Trust Frameworks in Application to Technology in Elections: selected case studies

David Duenas-Cid[1], Leontine Loeber[2], Beata Martin-Rozumiłowicz[3], Ryan Macias[4]

Abstract: The prevalence of technology in elections has increased in recent decades, both in terms of voting systems as well as ancillary ones. At the same time, the issue of public confidence and trust has come to the fore as certain threat actors have sought to undermine electoral integrity through publicized attacks and disinformation campaigns against such technology. This paper examines the nexus between this public trust and the implementation of technology through an electoral cycle approach. It also presents a number of case studies at various points of democratic development and election management body type to examine how various trust variables impact implementation to either increase trust or distrust. This is done to better understand the directionality of these criteria through a methodologically driven approach, based on a uniquely developed trust model. It is hoped that this study will help experts to better understand how these variables impact the critical trust that underpins robust democratic institutions.

Keywords: Trust, Distrust, Election Technologies

1 Introduction

Trust in elections and the outcome of elections is being actively undermined in many countries in the world. Looking at the current trust deficit, the political aims this is being put to it is imperative that such issues need to be addressed explicitly if voter confidence is to be maintained. This is especially relevant in the field of technology in elections where undermining trust is becoming a global phenomenon and likely to spread to various election tech areas (voter reg., RMS, etc.). This makes it important to understand what factors lead to trust and which factors contribute to distrust. This paper approaches those factors combining academic literature and real case-based knowledge.

We also want to highlight the difference between trust in a system and the trustworthiness of the system. This distinction remains underexplored in the specific literature, and this paper aims to show its importance for the cases presented. In some instances, high-trust levels were posited in untrustworthy systems and, in others, the reverse can be seen. Trust and distrust can manifest in different forms during different stages of the electoral cycle. The erstwhile focus on the election day phase of casting, counting and tabulation of the

1 Kozminski University, Pub-Tech Research Center, 57/59 Jagiellońska, 03-301 Warszawa, Poland and University of New South Wales, School of Information Systems and Technology Management, NSW 2052, Sydney, Australia david.duenas.cid@pg.edu.pl
2 University of East Anglia, Research Park, Norwich NR4 7TJ, United Kingdom
3 Independent expert consultant
4 RSM Election Solutions, 1717 N Street NW STE 1, Washington, United States

doi:10.18420/e-vote-id2023_07

votes is a too narrow approach; for example, the spread of misinformation during boundary delimitation, voter registration, or the campaign phase can also lead to trust or distrust. Another important phase is post-electoral disputes and the judicial processes with regard to election complaints. Although this is meant to create trust, long procedures with difficult rulings, lack of technical knowledge on the part of justices, and focused disinformation campaigns can also easily lead to mistrust. Again, the paper aims to contribute to the existing knowledge by applying the theory about these stages on real cases.

2 Theoretical Framework and Methodology

In order to develop a comprehensive theoretical framework for the comprehension of trust and distrust in electoral technology, it is of utmost importance to identify its potential sources including aspects related to the technology itself but, also, to the organizational and societal environment surrounding the elections and their organization. Election technologies are inserted in a complex socio-technical environment with a significant number of stakeholders that can, potentially, influence the perception that citizens have of the system. The list includes elements and stakeholders related to the technology but also the institutional framework, with the rest of the citizens and even with geopolitical relations [Du22].

But the adequate approach to those elements needs to be accompanied with a theoretical framework depicting how the process of creation of trust and distrust can be understood. For that, three main elements are to be considered.

First of all, trust and distrust should be understood as related but different theoretical constructs to be assessed and evaluated independently of one another. It has been stated that trust and distrust provoke different reactions [TH00]; the absence of trust affects the willingness to take risks and increases the demand for protection [TK96], while distrust creates anxiety and insecurity [Go92]. To embed this distinction between trust and distrust into the research on electoral technology, we can refer to the existing work in other social contexts [LMB98; Lu17; Lu79; MRW12; Ro98; TL06] approaching both constructs as independent variables. Assuming this distinction opens the door to their coexistence in parallel and towards the same target [OLS97; PP96]. That can contribute to enlarging the existing scope in the research on electoral innovations, where approaching what makes citizens trust has been notably predominant in front of what they lead them to distrust. Also, this approach allows understanding citizens' trusting / distrusting decisions as complex processes where several inputs are considered, and positions are mutable depending on the moment and the situation. Also allows understanding that similar inputs might have different impacts on citizens.

Secondly, trust and trustworthiness should also be understood as different constructs. The latter has been defined as an antecedent to trust [To20], as an aspect that affects a trusting relation by referring to a property of the trustee. Trustworthiness, then, plays an important role in the creation of trust, but the relation between them is not necessary causal since trust

is influenced by several other factor. In the case of electoral management, and given the relevance of the topic, the list of potential elements influencing trust creation is long and covers a wide range of actors [Wa06].

The different elements highlighted raise immediately a question of methodological nature: *how can we conduct a comprehensive analysis of the use of electoral technology and its impact on the different types of trust?* Prior electoral research has already described the different parts of the electoral cycle being more or less detailed (see Electoral Cycle section below) and even modelling parts of the electoral process [KDK21b]. In this research we opt for using the electoral cycle to detect and compare the touchpoints between technology and trust occurring in the different stages of the electoral process, and to compare them between different cases. Using this scope adds an interesting feature to the existing research: focusing on the moments that transcend what happens on the election day and vote casting process and widening the scope to other uses of technology used in the electoral process.

This paper uses an inductive approach to the question how the use of electoral technology impacts trust and distrust. To shed light on this research question, the paper uses the acquired in-depth knowledge from the cases to reflect on the relationship between election technology and trust. The dependent variable that the paper looks at is the perceived level of trust in the countries. The cases that are used are Poland, Kenya, the Netherlands and the United States. These cases were chosen based on their different structure of their Electoral Management Body (EMB) [Wa06]. Here, it has to be taken into account that the actual independence might change when ICT is introduced in elections, due to the technical knowledge, and thus often the reliance on vendors that is required when using ICT [Ja19]

Kenya has an independent EMB, the Netherlands and the U.S. have a governmental structure and Poland has an EMB that is comprised of the judiciary. Next to that, the trust level in the countries in question is quite different. Whereas trust in the Netherlands has always been high, the same can't be said for Poland and Kenya. In the US, trust in elections has declined since 2000. The cases also differ in the amount of experience that EMBs have had with the organization of elections. The Netherlands and the U.S. are usually considered to be old democracies, since they have held elections for over 100 years. Poland is a younger democracy, being part of the third wave of democratization. Kenya is a developing democracy, with less experience. Furthermore, the case of the U.S. adds another dimension to the study due to its singularity, complexity, and interest.

2.1 Electoral Cycle

The introduction of technology in elections has increased considerably in recent decades, both in terms of voting systems, but also ancillary ones. Many countries have looked at applying technology to improve efficiency and reduce the costs of aspects like voter registration and identification, and results management systems. Others have moved beyond voting machines

in controlled environments (e.g., polling station DREs), to piloting electronic voting in uncontrolled environments (e.g., internet voting) for certain categories of voter.

International support (either bilateral or organizational) for such initiatives, especially in developing democracies have supported this space financially and programmatically. Initial iterations focused primarily on provision of hardware and software for such systems. However, there is now a greater understanding within the international community that procedural, legal and feasibility elements should also be key elements of international assistance. There is also a growing awareness that technology introduction and increased trust do not necessarily go hand-in-hand.

That said, there is still a lack of a cohesive, coordinated methodology that starts with a needs-based approach. It is also apparent that any introduction of technology in elections needs to be buttressed through a more cohesive electoral cycle approach (see figure 1). This would place the introduction of electoral technologies as the locus of better electoral integrity, rather than as a potentially complicating problem in many recent cases of democratic backsliding. It also makes clear that electoral stakeholders need to be the drivers of 'follow-up processes' in between elections in order for reforms to have maximal impact. This should be the desired outcome, rather than the current *status quo* of approaching elections six months to one year out and not having the time, resources or knowledge to implement truly impactful change.

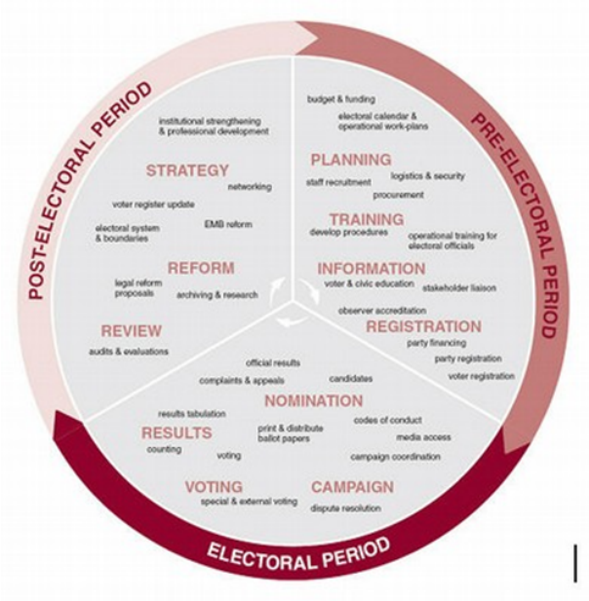

Abb. 1: The Electoral Cycle (developed by the European Commission, IDEA, and UNDP) [AC]

Various crises of public trust have also led to a better understanding that the introduction of technology in elections and increase in trust are not colinear processes. Rather, the

interaction between different trust variables at different stages of the electoral cycle needs to be better understood and documented. Without this fundamental understanding, it is possible that greater damage than good will result in building trust in democratic institutions. The cases studies are an addition to the existing literature by showing this interaction.

Very often, technology introduction is partially or wholly disconnected from this fundamental electoral cycle approach. Often, electoral stakeholders (be they government actors, political parties, or electoral commissions) have their own prioritization of programming that should be undertaken. Assistance providers are often driven by institutional impetuses, by aid agency priorities, and, to a certain level, by inertia in implementing activities done successfully in other countries, or at other time periods. Thus, very often, the disconnect happens by institutional ossification rather than by design. In constrast, the overarching approach should be of how technology can contribute to the democratic electoral process by increasing trust, rather than compromising it or reducing public trust. It is this question which forms the next part of our analysis.

3 Case Studies

For each of the cases, the paper will map out trust / distrust factors during the electoral cycle over a period of time that included decision-making, implementation, and post-electoral disputes. We will then look at causal variables that increase trust or distrust, specifically aspects related to voter trust or distrust in contrast to that of decision-makers. The relevant factors stem from the theoretical framework. The paper will rely on secondary data and research already published on the selected cases.

3.1 THE UNITED STATES OF AMERICA

In America, elections are conducted under the rules set forth by the respective legislature and certified by the Chief Election Official in each of the 50 States [BP21]. This means that the technology to conduct the elections also varies between states. The disperse structure can be both a security benefit, in that there is no single point of failure, but it can also lead to distrust in the process since voters are unfamiliar with the processes and technologies used in other jurisdictions across the country. Threat actors have exploited the disparate set of processes and technologies to call into question the election integrity amongst election jurisdictions.

It has been suggested that trust in American institutions, generally, is declining [St22b], amongst the reasons, the ongoing process since 2016 in which threat actors are attacking election technologies to try and decrease trust in democratic institutions. A Massachusetts Institute of Technology (MIT) report [MI21] states that the Bush v. Gore election of 2000 and the controversy around the recount introduced the term “voter confidence” into the

American elections. Following the 2000 election, the Help America Vote Act (HAVA) of 2002 [Se02] banned the use of pre-scored punch card voting technology and provided for the expansion of new voting technologies (NVT) across the country. The increased use of NVT in American elections has not gone without controversy. Many computer scientists and researchers exposed many of the security vulnerabilities that left opportunities for manipulation in election results via the NVT [Bo03; FHF06; Sc03]. This, along with many others, created opportunities for the American electorate, and potentially foreign adversaries, to spread theories that the NVT or the companies that developed the technologies had been manipulated or perpetuated fraud in the tabulation process.

While no manipulation of NVT software was or ever has been detected, over time the awareness of the vulnerabilities in the systems led to policy changes aiming to increase the security and resilience of both the NVT and the overall election process. As trust in NVT steadied, and at times increased, in 2016 the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) compromised the Illinois State Board of Elections (SBOE) computer network and was able to gain access and exfiltrate data of Illinois registered voters. Additionally, the GRU used spearphishing techniques to install malware on the network of an election technology company that develops software to manage voter lists [Mu16]. On January 6, 2017, the federal government designated elections as critical infrastructure. The designation allowed for election infrastructure to become more secure and resilient.

Trust in American election technology prior to 2016 had focused on NVT or more specifically the technology used to tabulate the votes. The GRU targeting electronic voter registration and verification systems (EVRVS) and companies developing software to maintain electronic voter lists, was used by threat actors to try to sow distrust in American elections by targeting all election technology, including ancillary ICT-election technology that is not used in determining the outcome of elections.

Leading into the 2020 election, a group of domestic threat actors used data obtained from election jurisdictions to purport that there had been manipulation, fraud, or other election integrity concerns through the exploitation of vulnerabilities in election technologies and the companies that develop those election technologies [Br21]. Additionally, according to the U.S. DOJ, Iranian nationals attempted to compromise, approximately 11 state voter websites, including state voter registration websites and state voter information websites, including gaining access to information on some voters in a state [De21] and that they gained access to a results management system (RMS).

As previously discussed ever since the designation of critical infrastructure American elections tried to become more resilient. There was an increase in the use of hand-marked paper ballots, and in the number of tabulation or outcome-based audits being conducted. As jurisdictions transitioned back to hand-marked paper ballots, especially postal voted ballots, there has been a need to adjudicate more ballots to determine the intent of the voter. Each of these situations has created complexities for the EMBs, so the NVT companies

have developed software aiming to make the process more efficient, secure, and transparent. But threat actors took the opportunity to exploit this new functionality stating that the NVT software allowed an EMB to change votes and manipulate the results. These changes are completely legal, appropriate, and required by law or policy. Further, EMBs have always been allowed, and required, to make such changes through a manual or 'remake' process. However, the automatization of the process and its integration into the NVT software as used as a means to decrease trust in the NVT. Specifically, the use of a Dominion Voting System application, Adjudication, was at the forefront of this attack and was exploited by threat actors. The claim that Dominion changed votes through the Adjudication software was amplified by many media outlets. That was one of the claims ultimately led to multiple defamation lawsuits by Dominion against media outlets and television personalities. One of those lawsuits was the Fox News defamation case where Fox News paid Dominion the unprecedented amount of $787.5 million to settle the case [Ra20].

As a result, after the 2020 election some voters were convinced that the NVT had been manipulated and wanted answers. In a small number of jurisdictions, the courts, legislatures, government officials, or members of the public legally forced or threatened EMBs into having the NVT software copied or reviewed. Many, if not all, of those instances have resulted in unauthorized entities, including potentially threat actors, gaining access to the NVT software and data which has been and may still be used to sow discord and reduce trust in American elections [Bi21; Co23; Gr22b; St22a; WA21]. The repercussion of these reviews has been seen in two local EMBs where they have regressed from electronic tabulation to conducting a full hand count tally of all results [Pa22a; Pi23]; experts agree that a full hand count tally in American elections is a less secure and less accurate method of tabulating votes [Pa22a]. Other people have attempted to have a court force a local EMB to get rid of their NVT and conduct hand counts in future elections; each of these cases has been unsuccessful to date [Gr22a; Le22; Me22; PK22; US22].

Continuing on after the 2022 election and as recent as the past few months, threat actors continue to sow discord by building distrust in ancillary ICT-election technologies. The attacks on NVT, and other ICT-election technologies, such as EVRVS, electronic voter lists, RMS, etc., have not subsided. Recently, the attacks have expanded to systems adjacent to elections (i.e., not used in the conduct of the election process). Threat actors have publicly attacked systems as innocuous as intrusion detection systems [Pa22b], ballot printing technology [SE22], and systems that are used to clean voter registration databases in order to prevent voter fraud [CC23].

With attacks against election technology continuing and expanding into new technologies, it is assumed that the trust in election technologies would further decrease. The MIT Trust in Elections study [MI21], however, actually found the opposite. As it pertains to voter confidence in election technology specifically, the study states "Americans were more confident in the electoral machinery following the 2020 election than they were in 2016. The difference is they were more polarized. . . " Further, in two of the incidents mentioned, the voters have decided to recall the election officials who were trying to sow distrust in the

NVT; one has resulted in a successful recall of the election official the other is currently awaiting a recall election. In both these incidents voters said they trusted the NVT and elections processes in their jurisdiction and wanted to oust the elected officials who were trying to distrust the democratic institution. While the study and recalls show there is more confidence in the election machinery, the increased polarization is creating chaos and sowing discord in American and democratic institutions.

3.2 THE NETHERLANDS

The case of the Netherlands is an interesting one because this is a country which went from elections with a high amount of technology back to paper ballots, even though public trust in the technology was not an issue. However, the use of software to tabulate and determine the results has now become a topic of discussion, due to experts calling the security of that software into question. Overall, even though trust in the electoral process is still high, certain parties are using the rhetoric of possible election fraud, which could undermine this public trust.

The Netherlands introduced voting computers (DRE's) in the early 1960's and continued to use these until 2006. At that time, almost 95% of the voters cast their vote using technology. The Netherlands also experimented with internet voting for voters living abroad, using it in binding parliamentary elections in 2004 and 2006. In 2006 however, an NGO called we don't trust voting computers successfully challenged the certification of the voting computers, claiming that they were not meeting the standards of transparency, verifiability and voter secrecy. The main problem that the action group had with the machines in use was the fact that they were lacking a paper trail, making it impossible to check if the outcome of the election was indeed what the voters wanted. The issues this group raised eventually let to the withdrawal of the certification of the voting computers and a return to voting with paper ballots [Lo14; Lo16]. In 2008, internet voting was considered for nationwide elections for the waterboards, a form of decentralized governments. Because of the discussion on the voting computers, a more substantial technical analysis of the intended system was performed, showing several weaknesses. This led to the decision not to use the internet voting system anymore.

During the 2017 Dutch Parliamentary Election Study, voters were asked two questions with regard to the use of technology in the process of casting a vote in elections. First people were asked which voting method they would prefer. It turned out that a small majority at that time stated that they preferred to use paper ballots, in contrast with 2006 and 2010 [Lo11]. Next, people were asked which voting method they would consider the most reliable. Almost 2/3 of the respondents felt that voting by paper ballot is the most reliable voting method. Curiously, this means, compared to the results mentioned above about the preferred method, that even though people do not feel that voting by voting computer is the most reliable, some of them would still prefer this. This difference in appreciation between preferred and most reliable method is even greater when it comes to internet voting; 18.1% of the respondents

prefer this method, whereas only 6.2% feel this is the most trusted method. In these cases, convenience of the voting method seems to prevail over the question of trust [Lo18].

Another area in the electoral cycle where technology is used in the Netherlands is for the tabulation and calculation of the votes. Software for this purpose, called OSV, was developed in 2008 by the Electoral Council and first used during the elections for the European Parliament in 2009. During the election process, nearly all political parties and municipalities use the software, although this is not legally mandatory. The software is used in different phases of the electoral cycle, both in the nomination phase and in the tabulation phase. Political parties that want to run in the elections can use the software to register their candidates. Furthermore, the software is used for the vote tabulation and seat distribution. For this part of the process, it should be noted that OSV is not used in the polling stations themselves. Votes are cast on paper and are still counted manually. The results are then manually entered into the software to determine the results on the municipal level. This process is repeated at the district level by the principal electoral committees and eventually by the Electoral Council. At various moments during the process, results are printed on paper, are brought to the next level in person and manually re-entered into the system. Up until the 2017 election it was also standard procedure that a digital file of the results was transferred together with the paper print by using usb-sticks. Due to questions concerning the safety of that procedure, this was abandoned [CY18].

Just before the 2017 parliamentary elections, a news report stated that the software was not safe, that it could be hacked in a way that would make it possible to change the outcome of the results. In order to ensure the integrity of the final results, the Electoral Council has introduced two new checks, where random samples from the polling stations are compared to the results from the software, looking at the total number of votes, but also at the seat distribution for parties and candidates. This was first done during the municipal elections of 2022 and resulted in the finding that there had been no issues with the software [Ho22].

So, what has all this done with the trust in elections in the Netherlands? Compared to other countries, trust has always been high and this continued. During the 2021 elections, 79% of the voters that were involved in the Dutch Parliamentary Election Study stated that they felt that the elections were fair. Almost 10% found them not fair. Although this number is, as stated, low compared to other countries, it is almost twice as high as in 2017, when only 5% of Dutch voters stated that they lacked trust in the outcome of the elections. Voters that did not trust the outcome mentioned different reasons for their lack of trust. During these elections, mail voting was used on a bigger scale than in previous elections, due to Covid-19. Some people felt that this wasn't safe. Also, voters mentioned the counting process as a reason not to trust the outcome. Interestingly, some of these latter voters pointed towards the (perceived) problems in the United States with the counting as a reason not to trust this part of the process in the Dutch elections [SLM21].

The case of the Netherlands has some important aspects for questions on trust in technology used in elections. First, the fact that technology has been used on a large scale and for a

long time doesn't mean that the issue of the trustworthiness of the technology will not surface. Therefore, it is important to ensure that the EMBs using the technology are aware of (technological) developments that can lead to questions of trustworthiness. The second thing that should be considered is that voters can trust technology, even when it is not trustworthy. The final point is that trust will often depend on what is stated in the media about the technology. Even though the counting of the ballots is still done by hand in the Netherlands, based on some news reports, many voters thought that this was done by possible malfunctioning software. Also, media reports on similar events in other countries can play a role, as shown by the fact that some Dutch voters had less trust in Dutch elections, due to the events in the 2020 U.S. elections.

3.3 POLAND

Although Poland never used or considered any form of electronic or internet voting, it is possible to extract from events occurred in the recent years in the management of Polish elections that are relevant for the understanding of trust-related aspects and election reform and technology adoption in other parts of the electoral cycle beyond the election day, and in other moments besides the moment of casting the vote. In this description, we will pay attention to the failure of the IT systems in 2014 Elections and the failure in the introduction of all-postal elections in 2020.

Poland hosts four types of elections (Sejm/Parliament, Presidential (two-round), Local and European), featured by a low turnout (in average). This low average turnout [MK20] (Sejm - 49,50: Presidential - 58,15; Local - 45,14; European Parliament - 28,73 – average values) triggered the introduction of postal and proxy voting in Poland in 2011 [St20], raising questions about election fraud and vote buying. It was argued that postal voting may pose a risk of vote declassification that would lead to fraudulent elections [Mu20]. The election code proposed in 2011 allowed significant vote-value disparities, conflicting with the Polish constitution requirement of voters equality [PS17]. Some of these concerns came back to the public debate on the occasion of the failed implementation of all-postal elections in 2020 to overcome the problems derived from Covid [KDK21a]. A combination of legal, managerial and trust-related issues [MK21] forced to cancel and postpone the elections, adopting a different format combining paper and postal elections. Trust, in this context, was related to the managerial capacity of the electoral management bodies and the Polish postal service to provide the service requested within the correct time and cost frames [Ko22; Zb13].

The second example shedding light on the functioning of Polish elections relates to the problems occurred in the Local Elections of 2014, when the electoral results were communicated late, due to a problem in the IT systems. Once presented, the results diverged substantially from the exit polls, provoking an important controversy in the country regarding the acceptance of the results. Two factors also strengthened the discussion: the exit polls were very accurate in the previous years, and the number of invalid votes was significantly higher on this election [Śl15].

A report by Fundacja Batorego [Fl15] describes how the problem in the IT system for calculating the results escalated and end up with the resignation of the members of the National Electoral Commission, demonstrations, media exposition and political tension. The same report highlights the causes of the crisis including the IT system, but also a number of organizational (including the lack of a contingency plan, the lack of auditing or the poor time management of the tender) and systemic reasons (including the lack of reflection about the election process, the lack of renovation of the National Electoral Office or the lack of interaction between the Electoral Office and external experts). Technology, hence, appears as the trigger of distrust, but a number of other elements that could have served as firewalls to prevent distrust expansion were not in place or correctly managed, allowing the escalation of the problems, and risking the overall elections.

3.4 KENYA

The case of Kenya here is educative in terms of public trust and the introduction of technology in elections. This case study takes a deep dive into the introduction of technology in elections in Kenya and the key role of trust / distrust in this process. The case of Kenya is particularly telling since it has included technology in some parts of the electoral process since the recommendations of the Kriegler report following the 2007 post-election violence. The introduction of technology in elections, however, has also become a focus for polarization, within society and across the political class.

On the surface, one would expect that the introduction of technology in elections would improve public trust in the election process and to reduce polarization. Yet, in the Kenyan case, the opposite proved true. In the previous 2017 general elections, the losing Orange Democratic Movement (ODM), led by Raila Odinga challenged the electoral results and his opponent, Uhuru Kenyatta (Jubilee Party), before the Supreme Court, claiming that various levels of institutional infractions meant that the elections should be overturned and re-run. Technology played a key role in this call for annulment.

The landmark 2017 Supreme Court decision that overturned the results and called for new elections was very much part of this trust/distrust calculus. Technology and its inconsistencies were identified as one of the fields where there was so much lack of clarity that the court felt it was impossible for them to establish the results. Certain recommendations were made to improve the process prior to the 2022 general elections, yet many of these things did not take place and implementation was rushed.

Why was this? In the first place, the Kenyatta government that emanated from the 2017 re-held elections had declined international involvement and assistance for a variety of reasons; some historical, some personal, some ideological. Although this was essentially a government decision, it should have been made in a more open and transparent process. To the author's knowledge, this didn't take place and elite decision-making played a pre-eminent role. This also led to a lack of strategic focus on the part of Kenya's Independent Electoral

and Boundaries Commission (IEBC) in planning for the 2022 elections until a change of heart in 2021 allowed international assistance providers to design and implement programs that finally resulted in an IEBC strategic plan being adopted. That said, this was much delayed and many of the deadlines were compressed to what a proper electoral cycle approach would entail. Thus, the 'management' variable was also lacking at this crucial stage, contributing to distrust.

Within the technology sector and given the past debacle, a decision had been made to transition to a new technology provider to design and supply the Kenya Integrated Election Management System (KIEMS) system for these elections. This would normally entail extensive and inclusive consultations on specification, tender and procurement of the technology with proper societal oversight. What ended up taking place was perfunctory at best, with limited time for review and limited input from key electoral stakeholders. Again, the 'technical trustworthiness' variable was undermined as a result, again increasing distrust.

There was also the issue of limited capacity. Although electoral stakeholders had developed their technology capacity since the introduction of the Biometric Voter Registration System (BVR) in 2013, technical expertise was also quite limited in the time frames allocation. Thus, there was only a basic level discussion of what needs are expected from the systems and a dovetailing of the specifications that would lead to the tender on this inclusive basis. This contributed to the distrust in the 'technical trustworthiness' of the system prior to the 2022 elections.

Then, in the procurement, there were anomalies in the process and potentially more questions could have been asked by electoral stakeholders. As the 2022 EU EOM final report found, "the IEBC did not publish the evaluation either for this [KIEMS] or the additional election technology related public procurement processes, undermining transparency, and leaving room for speculation." [Un22] Again, the 'transparency' variable was key here.

Throughout the implementation process, information to electoral stakeholders was rather limited. Some public testing was held with political party involvement, but independent mandatory audits of the system that had been put in place resulted in only limited information about its findings, recommendations, and subsequent changes made. Importantly:

"While party agents and stakeholders were given the opportunity to observe the assembling of the KIEMS kits and the IEBC published information on the security and contingency measures implemented in the KIEMS kits, no equivalent information was provided on the KIEMS backend applications used by the Constituency Returning Officers (CRO) and the National Returning Officers (NRO) nor on the hosting infrastructure, limiting stakeholders' capacity to assess the election technology."[Ke22]

So, in many ways, proper transparency and accountability of this important part of the electoral process fell short of what international standards would demand. At the same time, stakeholders did little to demand the level of transparency and accountability that should be required. The issue then became a central bone of contention in the formal and

information challenges to the electoral results at various levels and the lack of involvement also potentially sparked a greater level of disinformation of developments in this area, likely due to a sense of disconnection and impotence to do anything at the late stage.

Lastly was the roll of vendors in this process. While many EMBs choose to outsource the implementation of technology in their elections to outside vendors, many also try to abrogate ultimate responsibility to them for any gaps or system failure. Unfortunately, according to latest international standards, this is not a valid approach and EMBs should be considered ultimately responsible for any implementation of technology in elections.[Eu17]

One element that did serve to increase trust in the elections was the establishment of an online web portal where the polling station level results protocols (Forms 34A) could be uploaded for public scrutiny. Although the development of this portal was much delayed and untransparent, its appearance just prior to the election meant that on election day and after, stakeholders could check individual results remotely, which serve to raise public trust to some extent.

Throughout such technological application in elections, electoral stakeholders should have been better informed, better equipped to input and critique systems at a technical level, and better empowered to hold state institutions to account for their specification, procurement and implementation. In the case of Kenya, more targeted and incisive oversight could have led to greater transparency and accountability and, ultimately, to less polarization and disinformation in an already high-stakes environment.

From the analysis, we can conclude that the key variables of 'technical trustworthiness', 'management of the electoral process', but especially the lack of openness and 'transparency' meant that key moments in the electoral cycle in which public trust could be built were missed. Instead, the variables came together to decrease, rather than increase trust in the electoral process, although the element of the web portal operated in the opposite direction.

4 Findings and Conclusion

This paper seeks to analyse the concept of trust in technology in elections. It examines trust and distrust as two concurrent and collinear processes and develops a methodological framework of key variables that may impact on trust and distrust. It examines these variables through an election cycle approach and across four cases studies of countries that vary by election management body (EMB) model and by level of democratisation. Through a deep dive into the specific conditions surrounding technology in elections in Kenya, the Netherlands, Poland and the U.S., it aims to show which of the variables were salient and at what stages of the electoral cycle.

Key findings that can be induced from the cases include that trust issues are not only important when new technology is introduced, but can also become a topic of controversy at a later date. We see this most clearly in the Netherlands and U.S. case studies, but also in

that of Kenya. We also find that trust and trustworthiness are not the same thing. Very often, technology systems can be designed to be trustworthy, yet still not enjoy trust. Conversely, as the early stages of the Netherlands and Kenya implementation show, there can also be trust without trustworthiness. In addition to that, the use of NVT along the electoral cycle adds new layers of complexity at different levels (e.g. technical, managerial or procedural) that, in consequence, may serve as trigger for distrust related narrations (see USA case).

Overall, the cases found that throughout technology introduction and application in elections, electoral stakeholders should have been better informed, better equipped to input and critique systems at a technical level, and better empowered to hold state institutions to account for their specification, procurement and implementation. Ultimately, such a more holistic approach could have led to less polarization and disinformation in an already polarised environments. From the analysis, we can also conclude that the key variables of 'technical trustworthiness', 'management of the electoral process', but especially the lack of openness and 'transparency' meant that key moments in the electoral cycle in which public trust could be built were missed in all four cases. Instead, the variables came together to decrease, rather than increase trust in the electoral process. Also, it is worth to note that the number of stakeholders linked to the active provision of trust and those potentially providing distrust is clearly unbalanced towards distrust providers. In some occasions (see the Polish and USA cases) even actors that should be interested in providing trust in the democratic systems (political parties) can actively introduce distrust in the system searching for short term spurious benefits and not necessarily being aware of the potential long-lasting impacts in the overall trust in the electoral system.

Further research should look at the finding from the cases that trust and distrust are long-term issues that warrant much more incisive examination. They exist not just around election day, but at all stages of the electoral cycle, which proves to be a useful model of examination.

5 Acknowledgements

The work of David Duenas-Cid has received funding from the Electrust (EU H2020 MSCA programme, grant agreement no. 101038055) and Dynamika (braku) zaufania w kreowaniu systemów głosowania internetowego (Narodowe Centrum Nauki, OPUS-20 competition, grant agreement no. 2020/39/B/HS5/01661) projects.

Literaturverzeichnis

[AC] ACE Project - The Electoral Knowledge Network: Electoral Cycle, URL: https://aceproject.org/electoral-advice/electoral-assistance/electoral-cycle, Stand: 16. 05. 2023.

[Bi21] Birkeland, B.: Investigators: Mesa County Clerk Allowed Unauthorized Person To Compromise Voting Equipment. CPR News, 2021.

[Bo03] Boyle, A.: E-voting flaws risk ballot fraud. NBC News, 2003.

[BP21] Bush, S.; Prather, L.: Healthy democracy requires trust – these 3 things could start to restore voters' declining faith in US elections. The Conversation, 2021.

[Br21] Brown, E.; Davis, A.; Swaine, J.; Dawsey, J.: The making of a myth. Washington Post, 2021.

[CC23] Cassidy, C.; Carr Smyth, J.: State voter fraud system fractures as Republicans opt out. AP News, 2023.

[Co23] Cohen, Z.: Text messages reveal Trump operatives considered using breached voting data to decertify Georgia's Senate runoff in 2021. CNN, 2023.

[CY18] Castenmiller, P.; Young, P.: Elections and IT; the challenge of making it work in a changed world. In (Krimmer, R.; Volkamer, M.; Cortier, V., Hrsg.): Third International Joint Conference on Electronic Voting E-Vote-ID 2018. Taltech Press, Bregenz, S. 170–179, 2018.

[De21] Department of Justice O of PA: Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election. Washington, 2021.

[Du22] Duenas-Cid, D.: A theoretical framework for understanding trust and distrust in internet voting. In (Krimmer, R.; Volkamer, M.; Duenas-Cid, D. e. a., Hrsg.): E-Vote-ID 2022 Proceedings. University of Tartu Press, Tartu, S. 57–62, 2022.

[Eu17] of Europe, C.: Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. Council of Europe, 2017.

[FHF06] Feldman, A.; Halderman, A.; Felten, E.: Security Analysis of the Diebold AccuVote-TS Voting Machine. Princeton, 2006.

[Fl15] Flis, J.; Frydrych, A.; Gendźwiłł, A.; et al: Co się stało 16 listopada? Wybory samorządowe 2014. Batorego Foundation, Warszawa, 2015.

[Go92] Govier, T.: Distrust as a practical problem. J Soc Philos 23, S. 52–63, 1992, DOI: 10.1111/j.1467-9833.1992.tb00484.x.

[Gr22a] Griswold, J.: Final agency order of dismissal. 2022.

[Gr22b] Grossi, C.: Investigation into Third Party Access to Vote Tabulators. 2022.

[Ho22] Hofmans, T.: Kiesraad vindt geen onregelmatigheden bij gebruik van OSV-verkiezingssoftware. Tweakers, 2022.

[Ja19] James, T. S.; Garnett, H. A.; Loeber, L.; van Ham, C.: Electoral management and the organisational determinants of electoral integrity: Introduction. International Political Science Review 40, S. 295–312, 2019, DOI: 10.1177/0192512119828206.

[KDK21a] Krimmer, R.; Duenas-Cid, D.; Krivonosova, I.: Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting — the good, the bad or the ugly. Public Money & Management, 2021.

[KDK21b] Krimmer, R.; Duenas-Cid, D.; Krivonosova, I.: New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper? Public Money and Management 41, S. 17–26, 2021, DOI: 10.1080/09540962.2020.1732027.

[Ke22] of Kenya, S. C.: Presidential Election Petition E005, E001, E002, E003, E004, E007 & E008 of 2022. Supreme Court of Kenya, 2022.

[Ko22] Kobylski, P.: Powszechność w głosowaniu korespondencyjnym w dobie COVID-19. Wybrane zagadnienia. Studia z Polityki Publicznej, 2022.

[Le22] Leavitt, J.: Cnty. of Fulton v. Sec'y of the Commonwealth. 2022.

[LMB98] Lewicki, R.; McAllister, D.; Bies, R.: Trust and Distrust: New Relationships and Realities. Academy of Management Review 23, S. 438–458, 1998.

[Lo11] Loeber, L.: Voter trust in the Netherlands between 2006 and 2010. In: CeDEM11 Proceedings of the International Conference for E-Democracy and Open Government. International Conference for E-Democracy und Open Government, S. 323–333, 2011.

[Lo14] Loeber, L.: E-voting in the Netherlands; past, current, future? In (Krimmer, R.; Volkamer, M., Hrsg.): Proceedings of the 6th international conference on electronic voting (EVOTE). TUT Press, Tallinn, S. 43–46, 2014.

[Lo16] Loeber, L.: E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years. In: 3rd International Conference on Electronic Voting 2008. Gesellschaft für Informatik, Bregenz, S. 21–30, 2016.

[Lo18] Loeber, L.: The E-voting Readiness Index and the Netherlands. In (Krimmer, R.; Volkamer, M.; Cortier, V., Hrsg.): Electronic Voting: Third International Joint Conference, E-Vote-ID 2018, Proceedings. Springer, Bregenz, S. 146–159, 2018.

[Lu17] Lumineau, F.: How Contracts Influence Trust and Distrust. J Manage 43, S. 1553–1577, 2017, DOI: 10.1177/0149206314556656.

[Lu79] Luhmann, N.: Trust and Power. Wiley-Blackwell, Chichester, 1979.

[Me22] Merrill, B.: Alabama Voting Machines Challenge. 2022.

[MI21] MIT Election Data and Science Lab: Voter Confidence, 2021, URL: https://electionlab.mit.edu/.

[MK20] Musiał-Karg, M.; Kapsa, I.: Alternatywne metody głosowania w opiniach Polaków. Postawy i poglądy względem wybranych form partycypacji w wyborach. UAM-WNPiD, Poznań, 2020.

[MK21] Musiał-Karg, M.; Kapsa, I.: Debate: Voting challenges in a pandemic—Poland. Public Money & Management, 2021.

[MRW12] McEvily, B.; Radzevick, J.; Weber, R.: Whom do you distrust and how much does it cost? An experiment on the measurement of trust. Games Econ Behav 74, S. 285–298, 2012, DOI: 10.1016/j.geb.2011.06.011.

[Mu16] Mueller III, R.: Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Washington, 2016.

[Mu20] Musiał-Karg, M.: Głosowanie korespondencyjne podczas pandemii Covid-19. Doświadczenia z polskich wyborów prezydenckich w 2020 r. Przegląd Prawa Konstytucyjnego, 2020.

[OLS97] Otnes, C.; Lowrey, T. M.; Shrum, L. J.: Toward an Understanding of Consumer Ambivalence. Journal of Consumer Research 24, S. 80–93, 1997, DOI: 10.1086/209495.

[Pa22a] Parks, M.: Hand-counting ballots may sound nice. It's actually less accurate and more expensive. NPR, 2022.

[Pa22b] Parks, M.: Some Republicans in Washington state cast a wary eye on an election security device. NPR, 2022.

[Pi23] Pierce, A.: Shasta County Supervisors Opt To Hand Count Vote. Details Remain Scarce. ShastaScout, 2023.

[PK22] Prentice, P.; Kirkwood, T.: Verified Petition For Relief. 2022.

[PP96] Priester, J. R.; Petty, R. E.: The gradual threshold model of ambivalence: Relating the positive and negative bases of attitudes to subjective ambivalence. J Pers Soc Psychol 71, S. 431–449, 1996.

[PS17] Pierzgalski, M.; Stępień, P.: A Peculiar Interpretation of the Constitutional Principle of "One Person, One Vote" in Poland: Voter (In)equality in the Elections to 1,200 Local Legislatures. East European Politics and Societies, 2017.

[Ra20] Ramsland, R.: Antrip Michingan Forensic Report. 2020.

[Ro98] Rousseau, D.; Sitkin, S.; Burt, R.; Camerer, C.: Not So Different After All: A Cross-Discipline View Of Trust. Academy of Management Review 23, S. 393–404, 1998.

[Sc03] Schwartz, J.: Ohio study finds flaws in electronic voting. NY Times, 2003.

[Se02] Senate and House of Representatives of the United States of America: Help America Vote Act of 2002. Senate und House of Representatives of the United States of America, Washington, 2002.

[SE22] Snow, A.; Ellgren, N.: Voting snag in Arizona fuels election conspiracy theories. AP News, 2022.

[Śl15] Śleszyński, P.: Hipotezy głosów nieważnych w wyborach powszechnych w Polsce po 1989 r. Social Space Journal, 2015.

[SLM21] Sipma, T.; Lubbers, M.; van der Meer, T.: Versplinterde vertegenwoordiging: Nationaal kiezersonderzoek 2021. SKON, 2021.

[St20] Stelmach, A.: Postal Voting. Poland and Solutions in Other Countries. Przegląd Prawa Konstytucyjnego, 2020.

[St22a] Stern, G.: Nevada high court rejects plea to stop county's hand-count. AP News, 2022.

[St22b] Stewart, C.: Trust in Elections. Daedalus 151, S. 234–253, 2022, DOI: 10.1162/daed_a_01953.

[TH00] Tschannen-Moran, M.; Hoy, W.: A Multidisciplinary Analysis of the Nature, Meaning, and Measurement of Trust. Rev Educ Res 70, S. 547–593, 2000, DOI: 10.3102/00346543070004547.

[TK96] Tyler, T.; Kramer, R.: Whither Trust? In: Trust in Organizations: Frontiers of Theory and Research. SAGE Publications, Inc., Thousand Oaks California 91320 United States, S. 1–15, 1996.

[TL06] Tomlinson, E.; Lewicki, R.: Managing Distrust in Intractable Conflict. Conflict Resolution Quarterly 24, S. 219–228, 2006, DOI: 10.1002/crq.

[To20] Tomlinson, E. C.; Schnackenberg, A. K.; Dawley, D.; Ash, S. R.: Re-visiting the trustworthiness–trust relationship: Exploring the differential predictors of cognition- and affect-based trust. J Organ Behav 41, S. 535–550, 2020, DOI: 10.1002/job.2448.

[Un22] Union, E.: European Union Election Observation Mission: Kenya 2022, Final Report, Techn. Ber., European Union, 2022.

[US22] U.S. District Court in the District of Arizona: Lake v. Hobbs – Electronic Voting Machines (AZ). 2022.

[Wa06] Wall, A.: Electoral Management Design: The International IDEA Handbook. International Institute for Democracy und Electoral Assistance (International IDEA), Stockholm, 2006.

[WA21] WAKE Technology Services: Fulton County Pennsylvania - Election System Analysis. 2021.

[Zb13] Zbieranek, J.: Alternatywne procedury głosowania w polskim prawie wyborczym. Gwarancja zasady powszechności wyborów czy mechanizm zwiększania frekwencji wyborczej? Difin, Warszawa, 2013.