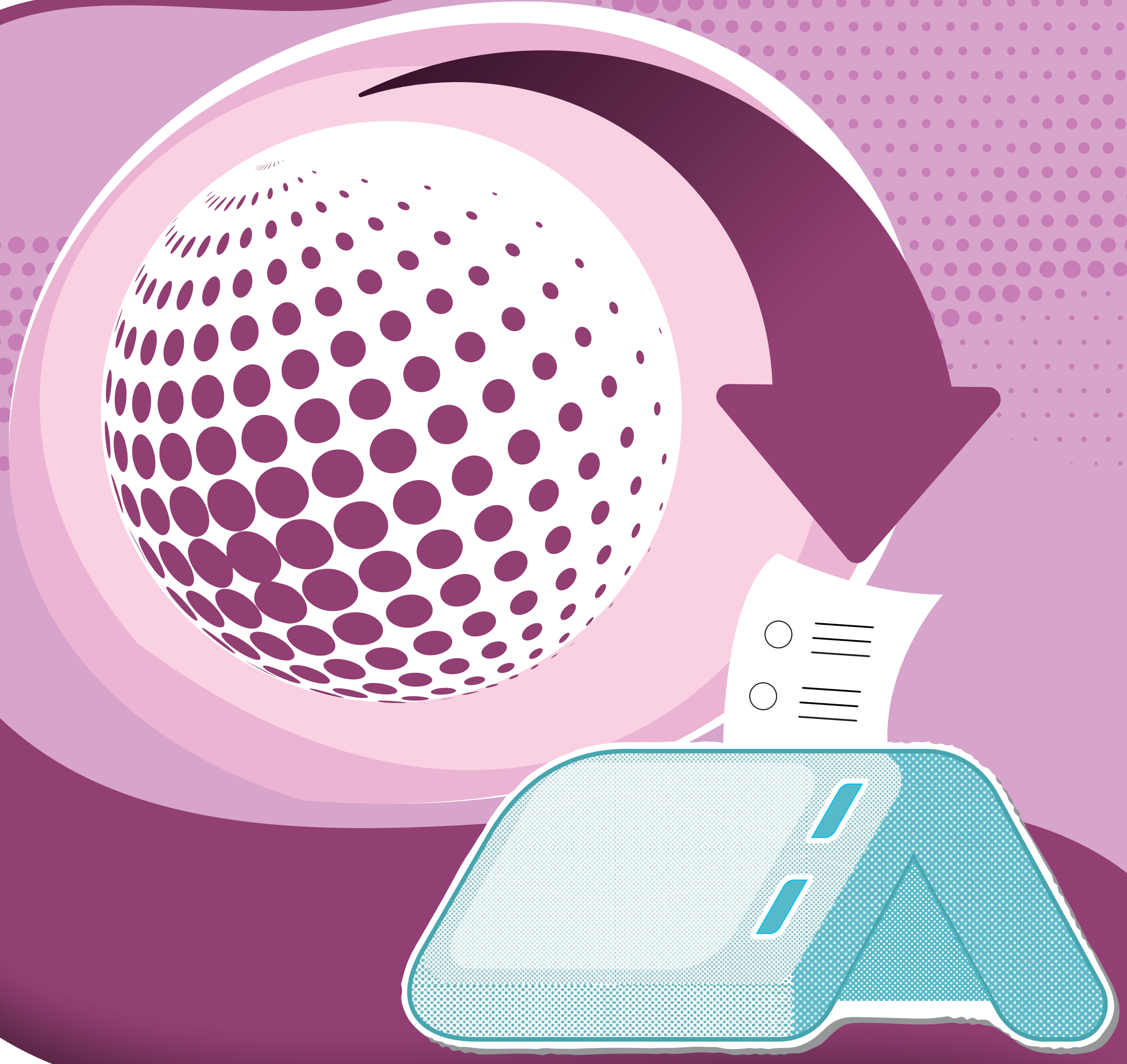
GEORGIAN YOUNG LAWYERS' ASSOCIATION



IMPLEMENTING E-ELECTIONS: THE KEY CONSIDERATIONS

IMPLEMENTING E-ELECTIONS:
THE KEY CONSIDERATIONS

Tbilisi
2024

The report was prepared by the Georgian Young Lawyers' Association, with the support of the United States Agency for International Development. The opinions expressed in the report belong only to the Georgian Young Lawyers' Association and its content may not reflect the views of the donor organization.

Report Supervisor: NANUKA KRUASHVILI

Author: REID JACKSON

Editor: KHATUNA KVIRALASHVILI

Technical Editor: IRAKLI SVANIDZE

Cover design: TEONA KERESELIDZE

J. Kakhidze street #15, Tbilisi, Georgia
(+995 32) 295 23 53, 293 61 01
www.gyla.ge

INTRODUCTION

Free and fair elections are a prerequisite for a functioning democracy.[1] Elections themselves are a widely understood practice, benefitting from thousands of years of history and the experiences of countless individuals who can recall examples dating back to their early childhoods, whether that be votes for a class president or a captain of a sports team. There is not a single correct way to conduct an election, but all elections should pay attention to some key considerations in implementing new systems. Unlike picking out a scarf, choosing an election system should not be one-size-fits-all.

No method of conducting an election ensures that an election is free and fair, but when considering a new method for an election, it is necessary to mitigate risks that can cause elections to be unfree or unfair, or both. The implementation of an election system should be carried out with regard to best practices while keeping the relevant cultural, political, economic, and technological context in mind. These considerations include political will, public trust, security, inclusiveness, and cost. When trade-offs appear between these considerations, decisions should be made through cost-benefit analyses and through pragmatic decision-making.[2]

In the Republic of Georgia, it is estimated that 90% of voters will vote through the use of electronic technologies in the upcoming 2024 elections.[3] The country has previously run trials of the electronic vote counting technology in previous elections, but 2024 marks their first expanded use in a national election.[4] In order to properly assess the implementation of an election system, it is necessary to provide a brief overview of the most common electronic voting systems themselves. Then, the aforementioned considerations of political will, public trust, security, inclusiveness, and cost will be discussed. The use of electronic technologies in elections is relatively new, but there are standards available to help guide states implementing these technologies.

The Council of Europe (CoE) has detailed the standards that it recommends its member states comply with when implementing electronic elections. These standards are meant to comply with the five principles of universal, equal, free, secret and direct suffrage.[5] Furthermore, there is an explicitly referenced principle of holding elections at regular intervals. The CoE is the only organization that has set intergovernmental standards for electronic voting, and therefore, it represents a useful benchmark for countries, regardless of whether they are member states.[6] When discussing voting systems these five principles should be held in mind.

ELECTION SYSTEMS OVERVIEW

Most elections are conducted without the use of information and communications technologies (ITCs), but some use ITCs in the form of electronic voting. Electronic voting (e-voting), broadly de-

[1] Elklit, Jørgen, and Palle Svensson. "The Rise of Election Monitoring: What Makes Elections Free and Fair?" *Journal of Democracy* 8, no. 3 (July 1997): 32–46. https://doi.org/10.1353/jod.1997.0041.

[2] McCormack, Conny B. "Democracy Rebooted: The Future of Technology in Elections." Atlantic Council, 2016. https://www.atlanticcouncil.org/in-depth-research-reports/report/democracy-rebooted-the-future-of-technology-in-elections-report/.

[3] Civil Georgia. "90% of Voters Will Vote Electronically in 2024 Parliamentary Elections," February 7, 2023. https://civil.ge/archives/524496.

[4] Chikhladze, Mariam. "FUTURE OF E-VOTING IN GEORGIA." Eastern European Centre for Multiparty Democracy (EECMD), 2021.https://www.agora-parl.org/sites/default/files/agora-documents/Future%20of%20E-voting%20in%20Georgia.pdf

[5] Council of Europe (Venice Commission). 2002. Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report. Strasbourg: Council of Europe. https://rm.coe.int/090000168092af01

[6] Electoral assistance. "E-Voting - Electoral Assistance - Www.Coe.Int." Accessed February 16, 2024. https://www.coe.int/en/web/electoral-assistance/e-voting.

fined, includes electronic technologies used in the recording, casting or counting of votes.[7] E-voting is an umbrella term, and it is important to note that it does not mean internet voting, though internet voting is a type of e-voting. According to the IDEA international database, 79% of countries surveyed do not use e-voting in any elections.[8] Instead, these elections are often conducted through the tried-and-true methods of the paper ballot and the pen. These votes are then compiled and hand-counted by election management bodies (EMBs).

Yet, in many countries different technologies have been adopted in pursuit of building election systems that are more efficient and trustworthy. This has led to a proliferation of different electronic technologies used around the world. This document will focus on some of the more prevalent e-voting systems, offering insights into their advantages and limitations.

Direct-Recording-Electronic (DRE) Machines

The first e-voting systems to consider are older generation direct-recording-electronic (DRE) machines, which became prevalent in the latter part of the 20th century, but have been steadily falling out of favor. For example, in the United States traditional DRE machines are considered outdated. Yet, mostly due to funding constrictions, 16 states within the US still use DRE machines as of 2022.[9]

DRE machines use an electronic interface that the voter interacts with to cast their vote. Voters use one machine through which their votes are both cast and counted. Although straightforward in principle, DRE machines are seen to have a 'black-box' nature because of the fact that it may not be clear to the average voter how the machine works, which may result in the voter not knowing whether their vote was cast as intended.[10] In the use of DRE machines, the voter is unable to instantly verify that their vote has been properly recorded because there is no physical evidence of their vote. Also, without a paper-trail, neither parallel vote counting nor physical audits of vote counts are possible using DRE machines.[11]

These problems have been resolved by certain EMBs through the implementation of newer DRE machines complete with what is known as voter-verified paper audit trail (VVPAT) technologies.[12] These DREs with VVPAT can take various forms, but ultimately voters using these systems cast their vote electronically on a DRE machine, which prints out a ballot, which then voters review, before their vote is finally submitted. The key disadvantages of DRE with VVPAT systems are their complexity and relatively high costs.[13]

[7] Wolf, Peter, Rushdi Nackerdien, and Domenico Tuccinardi. "Introducing Electronic Voting: Essential Considerations." Policy Paper. International IDEA, December 2011. https://www.idea.int/publications/catalogue/introducing-electronic-voting-essential-considerations.

[8] "Database Result (Question Only) | International IDEA." Accessed February 16, 2024. https://www.idea.int/data-tools/data/question?question_id=9348&database_theme=327.

[9] 8609, and 212. "Voting Machines at Risk in 2022 | Brennan Center for Justice." Accessed February 16, 2024. https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-2022.

[10] "Digital Technology in Elections: Efficiency versus Credibility?" European Parliament, October 9, 2018. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2018)625178.
"Voting Machines at Risk in 2022 | Brennan Center for Justice." Accessed February 16, 2024.
https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-2022.

[11] Norden, Lawrence D. "THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD." VOTING RIGHTS & ELECTIONS SERIES. BRENNAN CENTER FOR JUSTICE, June 2006. https://www.brennancenter.org/our-work/research-reports/machinery-democracy-protecting-elections-electronic-world.

[12] *Ibid.*

[13] Goldsmith, Ben, and Holly Ruthrauff. *Implementing and Overseeing Electronic Voting and Counting Technologies*. International Foundation for Electoral Systems and National Democratic Institute for International Affairs, 2013. https://www.ndi.org/implementing-and-overseeing-e-voting-counting-technologies.

Electronic Ballot Printers (EBPs)

A similar system that is used for casting votes makes use of electronic ballot printers (EBPs) and optical scanning technology. In this scenario, a voter makes their selections electronically and then is provided a printout of the ballot, which they are able to review. Finally, the voter then submits the printed ballot into a separate machine, which records and tallies their vote. EBPs do not record votes.[14] The voter's ballot is only counted once it is submitted into the second machine, the optical ballot scanner.[15] EBPs can also be used with the hand-counting of ballots, instead of an optical scanner.[16]

The EBP and optical scanning system has all the necessary hallmarks of a secure, inclusive, and efficient voting process, but, again, this method comes with added complexity as well as higher costs.[17] The technological know-how required to maintain these machines, combined with the high costs associated with using two electronic machines in the voting process, makes this system unfavorable for scenarios where the cost of elections is a key consideration.

Paper Ballot and Optical Scanning

Another electronic voting system just removes the EBP machines mentioned above. Here, voters are provided with a paper ballot which they mark using a pen. Then, they submit their paper ballot into an optical scanner that tallies their vote, usually through the use of Optical Mark Recognition (OMR) technology.[18] This is the method which will be used in Georgia in its upcoming elections.[19] Although no vote casting system is perfect, there are minimal unique disadvantages to this system. There are less costs associated with this method compared to other e-voting methods and it automatically has the feature of VVPAT, since the voter handles the physical ballot before it is submitted into the optical scanner for tallying. When recounts are needed, these paper ballots can be used to audit the machines for any errors.

Internet Voting (I-voting)

Another technology sparsely used internationally is internet voting (i-voting). I-voting can take place either on designated public computer systems or on remote systems in an uncontrolled environment (i,e. a personal laptop in the comfort of your own home).[20] The preeminent example of i-voting is Estonia, where roughly half of voters voted using i-voting in the most recent elections.[21] There are unique and important disadvantages to internet voting that get to the core of what it means to have

[14] "Common Electronic Voting and Counting Technologies." November 25, 2013. https://www.ndi.org/e-voting-guide/common-electronic-voting-and-counting-technologies.

[15] *Ibid.*

[16] Goldsmith, Ben, and Holly Ruthrauff. Implementing and Overseeing Electronic Voting and Counting Technologies. International Foundation for Electoral Systems and National Democratic Institute for International Affairs, 2013. https://www.ndi.org/implementing-and-overseeing-e-voting-counting-technologies.

[17] *Ibid*.

[18] "Optical Scanning Systems —." Accessed March 4, 2024. https://aceproject.org/main/english/et/et72.htm.

[19] "Georgia's Central Election Commission Allocates ₾54 Million for Advanced Voting Technologies From Smartmatic," September 20, 2023. https://ipress.ge/en/news/politics/georgias-central-election-commission-allocates-gel54-million-for-advanced-voting-technologies-from-smartmatic.

[20] Ehin, Piret, Mihkel Solvak, Jan Willemson, and Priit Vinkel. "Internet Voting in Estonia 2005–2019: Evidence from Eleven Elections." *Government Information Quarterly* 39, no. 4 (October 2022): 101718. https://doi.org/10.1016/j.giq.2022.101718.

[21] "How Did Estonia Carry out the World's First Mostly Online National Elections – e-Estonia." Accessed February 16, 2024. https://e-estonia.com/how-did-estonia-carry-out-the-worlds-first-mostly-online-national-elections/.

a secure, fair, and trustworthy election. Regardless, Estonia's unique cultural and historical relationship to technology has enabled them to develop a system which is mostly trusted by the electorate.[22] The Estonian example is useful in its uniqueness, necessitating the consideration of context in the development of a trusted election process.

TECHNOLOGY USED IN VOTER REGISTRATION AND IDENTIFICATION

Before casting a ballot, voters are often required to identify themselves for the purposes of ensuring their eligibility, security, and the prevention of voter fraud. During this stage of the voting process, biometric identification has been increasing in use over the past twenty years, but it is still used by less than a third of countries at polling stations.[23] Biometric identification can take multiple forms, but the most commonly used are fingerprint recognition systems and facial recognition systems.[24] The latter, to be used in the Republic of Georgia this fall, takes the form of a biometric ID card, which is scanned at the polling site to validate the voter's identity.[25] This ID card has a photograph of the individual's face on it, which is also checked by an election official at the polling station. The scanning of the card in the electronic identification device, checks the voter's eligibility by cross-referencing their card's information with an electronic voter register. The voter's identity is verified by the election official through biometric identification and the voter's eligibility is verified by the swiping of the ID in the electronic identification device.

This system of checking voter eligibility is more efficient, and less prone to error, than requiring election officials to verify eligibility through the less sophisticated process of manually searching through a register by entering the voter's identifiable information. As with all stages of the election process, voter registration and identification has trade-offs, particularly between election security and inclusiveness. For example, arduous identification processes could lead those who are eligible to vote, but lack the required documentation, to stay home. Transversely, if identification processes are not secure the possibility for voter fraud increases. These apparent trade-offs will be explored further in the following sections.

POLITICAL ENVIRONMENT

The political environment is a decisive factor in the pursuit and implementation of new election technologies. Political will and political consensus are two major concerns associated with the pursuit of electronic technologies in elections. The former is most necessary for the development of new digital technologies and the decision to implement them in elections, while the latter focuses on inter-party cooperation for the sake of public trust in elections.

[22] Ehin, Piret, Mihkel Solvak, Jan Willemson, and Priit Vinkel. "Internet Voting in Estonia 2005–2019: Evidence from Eleven Elections." *Government Information Quarterly* 39, no. 4 (October 2022): 101718. https://doi.org/10.1016/j.giq.2022.101718.

[23] "Database Result (Question Only) | International IDEA." Accessed February 16, 2024. https://www.idea.int/data-tools/data/question?question_id=9345&database_theme=327.

[24] Wolf, Peter. "Introducing Biometric Technology in Elections." International IDEA, June 20, 2017. https://www.idea.int/publications/catalogue/introducing-biometric-technology-elections.

[25] Perez, Gustavo. "Modernization of Latest Election in Georgia Proves Successful." Smartmatic.com, May 1, 2023. https://www.smartmatic.com/media/modernization-of-latest-election-in-georgia-proves-successful/.

Germany's historical experience with e-elections is a useful illustration of the impact of a lack of political will on pursuing new election technology. Germany once used electronic voting machines, but since the Constitutional Court ruled against their use in 2009 the country has returned to using paper ballots and hand-counting.[26] The court's ruling stopped the investigation of electronic election technologies in its tracks due to the cumbersome challenge of making sure that these systems are sufficiently transparent under German law.[27] On top of the legal challenges, there is a general lack of political will in Germany to invest in e-election technology, regardless of their advantages.

German MP Höferlin (FDP), according to an interview by Fitzpatrick and Jost, was skeptical about introducing e-voting back into Germany.[28] He highlighted that the current German electoral process was well-trusted and pointed out that Germany had a broader acceptance of electoral outcomes than other Western democracies.[29] The article goes on to say, "MP Höferlin's (FDP) fear is that a complex and technologically sophisticated e-voting process will provoke a decrease in public trust in the election outcome."[30] The cautious government official serves as a useful illustration. His argument supports keeping things as they are, as long as they are working well. His argument against the adoption of e-voting, has little to do with the concerns around the technology itself, but rather is focused on the fragility of voter trust in the system. Ultimately, this perspective exemplifies the idea that if the current voting system is trusted, it should be preserved. This instinct to preserve a trusted election process can be a strong barrier for the adoption of e-voting technology, creating a lack of political will in certain contexts.

Inter-party acceptance of new election technologies is an important factor in both passing legislation to invest in new election technologies and making sure that one party will not attempt to undermine public trust in the electoral system.[31] For example, in the United States, public trust in the validity of election results is largely dependent on party affiliation. According to a 2023 Associated Press-NORC Center for Public Affairs Research poll, "22% of Republicans have high confidence that votes in the upcoming [2024] presidential election will be counted accurately compared to 71% of Democrats."[32] This disparity between the parties is largely due to partisan politics, which have politicized election technologies. Former President of the US, Donald Trump, and his allies pursued an aggressive disinformation campaign after the 2020 election, which included accusations of miscounts by voting machines, wide-spread voter fraud, and ballot stuffing in mailboxes.[33] Ultimately, these accusations have been discredited, but public perception remains divided. In fact, Dominion Voting Systems, whose machines were used in the 2020 elections, was repeatedly targeted Republican-oriented news broadcaster Fox News, whose pundits disingenuously claimed its machines were

[26] Library of Congress, Washington, D.C. 20540 USA. "Germany: Constitutional Court Decision on Electronic Voting." Web page. Accessed February 28, 2024. https://www.loc.gov/item/global-legal-monitor/2009-03-25/germany-constitutional-court-decision-on-electronic-voting/.

[27] "The Constitutionality of Electronic Voting in Germany." Text, November 25, 2013. https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany.

[28] Fitzpatrick, Jasmin, and Paula Jöst. "'The High Mass of Democracy' —Why Germany Remains Aloof to the Idea of Electronic Voting." Frontiers in Political Science 4 (July 13, 2022): 876476. https://doi.org/10.3389/fpos.2022.876476.

[29] *Ibid.*

[30] Fitzpatrick, Jasmin, and Paula Jöst. "'The High Mass of Democracy' —Why Germany Remains Aloof to the Idea of Electronic Voting." Frontiers in Political Science 4 (July 13, 2022): 876476. https://doi.org/10.3389/fpos.2022.876476.

[31] AP News. "GOP Confidence in 2024 Vote Count Low after Years of False Election Claims, AP-NORC Poll Shows," July 11, 2023. https://apnews.com/article/2024-election-poll-voting-machines-confidence-trust-8efb007d94c2b37a510f9d866e3c6031.

[32] *Ibid.*

[33] AP News. "EXPLAINER: How Trump Ignored Advisers, Spread Election Lies," December 21, 2022. https://apnews.com/article/capitol-riot-trump-election-lies-explainer-816a43ed964e6d35f03b0930e6e56c82.

unreliable.[34] Donald Trump also accused Dominion's machine of miscounting votes in Michigan.[35] Ultimately, Dominion voting systems sued Fox News for defamation, and the case was settled between the two parties. Fox News agreed to pay Dominion $787 million and the court found that Fox News circulated false statements about Dominion voting systems.[36] Regardless of the validity of these accusations, the politically motivated targeting of electronic election technologies has eroded public trust in the US election process.

Another important aspect of the political environment includes building political consensus on the implementation of new electoral systems. According to Ben Goldsmith and Holly Ruthraud, "If there is political consensus behind the decision to adopt electronic technologies, the potential for successful implementation is much higher."[37] One effective way to build political consensus is to involve political parties in the process of adopting the new technologies, as this allows them to have a stake in the success of the new technologies to be implemented.

Malta's recent experience in adopting electronic technologies for vote counting provides a positive example of an EMB engaging political parties in order to build consensus. In the 2019 EU parliamentary elections, Malta introduced a new electronic ballot counting system, which was subsequently used in Malta's national elections in 2022.[38] According to a study published by the European Commission, "The political parties had been involved in the entire procurement and implementation process of the system."[39] The procurement process started 18 months before the EU parliamentary elections in 2019, and political parties were able to test the technology against their own vote counting softwares. By including the major political parties in all aspects of the implementation process, the EMB was enabled to build an environment of political consensus. Regarding Malta's 2022 Parliamentary elections, the ODHIR's Needs Assessment Mission Report found that there were no concerns about the electronic counting system and cited overall trust in the system as a primary reason.[40] The e-counting system also provided its expected benefit of decreasing the amount of time needed to tabulate results.[41] Ensuring that political parties have a stake in the success of a new technology helps to build broader political support and disincentivize the politicization of electronic election technologies.

[34] "Fox Stars Privately Expressed Disbelief About Trump's Election Fraud Claims - The New York Times." Accessed March 4, 2024. https://www.nytimes.com/2023/02/16/business/media/fox-dominion-lawsuit.html.

[35] AP News. "EXPLAINER: How Trump Ignored Advisers, Spread Election Lies," December 21, 2022. https://apnews.com/article/capitol-riot-trump-election-lies-explainer-816a43ed964e6d35f03b0930e6e56c82.

[36] "Fox, Dominion Reach $787.5M Settlement over False Election Claims | AP News." Accessed February 28, 2024. https://apnews.com/article/fox-news-dominion-lawsuit-trial-trump-2020-0ac71f75acfacc52ea80b3e747fb0afe.
Folkenflik, David. "Judge Rules Fox Hosts' Claims about Dominion Were False, Says Trial Can Proceed." NPR, March 31, 2023, sec. Media. https://www.npr.org/2023/03/31/1167526374/judge-rules-fox-hosts-claims-about-dominion-were-false-says-trial-can-proceed.

[37] Goldsmith, Ben, and Holly Ruthrauff. Implementing and Overseeing Electronic Voting and Counting Technologies. International Foundation for Electoral Systems and National Democratic Institute for International Affairs, 2013. https://www.ndi.org/implementing-and-overseeing-e-voting-counting-technologies.

[38] ORLAND, KEVIN SCHEMBRI. "Maltese Vote in General Election with Some Firsts for Nation." AP News, March 26, 2022. https://apnews.com/article/europe-elections-voting-general-elections-malta-4e3b0cc428e69f8803f347ca8bcdb4d9.

[39] TRASYS International. "Annex III: Explored Use Cases on the Use of Technologies in the Electoral Context ('Explored Use Cases')." Study on the Impact of New Technologies on Free and Fair Elections. European Commission, March 2021.

[40] "Malta, Parliamentary Elections, 26 March 2022: Needs Assessment Mission Report." Organization for Security and Co-operation in Europe, March 10, 2022. https://www.osce.org/files/f/documents/4/8/513907.pdf.

[41] "Malta, Early Parliamentary Elections, 26 March 2022: Final Report." Organization for Security and Co-operation in Europe, July 14, 2022. https://www.osce.org/odihr/elections/malta/522712.

PUBLIC TRUST

Trust is the signal component of a successful election system. A distrusted election system is an unsuccessful one, regardless of whether or not the distrust is merited. Put another way, "A voting system is only as good as the public believes it to be."[42] Public trust is context dependent and concerns should be addressed in accordance with that context. Reasons for distrust often include historical experience, lack of familiarity, perceptions of corruption, and lack of security in aspects of the voting process.

Voter trust requires a belief in the integrity of all aspects of the election system, from proper identification to the proper dissemination of election results, and properly conducted audits afterwards.[43] There are many concerns that can erode trust in an election system, including the perception that votes are improperly counted, that ballots are not secret, and that there is wide-spread voter fraud. All of these factors can lead to low voter turnout and illegitimate election results.

The secrecy of the ballot is an integral safeguard against election fraud and is viewed as, "an essential characteristic of legitimate democracies."[44]A broad societal belief that ballots cast cannot be tied back to an individual better enables citizens to vote in their own interest. The secrecy of the ballot helps to remove the specter of intimidation and coercion related to voting against a particular party. In the aftermath of elections, it can help protect the voter against retribution for voting against a particular party, since there is a lack of any evidence as to who voted for whom.

The secret ballot also diminishes the incentives for vote-buying due to principal-agent problems.[45] In other words, when the vote-buyer cannot ensure that the voter-seller will hold up their end of the deal, the likelihood for vote-buying in general decreases.[46] Transversely, in situations where parties can monitor voter behavior, the likelihood for vote-buying increases.[47]

This does not mean that more informal contracts cannot be arranged to buy and sell votes. For example, vote buying can occur without an actionable contract in certain cultural contexts where the moral value of "one's word" can be relatively binding.[48] Also, there is the question of negative voting buying, where prospective voters are paid to "stay home" in order to prevent votes in favor of a competing party.[49] This problem cannot be solved through the secret ballot itself, since the negative vote buying contract is based on the voter's decision whether to show up at the polls, rather than the voter's choice at the poll.

The secrecy of the ballot is a key consideration of an electronic election systems design. An electronic election system should provide for ballot secrecy by divorcing the voter identification process from

[42] Wolf, Peter, Rushdi Nackerdien, and Domenico Tuccinardi. "Introducing Electronic Voting: Essential Considerations." Policy Paper. International IDEA, December 2011. 16. https://www.idea.int/publications/catalogue/introducing-electronic-voting-essential-considerations.

[43] "Pillars of Trust in Elections | International IDEA." Accessed March 4, 2024. https://www.idea.int/news/pillars-trust-elections.

[44] Dowling, Conor M., David Doherty, Seth J. Hill, Alan S. Gerber, and Gregory A. Huber. "The Voting Experience and Beliefs about Ballot Secrecy." Edited by Gregg R. Murray. *PLOS ONE* 14, no. 1 (January 7, 2019): e0209765. https://doi.org/10.1371/journal.pone.0209765.

[45] Lehoucq, Fabrice. "When Do Parties Buy Votes? Theoretical and Empirical Perspectives on Electoral Corruption." *Massachusetts Institute of Technology*, September 1, 2002, 26–27.

[46] *Ibid.*

[47] *Ibid.*

[48] The Carter Center. "Postelection Statement on Guatemala Elections, Dec. 19, 2003." Accessed March 4, 2024. https://www.cartercenter.org/news/documents/doc1567.html.

[49] Morgan, John, and Felix Várdy. "Negative Vote Buying and the Secret Ballot." Journal of Law, Economics, & Organization 28, no. 4 (2012): 818–49.

the submission of the ballot.[50] This can be accomplished by excluding any voter information from the ballot itself. According to the CoE, "The e-voting process, in particular the counting stage, shall be organized in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous."[51]

Yet, in the case of i-voting, it currently can not be ensured that votes are indeed anonymous due to the technical security problems associated with tracing evidence via the internet. This is a key reason why i-voting is uncommon globally. That said, Estonia's i-voting system provides an interesting look at how trade-offs are made in the construction of a trusted electronic election system. In Estonia, voters can either cast their ballot remotely, or, in-person on election day.[52] In order to justify the system, according to research from the National Democratic Institute (NDI), "Estonia has argued that the principle of secrecy entails an obligation to provide the opportunity for a secret vote, but that voters are free to choose less secret voting options if they desire."[53] In this case, "less secret voting options" refers to remote e-voting (i-voting).

Despite serious concerns amongst experts related to security and secret suffrage, the Estonian electorate seems to be satisfied with their election system. According to survey data, a large majority of Estonians trust their election process.[54] Yet, this has to be seen in context. Estonia has a unique historical experience in the technology field. The private and public sectors invested heavily in technology in the 1990s and since then the e-government model has grown to touch most aspects of citizens' lives.[55] Voters have become deeply familiar with all aspects of the technology, according to Slovak, Willmenson, and Vinkel, "This digital infrastructure is used daily for hundreds of thousands of interactions across all levels of the Estonian state, the private sector and society, including in banking, taxation, health, and education".[56] The Estonian electorate has the unique experience of being immersed in digital governance, where trust is facilitated through familiarity and experiences in daily life. The key takeaway from the Estonian example is that trust is built over time and, with each passing election, the electorate will continue to have more confidence in the technology as long as it performs satisfactorily.[57] With its long list of security concerns brushed aside, Estonia shows that a voting system can build trust through familiarity.

[50] "Guidelines on the Implementation of the Provisions of Recommendation CM/Rec(2017)5 on Standards for e-Voting." Council of Europe, June 14, 2017. https://rm.coe.int/1680726c0b.

[51] "Recommendation CM/Rec(2017)51 of the Committee of Ministers to Member States on Standards for e-Voting." Council of Europe, June 14, 2017. https://rm.coe.int/0900001680726f6f.

[52] Ehin, Piret, Mihkel Solvak, Jan Willemson, and Priit Vinkel. "Internet Voting in Estonia 2005–2019: Evidence from Eleven Elections." Government Information Quarterly 39, no. 4 (October 2022): 101718. https://doi.org/10.1016/j.giq.2022.101718.

[53] "Internet Voting." Text, November 25, 2013. https://www.ndi.org/e-voting-guide/internet-voting.

[54] Ehin, Piret, Mihkel Solvak, Jan Willemson, and Priit Vinkel. "Internet Voting in Estonia 2005–2019: Evidence from Eleven Elections." Government Information Quarterly 39, no. 4 (October 2022): 101718. https://doi.org/10.1016/j.giq.2022.101718.

[55] Vassil, Kristjan. "Estonian E-Government Ecosystem: Foundation, Applications, Outcomes." Background Paper. World Development Report. World Bank, n.d. https://thedocs.worldbank.org/en/doc/165711456838073531-0050022016/original/WDR16BPEstonianeGovecosystemVassil.pdf.

[56] Ehin, Piret, Mihkel Solvak, Jan Willemson, and Priit Vinkel. "Internet Voting in Estonia 2005–2019: Evidence from Eleven Elections." Government Information Quarterly 39, no. 4 (October 2022): 101718. https://doi.org/10.1016/j.giq.2022.101718.

[57] *Ibid*.

SECURITY

The security of electronic voting systems is a key component of building public trust as well as mitigating the risks of outside interference in elections. E-election system security is inherently less transparent than traditional vote casting and counting methods because of its technological sophistication.[58] This lack of transparency allows more opportunity for public skepticism, which can be overcome through effective communication by the EMB about the security mechanisms in place which ensure that the system is trustworthy.[59]

These security mechanisms include the inspection of the source code of any electronic machines by internal and external stakeholders, controlling access to the physical machines, and the proper transference of data captured by those machines.[60] Through the implementation of these mechanisms, EMBs further assure voters that the system's software is secure, that ballots are correctly cast and secret, and that it is unlikely that bad actors can broadly impact election results throughout the election process.

When there are flaws in the security and reliability of voting machines public pressure may ultimately result in the removal of electronic technologies from elections. For instance, in the Netherlands, after 40 years of using electronic technologies in elections, a civil society movement helped lead to the demise of electronic voting in the country.[61] In 2006, a group of computer experts from a pressure group called "We Don't Trust Voting Computers" exposed security flaws in the DRE machines to be used in the fall 2006 elections.[62] These security flaws included the relative ease with which software could be replaced by changing memory cards in the voting machines, as well as the ability to "eavesdrop" on the machines through what is known in cybersecurity as a TEMPEST attack, which, if replicated by a bad actor, could compromise ballot secrecy by allowing for remote recording of the information emanated as radiation from voting machines.[63] The government responded by implementing updated security features in the machines based on the pressure groups findings for the 2006 elections, but these updates didn't alleviate public concern.[64] Ultimately, the Dutch Government returned to paper ballots and manual counting in 2008 due to the security flaws exposed by the pressure group.[65] The example of the Netherlands shows the risk of not effectively engaging

[58] Goldsmith, Ben, and Holly Ruthrauff. Implementing and Overseeing Electronic Voting and Counting Technologies. International Foundation for Electoral Systems and National Democratic Institute for International Affairs, 2013. https://www.ndi.org/implementing-and-overseeing-e-voting-counting-technologies.

[59] Staak, S. van der, P. Wolf, and I. I. D. E. Assistance. Cybersecurity in Elections: Models of Interagency Collaboration. International IDEA, 2019. https://books.google.ge/books?id=AxYBEAAAQBAJ.

[60] "The State and Local Election Cybersecurity Playbook." Belfer Center for Science and International Affairs, Harvard Kennedy School. Accessed February 26, 2024. https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook.

[61] Jacobs, Bart, and Wolter Pieters. "Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment." In Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures, edited by Alessandro Aldini, Gilles Barthe, and Roberto Gorrieri, 121–44. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. https://doi.org/10.1007/978-3-642-03829-7_4.

[62] Loeber, Leontine. "E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years." Edited by Robert; Grimm Krimmer Rüdiger. Electronic Voting 2008 (EVOTE08). 3rd International Conference on Electronic Voting 2008, Co-Organized by Council of Europe, Gesellschaft Für Informatik and EVoting.CC, 2008. https://dl.gi.de/handle/20.500.12116/29188,.

[63] Aydin, Hakan. "TEMPEST Attacks and Cybersecurity." International Journal of Engineering 5 (2019): 100–104.

[64] Jacobs, Bart, and Wolter Pieters. "Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment." In Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures, edited by Alessandro Aldini, Gilles Barthe, and Roberto Gorrieri, 121–44. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. https://doi.org/10.1007/978-3-642-03829-7_4.

[65] Jacobs, Bart, and Wolter Pieters. "Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment." In Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures, edited by Alessandro

with all stakeholders in building secure electronic election systems. When implementing e-elections it is necessary to properly engage experts, proactively communicate with the public about security risks, and maintain an effective election security strategy. This helps to avoid a lack of buy-in from a particular group, which can ultimately discredit an electoral system in the eyes of the public.

Another key consideration for EMBs is to make sure that electronic voting machines are not connected to the internet, and to effectively communicate that to the public. Electronic voting equipment should not be connected to any inter-connected network. A leading provider of voting machines, Smartmatic, clarifies that their machines, as a rule, are never connected to the internet during voting, and that they are isolated throughout the process, or in other words, they are not connected to each other.[66] Connecting electronic voting machines to the internet is a security risk because it opens up the possibility of attack through internet-based cyberattacks.[67] Due to high-profile cases of institutions being hacked via the internet, there is a relatively common perception that anything connected to the internet is not secure.[68] On top of that, people around the world often see election data as targets for cyberattacks.[69] For both the public perception of security, and the deep security concerns associated with internet-connected electronic voting machines themselves, EMBs must ensure that these machines are protected from internet-based cyberattacks.

Electronic voter registration databases are also potential targets for cyberattacks and steps must be taken to ensure their security. A recent example of the vulnerability of these systems comes from the 2016 US elections, where the Russian state intelligence agency (GRU) gained access to multiple US voter-registration databases.[70] Although no voters' records were altered or deleted, this breach shows the vulnerability of interconnected systems.[71] EMBs need an effective security strategy for all aspects of the voting system, not just the voting machines themselves.

INCLUSIVENESS

Adapting to new technologies can be difficult. When implementing new technologies into an election process it is important to consider the voter's experience. According to an analysis of voter turnout in Georgia in the United States in 2002, the introduction of new voting machines led to a decline in turnout amongst the elderly population.[72] This may have been due to a discomfort with using new

Aldini, Gilles Barthe, and Roberto Gorrieri, 121–44. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. https://doi.org/10.1007/978-3-642-03829-7_4.

[66] "Smartmatic Cybersecurity: Frequently Asked Questions." Smartmatic, May 2022. https://www.smartmatic.com/wp-content/uploads/2022/11/FAQ_Cybersecurity_ENG_May31_2022.pdf.

[67] "The State and Local Election Cybersecurity Playbook." Belfer Center for Science and International Affairs, Harvard Kennedy School. Accessed February 26, 2024. https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook.

[68] Anderson, Lee Rainie and Janna. "Theme 6: Trust Will Diminish Because the Internet Is Not Secure and Powerful Forces Threaten Individuals' Rights." Pew Research Center: Internet, Science & Tech (blog), August 10, 2017. https://www.pewresearch.org/internet/2017/08/10/theme-6-trust-will-diminish-because-the-internet-is-not-secure-and-powerful-forces-threaten-individuals-rights/.

[69] Fetterolf, Jacob Poushter and Janell. "International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security." Pew Research Center's Global Attitudes Project (blog), January 9, 2019. https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/.

[70] Chicago Sun-Times. "Mueller Report Confirms Russians 'compromised' Illinois State Board of Elections," April 18, 2019. https://chicago.suntimes.com/news/2019/4/18/18619441/mueller-report-confirms-russians-compromised-illinois-state-board-of-elections.

[71] Zetter, Kim. "How Close Did Russia Really Come to Hacking the 2016 Election?" POLITICO, December 26, 2019. https://www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171.

[72] Roseman, Gary H., and E. Frank Stephenson. "The Effect of Voting Technology on Voter Turnout: Do Computers Scare the Elderly?" Public Choice 123, no. 1/2 (2005): 39–47.

technology or a fear that they would not understand how to use it.[73] The study goes on to conclude that there is not any reason to believe that a decrease in turnout would persist over time.[74] For example, after an election older voters may hear how easy the technology was to use from others in their social circles and feel more comfortable voting in the next election.[75] This temporary reduction in voter turnout may result from the barriers elderly people face and their relative discomfort in adapting to new technologies.[76]

In order to make sure that certain groups are not discouraged from participating in an election, it is important to create far-reaching informational and educational campaigns that are targeted for their intended audience. For the example of elderly voters, it is important to create a familiarity with the new voting technology and processes, so that come election day, elderly voters will be confident in their ability to smoothly cast their votes. This process should also be replicated for other groups which may face unique barriers to voting, including voters with disabilities, voters who use a foreign language, and etc.

Another group of voters that can be difficult to reach are those who live in rural areas. When polling stations are few and far between and citizens have less access to information they are less likely to vote. In an interview, Nineth Montenegro Cottón, a member of the Congress for Alianza Nueva Nación (ANN) and a member of the Commission for Electoral Issues in Guatemala, summarized key considerations associated with rural voter turnout well, saying, "More permanent information campaigns are necessary, preferably bilingual or multilingual in order to include the various languages of the Mayan culture… The enrollment and polling stations need to be closer and made more accessible to the rural population, since they now only exist in the administrative centers of each region."[77] The key takeaways from Montenegro Cottón's quote are that information should be made available to citizens in a way they understand and that voting stations should be geographically accessible.

COST

An election system is not feasible if it is financially unsustainable. In some emerging countries the up-front costs attached to implementing a new e-election system would mean a misallocation of resources.[78] On top of that, it is unclear whether the use of electronic voting machines results in cost savings over time.[79] This means that a country's financial situation should inform its decision to adopt electronic technologies for use in elections. Yet, in some cases cost savings have occurred.

According to an analysis of India's introduction of e-elections, the transition to electronic voting machines resulted in cost saving because the Electoral Commision of India no longer had to print paper ballots.[80] Overall, there is a lack of consensus on the cost of conducting electronic elections,

[73] *Ibid.*

[74] *Ibid.*

[75] *Ibid.*

[76] Zhang, Mengxi. "Older People's Attitudes towards Emerging Technologies: A Systematic Literature Review." Public Understanding of Science 32, no. 8 (November 1, 2023): 948–68. https://doi.org/10.1177/09636625231171677.

[77] López Pintor, Rafael, and Maria Gratschew. "Voter Turnout Since 1945: A Global Report." International IDEA, 2002. https://www.idea.int/publications/catalogue/voter-turnout-1945-global-report.

[78] Russell, Martin, and Ionel Zamfir. "Digital Technology in Elections: Efficiency versus Credibility?" Briefing. European Parliamentary Research Service, September 2018. https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf.

[79] McCormack, Conny B. "Democracy Rebooted: The Future of Technology in Elections." Atlantic Council, 2016. https://www.atlanticcouncil.org/in-depth-research-reports/report/democracy-rebooted-the-future-of-technology-in-elections-report/.

[80] Debnath, Sisir, Mudit Kapoor, and Shamika Ravi. "The Impact of Electronic Voting Machines on Electoral Frauds, Democracy, and Development." SSRN Electronic Journal, 2017. https://doi.org/10.2139/ssrn.3041197.

which points toward the need to create a context specific cost-benefit analysis, where the price of implementing a new e-election system is compared against that of maintaining the current system.[81] Then, that analysis should be compared against the non-financial advantages and risks associated with e-elections. For instance, part of the objective in adopting electronic voting machines in India was to lower the cost of conducting elections.[82] Since cost-reduction was an objective for the implementation of new election technologies in India, that objective should be given weight.

Another example of cost-savings comes from an analysis of Estonia's i-voting system, which showed that i-voting is significantly less expensive than other voting channels within the country, also suggesting that i-voting could be the least expensive option in other electoral environments.[83] Yet, due to the security and secrecy of the ballot concerns previously mentioned, i-voting is not currently a suitable option for most countries. I-voting is still an emerging technology, and as more countries develop ways to effectively manage the technological issues surrounding security and secrecy, it may grow into a more popular method for conducting elections in the future.

CONCLUSION

The overriding concern in creating an effective election system is public trust. Without it, the electoral system is illegitimate. Public trust is built over time, through familiarity, and it is common for public perceptions of performance to lag behind the objective performance of the electoral systems themselves.[84] Therefore, the introduction of a new e-election system should be seen as a long term investment, which requires adequate commitment.[85] The other key considerations of political will and inclusiveness are contributing factors to building trust in the electoral process. Additionally, cost is a constraining factor in the implementation of new election technologies and it should be considered when weighing the benefits of new e-election technologies. All of these factors should be considered in their appropriate context. As shown with the examples of Germany, the Netherlands, the US, Estonia, and India, the unique historical, political, and cultural experiences of a country factor into the construction and implementation of election systems. The use of electronic voting systems is prevalent, but each system has its own particularities.

Communication with voters and external stakeholders is an important part of implementing an effective electoral system. Information campaigns should be as broad as possible in reach, yet targeted to the concerns of specific audiences, so that everyone is ultimately aware of any changes that will affect their participation in an election. External stakeholders should be engaged early and frequently during the process of adopting new e-election technologies for the purposes of identifying and resolving any deficiencies in the system and in order to secure a broad base of political support for the new system.

[81] "The Use of New Technologies in Electoral Processes." Workshop Report. International IDEA and RECEF, 2018.

[82] Debnath, Sisir, Mudit Kapoor, and Shamika Ravi. "The Impact of Electronic Voting Machines on Electoral Frauds, Democracy, and Development." SSRN Electronic Journal, 2017.

[83] Krimmer, Robert, David Duenas-Cid, and Iuliia Krivonosova. "New Methodology for Calculating Cost-Efficiency of Different Ways of Voting: Is Internet Voting Cheaper?" Public Money & Management 41, no. 1 (January 2, 2021): 17–26. https://doi.org/10.1080/09540962.2020.1732027.

[84] Nyhan, Brendan. "Communicating with Voters to Build Trust in the U.S. Election System." White Paper. Mapping Election Administration + Election Science. MIT Election Lab, October 2023. https://electionlab.mit.edu/research/projects/mapping-election-science/white-papers/voter-trust.

[85] Goldsmith, Ben, and Holly Ruthrauff. Implementing and Overseeing Electronic Voting and Counting Technologies. International Foundation for Electoral Systems and National Democratic Institute for International Affairs, 2013. https://www.ndi.org/implementing-and-overseeing-e-voting-counting-technologies. 231.

Ultimately, electronic voting systems, just like traditional paper-ballot and hand-counting systems, are imperfect. They are both vulnerable to fraud, interference, and error. Yet, electronic technologies have advantages in speed and accuracy.[86] Attached to these advantages are new security, transparency, public trust, cost, and usability considerations. If appropriate for the local context, EMBs, along with collaboration from a broad set of stakeholders, can effectively implement e-elections and even improve the quality of elections.

[86] Wolf, Peter, Rushdi Nackerdien, and Domenico Tuccinardi. "Introducing Electronic Voting: Essential Considerations." Policy Paper. International IDEA, December 2011. https://www.idea.int/publications/catalogue/introducing-electronic-voting-essential-considerations.