National Cyber Security Centre, Craig Westwood and Mark Williams of the Electoral Commission, and from a questionnaire circulated to IET members.

The bulk of the work for this report took place before the COVID-19 pandemic, which has changed the way society is now operating and will need to in the future. Remote working is now the norm for many, and activities are being moved online as society rethinks how it can and should operate.

In March 2020 the UK government announced that the May 2020 local elections would be postponed to May 2021 due to the pandemic. This naturally drives discussion about alternative approaches to conducting elections, such as greater use of postal ballots, as well as the possibility of online voting. This report considers that technology is not currently in a position to provide internet voting in a safe and secure way, and that further technological advances are first required. The challenges are substantial, but the pandemic has placed new urgency on addressing these technical challenges.

This document was produced by the IET's E-voting Working Group: Steve Schneider (Chairman), Nick Coleman, Richard Crowther, Eric Dubuis, Aggelos Kiayias, Dave Palmer, Jordi Puiggali, Awais Rashid, Mark Ryan, Barbara Simons and Thomas Zacharias.

Consensus of opinion has not always been possible from the expert members of the IET working group that compiled this report. As such, it's fair to say that not all the conclusions and recommendations of this report have been agreed by all working group members. This reflects the leading edge thinking and unresolved issues around this topic. We hope that our findings add to the debate and lead to further discussion, research, analysis and publications.

The IET Digital Sector welcomes any comments or suggestions. Please send these to **sep@theiet.org**.

1. Executive summary

Internet voting for statutory political elections is a uniquely challenging problem. This is because of the high cybersecurity risks for any such system, given the need to conclusively deliver the right result while protecting the secret ballot.

This report considers what would be required of an internet voting system. It reviews the motivations for internet voting, discusses the risks associated with it, and the socio-technical issues associated with the introduction of any such system to justify and maintain public trust.

Finally, it considers the demanding technical requirements that would be necessary to underpin trustworthy internet voting. Although there have been advances in this area, it concludes that cybersecurity is a critical challenge, and technology is not now – or in the near future – ready to address the range of cybersecurity threats that could undermine an internet voting system.

1.1 Recommendations

1. Cybersecurity is a critical challenge for internet voting. Technology is not currently in a position to address the range of cybersecurity threats that could undermine an internet voting system. Internet voting requires further technological advances in the areas of platform security, digital identity management, usability and designing systems that provide voters and observers with the ability to verify the result of the election.

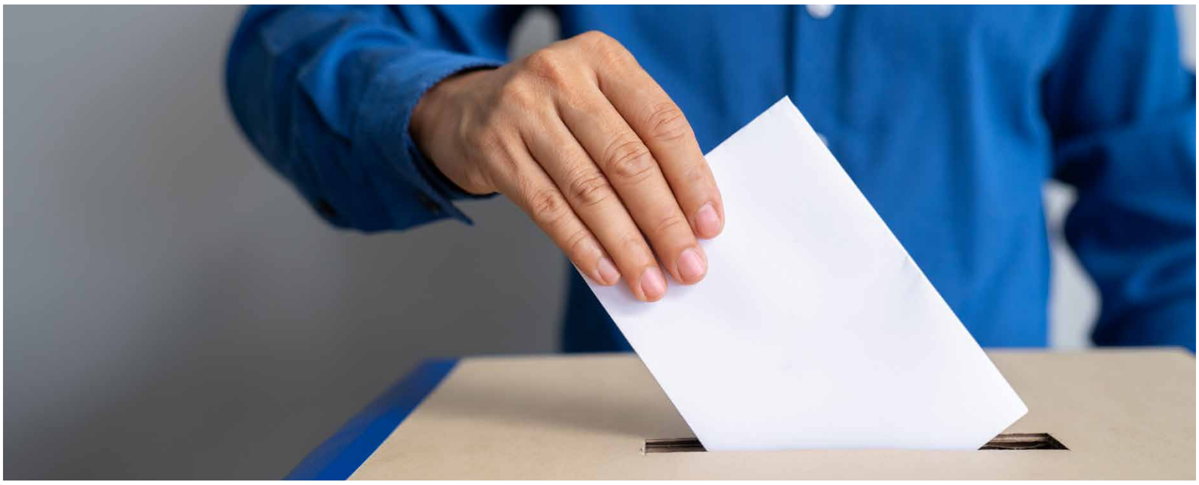
2. Given the critical nature of elections and the requirement for public trust, transparency of the system design will be essential. Open reviews and trials will be necessary. The system design will need to integrate mitigation strategies that protect elections in the case of cyberattack. Complete risk elimination is impossible to achieve, therefore it's crucial for any system to verifiably achieve sufficient accuracy to ensure the correct result for the election and to detect and recover from cyberattacks.

3. Internet voting should be considered as an additional voting channel rather than a replacement of traditional voting channels. One of the objectives of any electoral process is to be as inclusive as possible. It's important that solving an accessibility issue doesn't generate a digital divide.

4. Current technology is suitable for elections in low-coercion environments. These include elections within companies and other organisations, and for elections where the secrecy of the ballot is not required – for example shareholder ballots or votes within parliament.

2. Outlining the opportunities of online voting

The current UK voting process favours those who can travel to a specific location, at a very short and fixed window in time, and have a fixed address for voter registration – descriptions that don't reflect the full breadth of UK citizens' lives. There may be opportunities for more flexible methods of voting to empower parts of our society that are currently underserved, or reliant on others to assist them in voting. Postal voting provides some flexibility, but online voting is also encouraged by advocates as a potential solution.



2.1 Increasing accessibility

Voting accessibility is an area that has seen significant improvement over time, but more progress still needs to be made. Research carried out by the Electoral Commission in the wake of the 2017 General Election found that there are still polling stations that are inaccessible to people with physical or mental disabilities. Of those surveyed, 5% reported difficulty getting into the station when going to vote[1], and more said that voting through the traditional method has made them feel uncomfortable.

In response, the Royal National Institute of Blind People (RNIB)[2] has called for an online and/or telephone option for blind and partially sighted people to cast their vote independently and in secret if they aren't able to vote at their polling station.

The UK Government[3] has identified that technology can improve accessibility for disabled voters. It reported that the use of IT should be able to provide a better service and support, but also that there's a wider issue about the security and integrity of e-voting that precludes it being considered as a solution.

Online voting could provide one way to overcome accessibility problems by allowing people to vote from any location and enabled by technology that's more suited to their needs – provided it can be done securely. However, we note that alternative approaches to accessibility are also possible without the need to return the vote electronically, such as allowing voters with disabilities to download a blank ballot onto their systems, mark the ballot using their accessible technology, print it out, and return it by post[4].

[1] https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Accessibility-report-call-for-evidence.pdf
[2] https://www.rnib.org.uk/campaigning-policy-and-reports-hub-access-information/access-information-reports
[3] https://www.gov.uk/government/consultations/access-to-elections-call-for-evidence
[4] https://www.fivecedarsgroup.com

2.2 Increased convenience

UK citizens with busy lives may be better served by online voting if it can be done securely. Having the freedom to vote remotely brings added convenience for many, but would be particularly helpful to those outside of their local region on polling day, who have changeable working or care-providing patterns, have no predictable home address, or are simply disrupted on polling day.

It's been argued that the ability to vote from 'anywhere' could potentially increase participation, or at least halt the decline, and could lead to greater involvement from younger generations. However, studies[5] on voter behaviour have found that the existing availability of internet voting hasn't in practice increased overall turnout or engagement among younger voters.

Younger generations have been using electronic means in many aspects of their social life, with 99% of adults under 44 using the internet daily or almost daily[6]. When the time comes for them to vote, their participation could be influenced by the way they're asked to engage in the election process. Online voting could come as a natural interface for new generations, enabling them to smoothly embrace democratic procedures. Of course, younger voters may eschew online voting because they understand, possibly better than their elders, how insecure the internet is.

99%

of adults under 44
use the internet daily
or almost daily

There are also general considerations around cost, as well as speed and accuracy of the tallying and obtaining the result of UK elections. However, it's expected that costs would increase, especially in the short-term, if online voting supplements rather than replaces the current paper-based system. It appears that reduction of costs is not a primary driver for online voting.

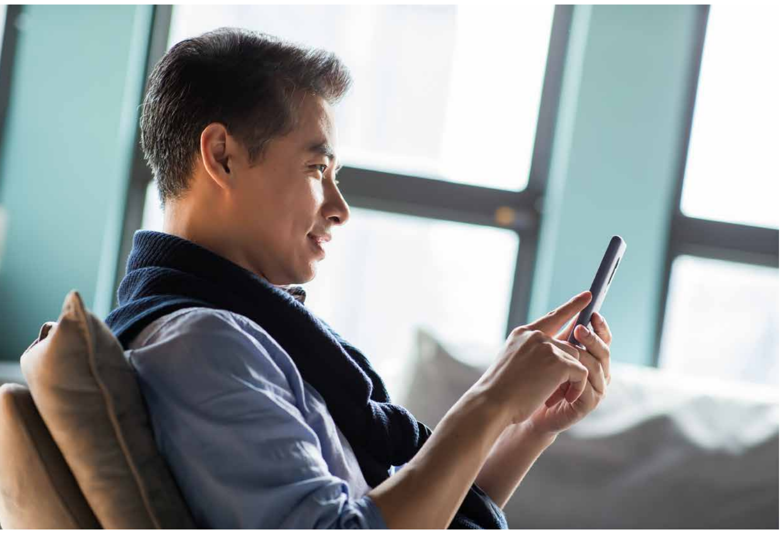
Similarly, while speed of delivering the result and potential improvements in exactness of the tally might be welcome, current hand-counting processes are considered appropriate for delivering sufficiently accurate results, so there are no issues around speed and accuracy to address.

[5] https://elections.bc.ca/docs/recommendations-report.pdf
[6] https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2019

2.3 Achieving effective e-voting

E-voting systems that support **end-to-end verifiability** allow voters to verify the correct counting of their votes, without having to put trust in any voting device or election server. Such transparency isn't available in the current UK voting system and it may boost citizens' trust in the election process.

There are such systems available for low-coercion online elections[7,8,9], appropriate for private elections within organisations such as companies, building societies, professional societies, student unions and trade unions. No such system for online voting currently exists suitable for high-stakes ballots such as national elections. Systems for polling place voting such as Scantegrity[10] and vVote[11] have demonstrated end-to-end verifiability in statutory elections, but they have not entered the mainstream. Microsoft's open source ElectionGuard[12] project enables end-to-end verifiability to be integrated into voting systems. None of these are designed for internet voting. However, it's possible that in the future there may be a workable end-to-end verifiable voting system for voting over the internet[13].



Looking forward, online voting could potentially lead to more sophisticated and nuanced engagement with the UK electorate. If online voting became the norm, then higher volumes of elections and referenda wouldn't have as high an incremental cost over and above the sunk cost of maintaining the online infrastructure. This could provide the opportunity to increase the frequency that the electorate is consulted on issues, as happens in Switzerland. There's also been discussion about the potential opportunity to offer a wider number of carefully described and more specific options on referenda.

Online voting could also be a key enabler for more significant changes to the UK's current representative democracy. For example, enabling direct democracy where all participants must vote on key issues, or liquid democracy (also known as delegative democracy[14]) approaches. This is where citizens can choose to delegate their vote to individuals, potentially on a per issue basis, resulting in a half-way house between the current representative approach and having influence on individual policies.

Moving voting online may open opportunities to new forms of democracy. Facilitating referenda can give power to special interests who can influence voters, and **the impacts of such opportunities need to be carefully evaluated and understood before deciding whether to introduce them**.

[7] https://heliosvoting.org
[8] https://zeus.grnet.gr/zeus
[9] https://www.belenios.org
[10] Scantegrity II Municipal Election at Takoma Park: The first E2E Binding Governmental Election with Ballot Privacy. Richard Carback et al., Proceedings USENIX Security, (2010)
[11] vVote: a verifiable voting system. Chris Culnane et al., ACM Transactions on Information and System Security 18 (1) (2015)
[12] https://github.com/microsoft/electionguard
[13] https://www.usvotefoundation.org/E2E-VIV
[14] https://wiki.p2pfoundation.net/Liquid_Democracy

3. Case study: United Kingdom

In 2002, the Electoral Commission proposed piloting new voting methods and technologies under the 2000 Representation of the People Act (RPA). This was to look for possible ways to mitigate the turnout drop detected during the elections carried out in June 2001.

The objective was not only to increase or keep the participation turnout, but also to improve the efficiency and accuracy of the election administration[15]. During the pilot programme, different voting systems and technologies were tested in a number of authorities, with the aim of evaluating their impact in the electoral processes. Pilots comprised of different voting systems including all-postal voting, internet voting, telephone voting, SMS voting, digital TV voting and kiosk voting. Internet voting was piloted in three different municipal elections: 2002, 2003 and 2007.

To achieve the evaluation and reporting requirements of the pilots, the Electoral Commission participated actively in the evaluation of the pilots and issued reports after analysis, providing conclusions and recommendations for future ones. External lead evaluators, technology and socio-political experts assessed each individual pilot, and evaluation was based on six issues[16]. These were efficiency, impact on voting, impact on the counting of the votes, security and confidence, turnout and cost. Based on the individual reports, the Electoral Commission issued a global report compiling the information of the different pilot schemes and providing recommendations for next pilots. All the reports are available through the Electoral Commission website[17].

The evaluation report[18,19] following the final 2007 pilot scheme considered that the pilots provided useful information on the various technologies from an operational point of view, but that sufficient time hadn't been allowed for effective planning, testing and quality management. It also noted that the value of the pilots had been significantly reduced by the absence of an overall electoral modernisation strategy. It recognised that "*there are clearly wider issues associated with the underlying security and transparency of these e-voting solutions*".

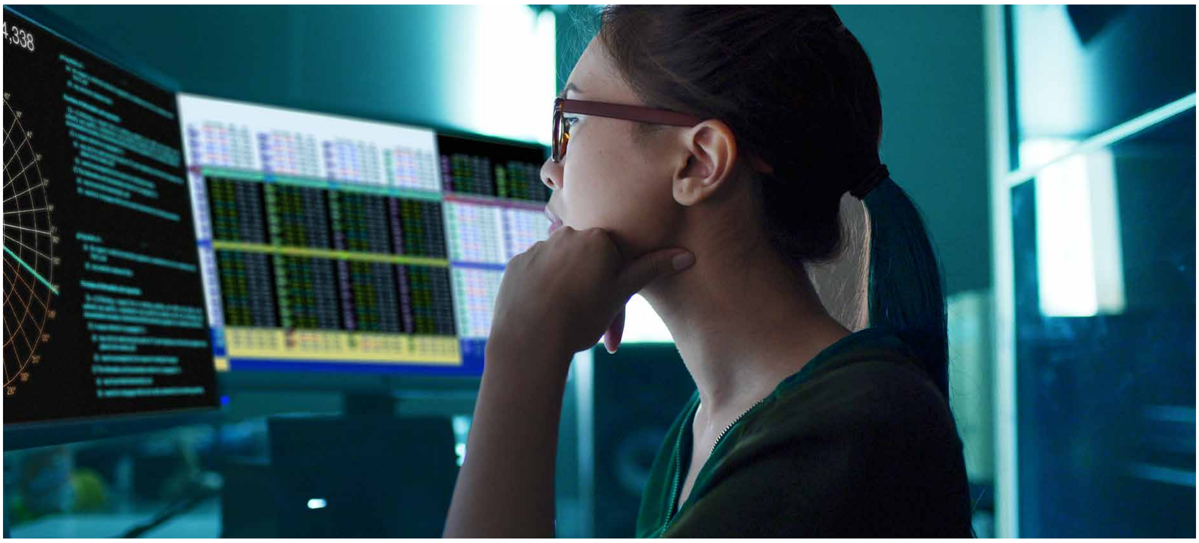
The report recommended that no further e-voting pilots should be undertaken until there's a "*comprehensive electoral modernisation framework covering the role of e-voting, including a clear vision, strategy and effective planning [which] must outline how the important issues of transparency and public trust will be addressed...*", and an accreditation and certification process and a more robust procurement framework is set up for evaluating and selecting the technologies to use in the pilots. Since then, no further e-voting pilots have been conducted in the UK.

In addition to pilot reports, other studies were made available relating to the study of the pilot schemes. One report, issued by the Communications-Electronic Security Group (CESG), related to an e-voting security study[20]. This was published after the 2002 voting pilots, with the objective of making an assessment framework about the security risks, potential mitigations and plausible approaches to consider when implementing and evaluating the security of e-voting pilots.

The study made 15 recommendations, including several which are reflected in our report: the requirement to provide confidentiality and integrity of the vote without the need to rely on the delivery mechanism to provide these, availability of the e-voting system, the challenge of coercion and vote selling/vote fraud, and the need to consult the public, academic community and commercial suppliers. The background review concluded: "*there are a number of barriers to successful introduction of a national online voting system. The principal areas requiring consideration are insecurities of the client platform, system design issues, and user education*".

[15] The Electoral Commission. "Modernising elections. A strategic evaluation of the 2002 electoral pilot schemes", 2002.
[16] The Electoral Commission. "Statutory evaluation of electoral pilot schemes May 2007. Evaluation Framework for Lead Evaluators", 2007.
[17] https://www.electoralcommission.org.uk
[18] The Electoral Commission. "Electronic voting May 2007 electoral pilot schemes", August 2007. https://www.electoralcommission.org.uk/sites/default/files/electoral_commission_pdf_file/Electronicvotingsummarypaper_27194-20114__E__N__S__W__.pdf
[19] The Electoral Commission. "Key issues and conclusions. May 2007 electoral pilot schemes", August 2007.
[20] CESG. "e-Voting Security Study. Issue 1.2", July 2002.

4. Threats, attacks, risk and targets



In a time when cyber threats are rapidly increasing in terms of both frequency and severity, it's obvious that highly robust cybersecurity processes must be in place for any internet voting system to be considered feasible.

No voting system can be entirely risk free. As a result, together with the opportunities that come with internet voting systems, you have to carefully assess and mitigate the risks that could be introduced by its deployment and consider whether they outweigh the benefits. The high stakes of statutory elections mean that the risks are substantial.

According to the World Economic Forum, cyberattacks now represent one of the most serious threats to humanity[21], ranking in the top ten risks for both likelihood and impact. In the UK alone there were almost 150,000 attempted cyberattacks in the second quarter of 2019, which equates to one attack every 50 seconds[22]. Now three years old, the National Cyber Security Centre (NCSC) has reported defending the UK from more than ten attacks per week, with the majority of these coming from hostile nation states[23]. Major cyber operations including distributed denial of service, espionage and penetration have been publicly attributed to a number of countries[24]. Individuals such as criminals and malicious hackers make up the bulk of the remaining threat, though insiders with privileged access are also potential threats.

All of these are plausible threat actors in the context of political elections, as they're well-resourced and have the capability for sophisticated cyberattacks. Interference in elections by nation states has already been identified as an ongoing activity[25], and technology provides a target for adversaries seeking to affect the outcome of an election. It follows that any use of internet voting should be accompanied by a comprehensive risk analysis and mitigation plan.

When assessing the risks associated with any system, there are three dominant dimensions to be considered. These relate to the integrity of the system, the confidentiality of the information it processes and the availability of the system. Furthermore, and specifically in the context of elections, you have to also consider the risk of manipulation of the inputs provided by voters.

Here we expand on the exact nature of these risks, overview the possible attack targets and conclude with risk mitigation recommendations.

[21] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
[22] https://www.beaming.co.uk/cyber-reports/uk-cyber-threat-report-q1-2019
[23] https://www.ncsc.gov.uk/annual-review/2018/ncsc/docs/ncsc_2018-annual-review.pdf
[24] https://www.solarium.gov
[25] https://ec.europa.eu/epsc/sites/epsc/files/epsc_-_election_interference_thinkpieces.pdf

4.1 Integrity risks

In the context of internet voting, an integrity break refers to the risk of misreporting or otherwise subverting the process under which the election outcome is calculated.

The following thought experiment is helpful when thinking about integrity. Consider a specific election and freeze it at a particular instant when all the election options are given, the electoral roll is fixed and all voters have made up their mind in some way about how to vote or abstain, but have not yet submitted their vote. In that hypothetical moment, the outcome of the election is determined. The relevant question is whether the voting system can faithfully discover and report it. Ensuring that there's no divergence between the well-defined, but otherwise inaccessible, outcome of the thought experiment and its open report by the voting system, even in the presence of powerful adversaries, is essential to integrity risk mitigation.

There are also risks that come from the manipulation of the election tallying process, or the exact specification of the actual election choices. These can gravely affect the outcome and in the past have been effectively used to manipulate or gerrymander elections' integrity. The presentation of the election choices in the user interface (UI) is a serious concern, and it's been observed in a variety of cases, independently of internet voting, that election manipulation can take place by controlling the way the UI presents the elections' choices to the voters.

Another important component that should be considered is the electoral roll. Determining who's eligible to vote can have a paramount influence on the election outcome. Breaking the integrity of the voter roll can result in the introduction of non-existent participants whose credentials may even be controlled by the attacker, resulting in a 'ballot-stuffing' attack and a biased election outcome. Likewise, selectively removing voters that are eligible results in another integrity failure.

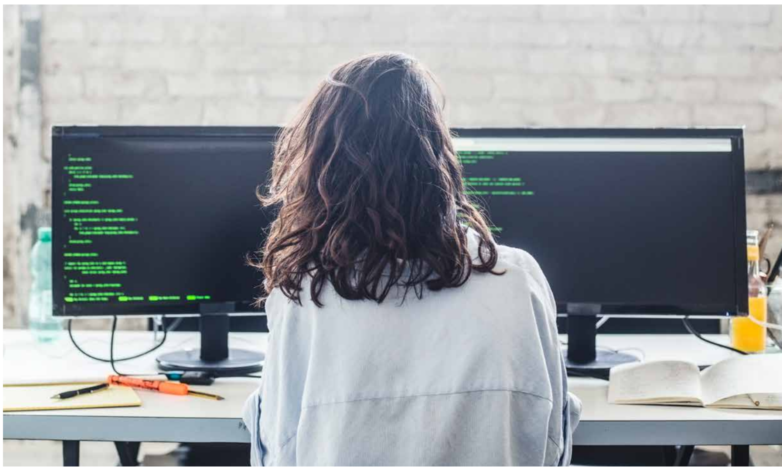
4.2 Confidentiality risks

Many election processes require the confidentiality of the voters' input. The input of the voter must be suitably protected whilst the ballot is cast and tallied, and at the same time the tallying of the election result should not reveal too much information about an individual voter and their choice.

Confidentiality is also essential in preserving the independence of the voters' inputs. To see the potential risk here, remember that when confidentiality is breached, it's possible that votes cast later in the process can be influenced by the choices submitted early on.

In an internet voting setting, a breach of confidentiality may also occur by correlating information from the network layer. For instance, correlating a user's IP address or location to their choice in the election may be possible by examining the protocol's network traffic captured in transit. It's worth noting that confidentiality is a property that needs to be protected indefinitely, given that election choices, revealing voters' political beliefs for example, may exacerbate problems of social exclusion and/or discrimination in the future.

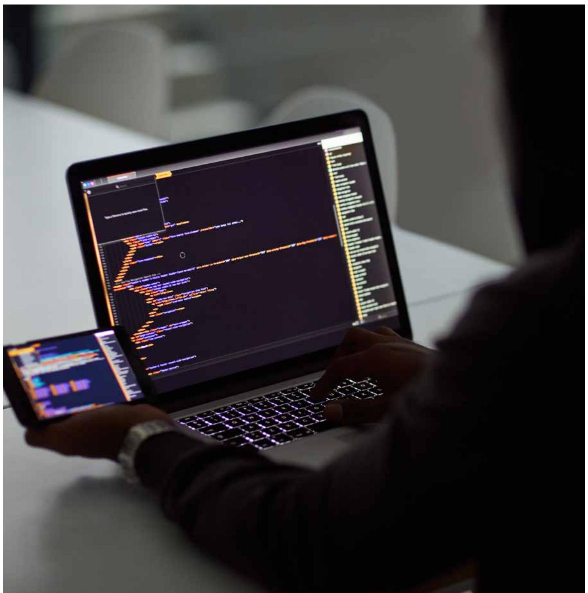
The risk of losing confidentiality also introduces the risk of having the voters coerced to follow a voting strategy. As well as breaching confidentiality this also establishes the potential of biasing the election outcome.



4.3 Availability risks

Availability refers to the ability of users to access the system when they're supposed to. Naturally, the first thing that comes to mind is the ability of voters to connect to the system during the period of the election. However, availability risks extend throughout the election cycle, starting from online voter registration, where a denial of service (DoS) attack would disproportionately affect people voting for the first time, to initialisation of equipment and/or software for a particular election and through to the final stage of auditing and ultimately archiving the results and votes.

Availability can be affected by natural causes such as power outages, equipment failure or system overload, sometimes referred to as benign faults. They can also be due to the coordinated effort of an adversary, sometimes referred to as malicious faults. While the internet as an environment is, in general, robust against benign faults, it can be a particularly hostile place in the presence of a coordinated attacker that aims to disrupt a service through a DoS attack. The problem's exacerbated further in the context of voting, since the attacker may choose to selectively and adaptively disrupt system availability, targeting specific areas that support a particular candidate or election choice that the attacker wants to suppress. Given the potentially small margin between election outcomes, it's conceivable that minor targeted availability failures can significantly influence an election outcome. For this reason, it's natural to impose a vigilant regime for protecting availability, ensuring that the voting system enjoys near perfect availability throughout the election lifecycle.



4.4 Manipulation risks

Manipulating the election is a general risk referring to an attacker's ability to influence a voter's input so that the outcome is biased in a certain way. Manipulation attacks and risks that in some way involve the technical aspects of the underlying election protocol are critical to consider.

Coercion in the context of a voting system can be achieved by either forcing the voter to deliver the credential they've received in order to participate in the election process, or forcing the voter to follow a particular strategy during ballot casting that will enable the coercer to influence the voters' choice. A coercer is always capable of trying to influence a voter, but what's of interest here is understanding whether any underlying technical features of the voting system make it easier for the coercer to attack the voting process.

Internet voting can be particularly susceptible to coercion attacks since many internet voting systems outsource the responsibility of creating a private environment for ballot casting to the voter. This is in contrast to onsite voting, where voting takes place privately, under controlled conditions.

Vote selling and buying is the flipside of the same problem. If a voter can demonstrate how they voted, this gives the ability to sell the vote. It is important to eliminate the risk that the underlying system somehow facilitates this vote buying, and particularly the risk that this could be automated.

Internet voting also risks trivialising the election process. Participating in an election can be perceived by many as a form of ritual that underscores this important citizen responsibility. Terms such as 'celebration of democracy' have been frequently associated with an election day by the media. Given this and the ease with which a point-and-click internet voting system can operate, there's a potential risk of trivialising the election process, leading to higher uninformed participation, randomisation of inputs and potentially increasing further the risk of manipulation.

4.5 Attack targets

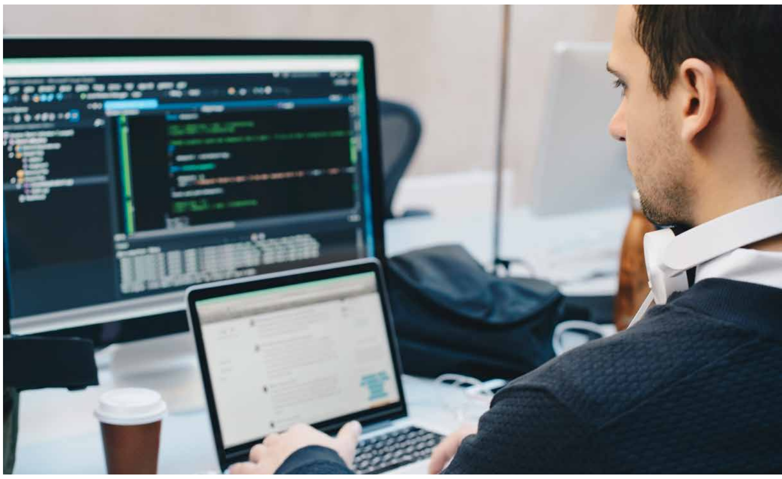
A natural target for cyberattacks would be the central election management systems responsible for running the election, management of electoral roll, voter authentication, and management of the votes as they are cast and tallied.

A range of possible attacks can be considered. Distributed denial of service (DDoS) attacks can disrupt the voter registration process or the election itself and can be targeted to affect particular voting groups. Alternatively, the authentication processes might be bypassed or undermined on the election servers or at the certification authorities, enabling additional votes to be cast directly. Intruders may be able to access the electronic ballot box, which could enable vote tampering or ballot stuffing. Such attacks may be carried out at election time by an active adversary or might be the result of malware or malicious hardware planted ahead of time.

In any case, there needs to be a high degree of confidence in the software, hardware and infrastructure running the election systems, as bugs and faults can also introduce errors that may impact on election results or on the smooth running of an election. A DoS is no less disruptive for being accidental, for example if too many voters attempt to access the system simultaneously.

Another target could be the computers used by voters to register and cast their votes. These devices might still have legacy applications, such as out of date browsers with known vulnerabilities, making them susceptible to a range of exploits. Even devices with up-to-date security are vulnerable to a wide range of zero-day exploits. Attacks can be carried out through malware, which could change the vote cast by the voter so that a different choice is sent to the election system. There's also a risk to vote privacy through unauthorised monitoring of how the vote is being cast, such as keylogging.

Finally, humans can also be targeted. Human factors play a key role in cybersecurity, and the ability of voters to follow the voting process correctly will be critical. This is a general security issue, but in our case there's a risk that voters will be the subject of misinformation campaigns, perhaps resulting in failure to register, cast a vote, or carry out the security checks required to ensure it's been cast correctly.



Particular sets of voters, such as subscribers to a left/right leaning group on social media, might be directed towards a fake website that convincingly poses as the official voting website, possibly through email or social media phishing campaigns. This would lead to those votes being lost and not counted, or the theft of their voting credentials which could be used to cast an alternative vote on the genuine site.

Another key element to consider is the **usability** of any cybersecurity mechanisms. A large body of research has highlighted that if cybersecurity disrupts the primary task, then users are likely to see it as a burden. This may lead to disengagement with the system in the first instance, and workarounds or misunderstandings that may open up opportunities for those interested in compromising the integrity and authenticity of the voting process.

4.6 Risk mitigation

Any voting system, independently of whether it runs over the internet or not, should provide concrete risk mitigation strategies and techniques against all the issues identified and consider the vulnerability of the possible targets.

It's expected that complete risk elimination might be impossible in most cases. Therefore, it's important to understand what procedural, system and mathematical, if any, assumptions are made to minimise the potential risks, and importantly whether these are outweighed by the benefits.

Furthermore, in case a risk materialises, it's crucial for the system to have the ability to recover an election and identify the perpetrators. This is a particular challenge if the culprits reside in another country or if the attacker is a nation state.

5. Case study: Norway

In 2007 the Norwegian Parliament decided to pilot internet voting. The objective was to test internet voting in a limited set of municipalities until 2013, and then evaluate to further adopt it across the country.

The project, known as eValg, was managed by the Ministry of Local Government and Regional Development (KRD), which set up an internal project team in 2008. Since the beginning, the team recognised that any implementation of internet voting should be transparent and auditable in addition to providing privacy and integrity of the election. For this reason, individual and counted-as-cast verifiability were some of the main requirements of the voting system. In addition, KRD involved external experts and academics during the evaluation of the different solutions and the implementation of the internet voting system before and during the election.

The requirement for transparency also meant that source code for each pilot was published, and reports from auditors and complete documentation about the voting system were also made public[26], including specifications of the security functionalities, risk analysis and security architecture, using the Common Criteria framework as reference.

In addition to standard security properties such as end-to-end encryption, in 2011 the Norwegian internet voting system initially used cast-as-intended and counted-as-recorded verifiability. Cast-as-intended verifiability was implemented using return codes[27], while counted-as-recorded was implemented by using a universal verifiable heuristic proof of a shuffle[28].

The 2013 system incorporated some improvements on verifiability, such as recorded-as-cast by means of voting receipts and a public bulletin board. A coding error in 2013 resulted in weak encryption of 40,000 ballots before this was discovered during the election and corrected.

To mitigate vote coercion, the system allowed multiple voting from the internet, only the last one was counted, or at polling stations. At polling stations, voters were allowed to cast only one vote, but this vote invalidated any other vote cast from the internet.

The final participation numbers from the 2011 election reflected a high acceptance of internet voting for the advanced voting electorate. Internet votes represented the preferred channel with 73% of the advance votes, comprising 27% of the overall votes. For 2013, internet voting participation increased and improved the numbers achieved in the previous municipal election, with 76% of the advanced votes representing 36% of the total votes. However, overall turnout didn't increase in the trials.

From a political point of view, the internet voting pilots in both 2011 and 2013 were highly controversial, and motions to stop them were put forward by the Conservative Party and supported by the Progress Party, in both rounds. Further piloting was halted after a coalition of the Conservative and Progress parties came into power after the 2013 election, and the Ministry of Local Government and Modernisation identified that political disagreement wasn't conducive to the introduction of internet voting[29]. Research commissioned by the KRD also showed that voters' knowledge of the security mechanisms was little known, for example that a paper vote would cancel an electronic vote. This undermined re-voting as a coercion resistance measure.

[26] https://web.archive.org/web/20120309072858/http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/source-code/the-system-architecture-.html?id=645240

[27] Jordi Puiggalí, Sandra Guasch. Cast-as-Intended Verification in Norway. Proceedings of the 5th Conference on Electronic Voting 2012 (EVOTE2012) P-167, LNI GI Series, Bonn, July 2012.

[28] Jordi Puiggalí, Sandra Guasch. Universally Verifiable Efficient Re-encryption Mixnet. EVOTE2010: The 4th International Conference on Electronic Voting, Bregenz (Austria), July 2010.

[29] https://www.regjeringen.no/no/aktuelt/Ikke-flere-forsok-med-stemmegivning-over-Internett-/id764300

6. Socio-technical factors

> Although we don't believe the UK is currently ready to deploy internet voting in statutory political elections, here we consider the socio-technical issues that need to be considered ahead of any future deployment.

One of the most crucial factors that make an internet voting system viable is sufficient **public demand**. The Electoral Commission's 2019 Winter Tracker survey revealed that 76% of respondents are satisfied with the current voting process. It also showed that 90% of those who vote in polling stations trust that their vote is safe from fraud and abuse, but this drops down to 68% for postal voters[30].

On the other hand, a recent consultation in Scotland[31] identified a strong diversity of views without any clear consensus on whether e-voting could guarantee the electoral process to be "*verifiable, secure and anonymous*". It's clear that there are concerns around the security of such systems among some proportion of the public. Concerns about trustworthiness and security were also reported in a recent report of the House of Lords Select Committee on Democracy and Digital Technologies[32].

When considering the widespread deployment of internet voting, we must consider the wider socio-technical context in which such a system will exist. There are many factors to consider from public demand and acceptability through to trust and ensuring equal access. With widespread reports of nation state interference in elections overseas, there's a risk that public trust in electoral systems and their integrity is eroding. Trust can, of course, be generated by demonstrating that a technological development is *provably* free from interference. However, most users will be non-specialists and hence non-technical factors – that is social, organisational and informational indicators of trust – are equally important, if not more so.

In current voting systems, there are many of these markers. People put their faith in polling station voting because they know the ballot box will be sealed and there are other processes in place to protect their vote. It's as much due to the visual markers, processes, for observing counting and requests for recounting, and ritualistic nature of voting that trust is generated as it's due to the perceived integrity of the electoral commission and the officials in charge.

76% of UK respondents are satisfied with the current voting process

[30] https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-views-and-research/our-research/public-attitudes

[31] https://www.gov.scot/publications/electoral-reform-consultation-analysis/pages/3

[32] Digital Technology and the Resurrection of Trust, House of Lords Select Committee on Democracy and Digital Technologies, 29th June 2020.

90% **of UK voters using polling stations** trust that their vote is safe from fraud and abuse, **but this drops down to 68% for postal voters**

How do you generate trust in the absence of such markers? Informing users that the voting mechanism is provably secure in a *mathematical or technical sense* alone isn't sufficient, and can also be targeted by disinformation campaigns to compromise trust. With widespread news of vulnerabilities in mobile devices, applications and software and persistent legitimate concerns about leakage of private information, a detailed and thorough analysis is required as to what factors and assurances will be needed. This is especially difficult in the context of fake news, where unsubstantiated claims challenging election results need to be rebutted.

As well as public acceptance, **political consensus** is required for the introduction of online voting. Politicians will want to ensure the highest possible levels of security, usability and trust before implementing such a system. Although digitising electoral services could win them favour with the electorate, they wouldn't want to be held responsible for rolling out such a critically important, democratically sensitive system that then fails, or is perceived to be unsafe, untrustworthy or otherwise not fit for purpose. Having a political consensus would also help avoid a situation where a change in government pushes for a recently introduced system to be withdrawn, as occurred in Norway after the 2013 trials.

The introduction of technology into elections will need to consider the impact on various demographics to ensure that particular social groups are not disadvantaged or excluded. In Great Britain, 7% of households still don't have access to the internet, and there is less frequent use among older people[33]. The needs of voters in these demographics must be catered for.

It's equally important that any introduction doesn't disenfranchise already disengaged individuals and communities. Many individuals and communities have concerns about sharing their private information with online platforms, exacerbated by scandals such as Cambridge Analytica, and would require assurances and evidence of proper use, checks and balances, before engaging with such a system.

For all of these reasons a **gradual introduction** or transition with a **dual paper/electronic** system would be needed, at least at the outset. **Transparency** will be critical for generating trust. It's noteworthy that the approach taken in Norway placed a deliberate emphasis on the openness of the system, and the authorities in Switzerland required a public intrusion test of their system as a precondition for deployment. A gradual introduction would require small-scale trial locations/populations to be appointed before the system is scaled up, and decisions would have to be made about where these trials take place, when, and why that sample size/area was chosen.

This approach was taken in Norway, in the UK trials and also in Switzerland in terms of managing the initial scale. Any such trials would need to be preceded by scoping studies to identify the types of indicators, processes, information and potentially institutions that would be required to generate trust and acceptability in a diverse range of users. These would then need to be tested and evaluated as part of the trials. Without due consideration and evaluation of such socio-technical factors, even the most secure internet voting system may not see widespread adoption or usage.

7%

of households in Great Britain still don't have access to the internet, and there is less frequent use among older people

[33] https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics
homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2019

7. Case study: Estonia

Estonia's approach to internet voting was underpinned by e-id cards, use of repeated voting and the evolution of technical aspects of the system.

In 2005, the country introduced internet voting to run as an additional voting channel alongside polling stations. Between 2005 and 2019, internet voting has been used a total of 10 times, in local municipal elections, national parliamentary elections and European Parliament elections. The proportion of voters voting over the internet has gradually increased over that period. The 2019 parliamentary elections had a total of 247,232 votes over the internet; 43.8% of the total and the highest proportion to date. Estonia doesn't use postal voting, so voting over the internet is the only option for remote voters unable to vote in person.

The voting system is underpinned by the Estonian national e-identity infrastructure, which manages citizens' state issued digital identity. Citizens are able to authenticate remotely and to provide legally binding digital signatures by means of the Estonian ID-card; an identity document and smart card that Estonian citizens are required to have, and from mobile devices either via an enhanced SIM or application. These all provide access to Estonia's secure online services.

E-voting is allowed ahead of the election day, but not on the election day itself. Voters vote via an application on their platform of choice. The application confirms their identity and eligibility to vote, manages the choices offered, collects the candidates made choice and encrypts and submits this to the electronic voting system. The system assumes that the owner of the card is the person who is voting. Voters can cast multiple electronic ballots, with only the last one counted as the vote. Voters can also cast a paper ballot in a polling place, which supersedes any electronic vote they have cast.

The system provides voters with individual verifiability, so that they can optionally confirm that their vote has been correctly received by the system. This is carried out on an independent device via a verification application, which uses a QR code from the voting application and downloads the vote from the central system so the voter can confirm it corresponds to their choice. This opportunity is available for a limited time (30 or 60 minutes) following the casting of the vote.

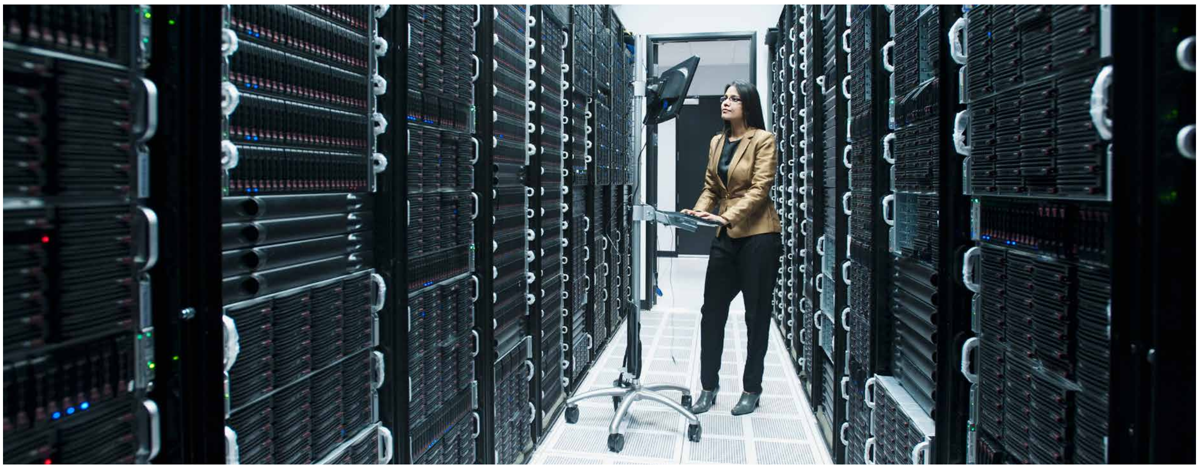
The system also uses universal verifiability mechanisms for processing the electronic votes, including a mix net, a cryptographic mechanism for shuffling and anonymising the votes. This verification is not public but carried out by the official data auditor, although it could in principle be performed by independent observers. However, there are no independent means to verify that the votes tallied correspond to the votes cast.

The security of the system relies on the security of the database of signed and encrypted cast votes. The server-side source code and mobile phone verification application have been made available for open review since 2013.

Since its introduction, there have been ongoing challenges to various aspects of the system, including legal challenges raised and insecurities identified[34]. The Estonian National Electoral Committee has defended its deployment of the system. Several aspects of the current deployment, including individual verifiability (2013), the publication of the source code (2013) and universal verifiability (2017) have been introduced over the years in response to such concerns. In June 2019 the Minister of Entrepreneurship and Information Technology set up a working group to assess the verifiability, security and transparency of the Estonian electronic voting system. At the time of writing, this assessment is ongoing.

[34] For example, see Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, J. Alex Halderman: Security Analysis of the Estonian Internet Voting System. ACM Conference on Computer and Communications Security, 2014.

8. Technical and system requirements



The security requirements of electronic voting make it very challenging to design and implement a suitable system. The security requirements fall into two categories:

- **Integrity properties**; the declared outcome should be correct, and **verifiability** properties; it should be possible for a voter or independent observer to independently verify the correctness.
- **Secrecy properties**; the way a particular voter votes should not be revealed, and **incoercibility properties**; a voter can't convince a potential coercer or vote-buyer that they have voted in a particular way.

These properties are hard to achieve, especially when you consider the potential capability of an adversary. The adversary could be a well-resourced nation state, capable of spreading malware on a big scale and of corrupting, amongst others, high-ranking officials, system providers and maintainers and software developers.

Over recent decades, the computer security industry has developed a variety of security mechanisms. These include technologies commonly used for securing phones and laptops, such as virus scanners, patches and updates, opensource software and remote device management. More recently there has been interest in *hardware roots of trust* on consumer devices, either in the form of specialised chips like a *trusted platform module* and Google's *Titan* chip, in special processor modes such as Intel *SGX enclaves* and ARM *TrustZone*, or in due course through emerging technologies such as CHERI architectures.

Second-factor devices for authentication, such as special hardware devices for electronic banking, RSA key fobs and authenticator apps on mobile phones, have also made valuable contributions to consumer applications, such as electronic banking and access to corporate accounts. But all these technologies rely on the trustworthiness of manufacturers and programmers. In the context of the nation-state adversaries we have in mind, they appear inadequate.

It's helpful to directly compare the security requirements and risks of electronic banking and electronic voting. Perhaps surprisingly to some people, electronic banking is much easier to make secure than e-voting. From the point of view of integrity, that's partly because a banking user has easy mechanisms to verify whether their account has been manipulated or not. A bank holder can simply look at the statement of transactions and contest any that don't look right. But in voting that's not possible. The secrecy requirements mean that we can't publish a statement of who voted how, for everyone to see. In electronic banking, the secrecy requirement is very low. While we may not want our banking records published in the public domain, we accept that hundreds of bank employees and administrators can read them. Therefore, the potential strength of the adversary, and the dual requirements of secrecy and integrity, make e-voting a uniquely difficult challenge for computer security.

9. Case study: Switzerland

Regarding e-voting, the Swiss Federal Chancellery states[35]:

"In Switzerland, e-voting means voting online via the internet. The Confederation and the cantons have been conducting trials with e-voting for more than 15 years as part of the 'Vote électronique' project. A significant number of voters have been able to cast their ballots online in National Council elections and in popular votes on federal proposals. In over 300 trials to date, a total of 15 cantons have allowed certain groups of citizens to vote online. Up to two-thirds of voters in cantons where online voting is possible have chosen to make use of the e-voting option."

"The Confederation and cantons have followed the principle of 'security before speed'. In Switzerland, e-voting is only permitted if strict requirements under federal law are met. The key security element is verifiability. Currently, systems with individual verifiability are being used."

"A completely verifiable system could be available starting from 2020."

"Certification, the publication of the source code of the systems and the conduct of public intrusion tests are required before systems with complete verifiability can be used."

Individual verifiability is achieved by producing individualised verification codes per voter, together with a finalisation code. The verification and finalisation codes are sent by mail to the voters. When they cast a vote, the system computes, without breaking the vote secrecy, one or more verification codes and returns them to the voter. They then compare these with the ones received earlier by postal mail. If they match, the voter then confirms the successful casting of a vote by sending the finalisation code.

The legal basis for e-voting in Switzerland is provided by an ordinance and its technical annex. The ordinance states that if 100% of the electorate shall be permitted, then the e-voting system must provide individual and universal verifiability. If an e-voting system provides individual verifiability only, then only 50% of the electorate are allowed to cast their votes electronically. An addendum to the ordinance adds the obligation to system providers to open source the formal specification and the source code of the software. The ordinance defines a certification process and requires that once certified, the supplier publishes its source code and related documentation and carries out a public intrusion test[36]. It's worthwhile noting that the ordinance doesn't require an e-voting system to provide means against coercion.

At the end of 2018 the Swiss Post (Scytl) voting system achieved the certification for 100% of the electorate and in early 2019, a public intrusion test was carried out with the Scytl system. Before the public intrusion test, the specification of the system as well as the source code was published.

A number of groups and individuals analysed the system specification and published findings highlighting that it was possible to manipulate election data in a way that a universal verifier wouldn't be able to detect. This manipulation could lead to a changed voting result and/or to invalid votes in case a malicious insider has full control of the first node of the counting process and can get access to the vote casting process. It turned out that the same findings applied to the source code, but the protocol computational proofs used to prove the security of the voting system weren't affected[37].

In parallel, the public intrusion test identified 16 non-critical vulnerabilities. Since the implementation issues impacted the verifiability requirements of the certification process, the Scytl voting system wasn't authorised for use in elections until solving the detected issues and re-certifying the voting system again.

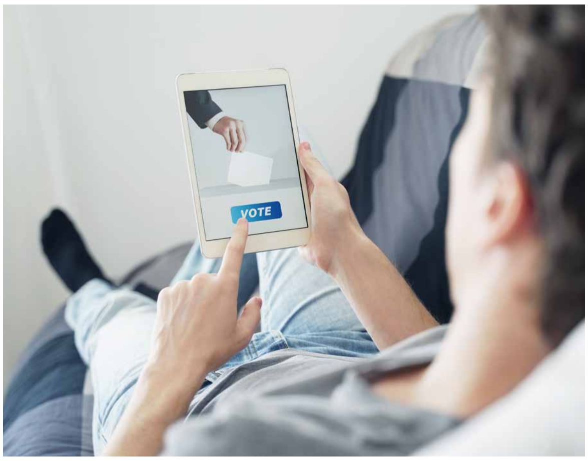
As a consequence of these shortcomings, the Federal Council decided on 26 June 2019 not to use e-voting until further notice and instructed the Federal Chancellery to redesign the e-voting trials by the end of 2020.

[35] https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

[36] Puiggali, J., Rodriguez-Peréz, A.: Designing a national framework for online voting and meeting its requirements: the Swiss experience. In: Krimmer, R., et al. (eds.) E-Vote-ID 2018 Proceedings, pp. 82–97. TUT Press, Tallinn (2018)

[37] Puiggalí, J: Implementing a public security scrutiny of an online voting system: the Swiss experience. In: Krimmer, R., et al. (eds.) E-Vote-ID 2019 Proceedings, pp. 311–326. TUT Press, Tallinn (2019)

10. The academic researcher's dream: outcome verifiability



To address the challenge of security, researchers have proposed the concept of 'outcome verifiability'; where a voter, or observer, has an independent means to verify the outcome of the election. Three aspects can be verified:

- That a vote was included in the declared outcome. This is called **individual verifiability**.
- That only eligible votes were included in the count. This is called **eligibility verifiability**.
- That the outcome was computed correctly. This is called **universal verifiability**.

The case studies from Switzerland, Estonia and Norway underscore that verifiability is recognised as a necessary aspect of an internet voting system. They all contain forms of verifiability, particularly cast-as-intended; an element of individual verifiability allowing the voter to confirm that their vote was captured as they intended.

Outcome verifiability is also called 'software independence', a term that emphasises that the outcome is verifiable independently of the software and hardware that was used to produce it.

Another way to think about outcome verifiability is via the concept of a trusted computing base (TCB). The TCB of a system is the set of hardware and software components required to be assumed to be trustworthy. In computing, the operating system is usually in the TCB since it's required to be trusted in order for the whole system to be trustworthy. If the TCB of a system is very large, it means we have to assume a lot of things are secure. If the TCB of a system is small that's much better, we can make fewer assumptions. The idea of outcome verifiability demands that the TCB is the empty set, that is, there are no components of the system which have to be assumed trustworthy. This shows again that e-voting is a uniquely hard challenge.

The familiar technologies of computer security mentioned earlier: virus scanners, software patches, and even specialised hardware in the form of integrated chips or second-factor devices, aren't able to provide outcome verifiability.

How could outcome verifiability be achieved? Because it's difficult to directly verify the means by which the outcome was computed (the hardware and software of the voting system), researchers have focused on providing voters with the ability to verify the result themselves. The idea is that the system should output data which can be analysed by voters and observers. Of course, this data cannot reveal how individual voters voted, so it will need to be encrypted. But the encryption must be such that meaningful analysis is possible, even though the votes of individuals cannot be identified.

Therefore, voting schemes typically use techniques including homomorphic encryption and zero-knowledge proofs, which allow just enough information to be disclosed for the verification to be possible, while not violating the requirements of secrecy. Ideally, a scheme should offer everlasting privacy, meaning that votes are not revealed even if there are advances in cryptanalysis or computing against the encryption schemes used.

Unfortunately, systems that provide outcome verifiability tend to have rather weak usability properties. They may require users to perform procedures whereby the purpose is hard for people to understand, and that aren't required in traditional elections. For example, some systems require the voter to use two devices, one that constructs their encrypted ballot and another that audits this construction. However, there is an additional requirement that an audited ballot can't be cast, so the voter is told that they can construct and audit as many as they like to gain confidence in the system, but have to cast one that they haven't audited. This can be complicated and confusing for users.

11. Conclusion: where should we go from here

While outcome verifiability is a commendable aim, no system has been proposed that implements it in a way that could be used in practice by millions of voters in a large-scale, politically binding election.

But there's still a compelling case for some form of e-voting. In proposing outcome verifiability as the key requirement, perhaps security researchers have set the bar too high. Paper-based voting systems are certainly not perfect from a security perspective. Their main advantage is that large-scale attacks are difficult to perpetrate and that those systems, including their flaws, are well-understood by voters and observers.

Even though there's still research in the area, we have to accept that we might never have a satisfactory system satisfying outcome verifiability. Therefore, the challenge emerges of properly defining security requirements that are weaker than outcome verifiability, in a well-understood and acceptable way, but are intuitive and realisable on a suitably large scale.

Additionally, there are practical requirements that, to date, haven't gained significant attention by researchers:

- **Secure identity management** is a prerequisite for outcome integrity, alongside the reliability of the electoral roll. The need for voters to establish their eligibility to vote, and not have their credentials stolen or passed on, requires some form of digital identity management, as well as ease of self-enrolment. Estonia's system requires users to log-on using their national ID-card or their Mobile-ID[38], which underpins the whole process. The UK doesn't currently run any such system, and it's not clear whether the public would be in favour of a similar approach.

- **User interface design** is challenging for secure applications; voters won't always be thinking about security when interacting with voting systems. It's a socio-technical problem to design usable and intuitive systems in which security is assured in the context of typical user behaviour, especially for a system that will be infrequently used. There's also the risk of fake voting apps or websites that look like the real one but interfere with the vote.

In conclusion, electronic voting has unique and challenging security requirements, and no system has been proposed which is capable of meeting them in their strongest form. Most academics hold the view that there are still challenges to be solved before we are ready to deploy electronic voting in large-scale national political elections. While small scale and lower stakes elections can be fertile ground to deploy and improve verifiable e-voting systems and should be pursued, development of e-voting for national elections should wait and allow more time for the technology to mature and become standardised by wide national and international coordination efforts.

With respect to the current system of voting in the UK, we consider that **accessibility** is the strongest driver for internet voting, enabling voting remotely and through use of technology which voters with disabilities may need to cast their ballot in secret. However, cybersecurity is a critical challenge and technology isn't now, or in the near future, in a position to address the range of cybersecurity threats that could undermine an internet voting system.

[38] https://e-estonia.com/solutions/e-governance/i-voting

12. Acknowledgements

The IET would like to thank the IET members, volunteers and their organisations, and others, for their participation in the round tables and contributions through the questionnaire. In particular we'd like to thank the following individuals for their time spent with the authors in the creation of this document.

Pascal Crowe
Data and Democracy Project Officer, Open Rights Group

Ian Levy
Technical Director, National Cyber Security Centre (NCSC)

Craig Westwood
Policy and Research, The Electoral Commission

Mark Williams
Policy Manager, The Electoral Commission

13. About the IET

We are the IET - a charitable engineering institution with over **167,000 members in 150 countries** – working to engineer a better world.

Our mission is to inspire, inform and influence the global engineering community to advance technology and innovation for the benefit of society.

As a diverse home across engineering and technology, we share knowledge that helps make better sense of the world in order to solve the challenges that matter. It's why we are uniquely placed to champion engineering.

We bring together engineers, technicians and practitioners from industry and business, from academia and research, and from government and the third sector. We are member-led, independent and impartial.

We cover engineering across industry from design and production, digital and energy to healthcare, transport and the built environment. We champion engineers and technicians by offering networking, volunteering and thought leadership opportunities.

To find out more contact **sep@theiet.org**

The Institution of
Engineering and Technology

Our offices

London, UK
T +44 (0)20 7344 8460
E faradaycentre@ietvenues.co.uk

Stevenage, UK
T +44 (0)1438 313311
E postmaster@theiet.org

Beijing, China
T +86 10 6566 4687
E china@theiet.org
W theiet.org.cn

Hong Kong
T +852 2521 2140
E adminap@theiet.org

Bangalore, India
T +91 80 4089 2222
E india@theiet.in
W theiet.in

New Jersey, USA
T +1 (732) 321 5575
E ietusa@theiet.org

@TheIET

theiet.org

The Institution of Engineering and Technology (IET) is working to engineer a better world. We inspire, inform and influence the global engineering community, supporting technology innovation to meet the needs of society. The Institution of Engineering and Technology is registered as a Charity in England and Wales (No. 211014) and Scotland (No. SC038698). Michael Faraday House, Six Hills Way, Stevenage, Hertfordshire, SG1 2AY, United Kingdom.