JeDEM Issue16 (3): 29-49, 2024
ISSN 2075-9517
http://www.jedem.org
Date of submission: 17.05.2024
Date of acceptance: 05.09.2024
Article DOI: 10.29379/jedem.v16i3.922

Trust and electoral technologies throughout the election cycle: Comparing the USA, Netherlands, Poland, and Kenya

David Duenas-Cid

ORCID Nr 0000-0002-0451-4514
Kozminski University, Pub-Tech Research Center, 57/59 Jagiellońska, 03-301 Warszawa, Poland. dduenas@kozminski.edu.pl

Leontine Loeber

ORCID Nr 0000-0002-2272-6887
University of East Anglia, Research Park, Norwich NR4 7TJ, United Kingdom. leontine_loeber@xs4all.nl

Beata Martin-Rozumiłowicz

Independent expert consultant. ElectConsult, 123 Crescent Road, Oxford OX4 2NY, UK. rozumil@hotmail.com"

Ryan Macias

RSM Election Solutions, 1717 N Street NW STE 1, Washington, United States. ryan@rsmelectionsolutions.com

Abstract: Technology and election organization are increasingly intertwined, encompassing voting systems and supporting infrastructure. This interaction puts at the spotlight aspects related to trust and public confidence, fuelled by threat actors from actors aiming to disrupt electoral integrity using publicized attacks and disinformation campaigns against the use of such technologies. In the literature, there is still a lack of a cohesive, coordinated methodology for this issue that starts with a needs-based approach. This paper analyses the relationship between trust and technology implementation across the electoral cycle by presenting a set of selected case studies presenting diverse levels of democratic development and types of election management bodies. While examining how trust- and distrust-related factors influence implementation, this paper supports experts aiming to approach aspects related to the current erosion of trust in democracy and technology's impact.

Keywords: trust, distrust, election technologies

Acknowledgement: 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.

1. Introduction

Elections are one of the most important societal agreements in place in our everyday lives. Their management plays a crucial role in power delegation from citizens to political elites and power transition between elites, trust being at the core of this process: citizens and politicians need to trust that elections were genuinely and democratically managed to accept its outcomes and have a peaceful transition of power. At the same time, seeding distrust is one of the most common strategies for undermining democracies globally, putting pressure on finding strategies to combat distrust creation strategies (i.e., disinformation) to preserve voters' confidence in elections and democracy. The use of technology in elections adds a new layer of complexity to this already intricate equation [1], targeting new elements of potential distrust (voter registration, result management systems - RMS, etc.) and increasing the need to understand what factors help build trust and distrust and how they interact [2]. This paper contributes to this discussion by examining four cases with substantial differences but also with common ground; they all use some forms of electoral technology, and trust- and distrust-related elements can be identified throughout their electoral cycles.

A second element to consider is understanding technologies (in general, not only electoral ones) as socio-technical constructs and how this relates to the previous. This assumption quite extended in the research on social sciences and technology [3], considers that every technology is contextualized in a societal environment, helping in its definition, development, and use. Accordingly, for approaching trust, the two aspects of technology (technical and societal) should be considered, leading to a distinction between the trustworthiness of the technology and the trust in the technology itself. On some occasions, trust is posited in untrustworthy systems, and, in other cases, the opposite might occur; the reasons for the previous are diverse and focus on different parts of the electoral cycle. This is an important element to consider since a traditional focus in the research on the topic has centered on what occurs on election day, i.e., casting, counting, and tabulating the votes. However, this scope is too narrow to include aspects such as the spread of misinformation during boundary delimitation, voter registration, the campaign, or other electoral phases, which can also lead to creating trust or distrust. The same applies to post-electoral disputes and judicial processes to resolve election complaints. Although meant to create trust, lengthy procedures with difficult rulings, lack of technical knowledge on the part of justices, and focused disinformation campaigns can also easily lead to mistrust.

This paper, again, aims to contribute to the existing knowledge by analyzing four cases (USA, The Netherlands, Poland, and Kenya) and looking at the interaction between the theoretical literature and concrete examples of what transpired in these recent elections. Examining the chosen cases contributes to detecting and understanding elements creating trust and distrust and placing them

in different moments of the electoral cycle, expanding the perspective beyond the election day and providing a more realistic picture of election technology impacts.

2. Theoretical Framework and Methodology

The introduction of technology in elections has increased considerably in recent decades [4], 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 [5] and results management systems [6]. Others have moved beyond voting machines in controlled environments (e.g., polling station Direct Recording Electronic Machines DREs) [7] to piloting electronic voting in uncontrolled environments (e.g., internet voting) for certain categories of voters [8]. International support (either bilateral or organizational) for such initiatives, especially in developing democracies, has supported this space financially and programmatically [9]. Initial iterations focused primarily on providing 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.

In addition to that, there is also a growing awareness that technology introduction and increased trust do not necessarily go hand-in-hand [10]. The relationship between trust and electoral technologies is complex, starting with the very distinction between trust and distrust or between trust and trustworthiness. Research suggests that trust and distrust are not symmetrically opposed concepts but related but different theoretical constructs to be assessed and evaluated independently of one another [11]. This assumption allows considering the coexistence of trust and distrust in parallel and towards the same targets [10, 12, 13], for example, on democratically concerned hacktivists who discuss the adequacy of certain voting technologies (distrust) to improve the overall quality of elections (trust) [14]. It also allows overcoming a traditional gap in the research on technological innovations, where approaching the elements that make citizens trust has been notably predominant in front of those leading to distrust [15]. Similarly, trust and trustworthiness should be regarded as different concepts. The latter has often been considered as an antecedent to trust, in other words, as an aspect that influences a trusting relationship by referring to the trustee's property. Trustworthiness, then, plays an obviously important role in the creation of trust [16], but the relation between them is not necessarily causal since several other factors influence trust. In the case of electoral technologies, trustworthiness connects with the technological properties of the system in use in terms of security, reliability, or performance [17] and can be linked with actual trust and distrust by providing adequate (or not) management and transparency, as will be further discussed in this piece. In contrast, trust and distrust also expand to the societal dimension of the process by including a more extensive set of stakeholders and inputs in the equation [10].

Approaching trust in election technologies, hence, permits an analysis of the socio-technical nature of technology [18]. The societal dimension of electoral technologies is undeniable, being that elections are at the core of the functioning of a society and, as a result, enmeshed in a complicated set of political influences. In parallel, electoral technologies are inserted in a complex organizational environment with a significant number of stakeholders that can potentially influence citizens' perception of the system. This list includes issues and stakeholders related to the technology but also

the institutional framework, relations with citizens, and even geopolitical relations [2]. However, not only the organizational setup of elections influences the adoption or not of technologies [19, 20] and their further promotion amongst the citizenry [21].

Although, as mentioned before, there is a growing interest in these issues and aspects of trust, we find that in the literature, there is still a lack of a cohesive, coordinated methodology that starts with a needs-based approach. Such an approach is necessary to really capture the different dimensions of trust in electoral technologies. Another area that needs more academic attention is the connection between introducing electoral technologies and the electoral cycle. Often, technologies are inserted in one area of the cycle without a clear idea of how this might affect other areas of the cycle. The framework used in this paper explicitly uses this more cohesive electoral cycle approach (see Figure 1) [22]. 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 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.

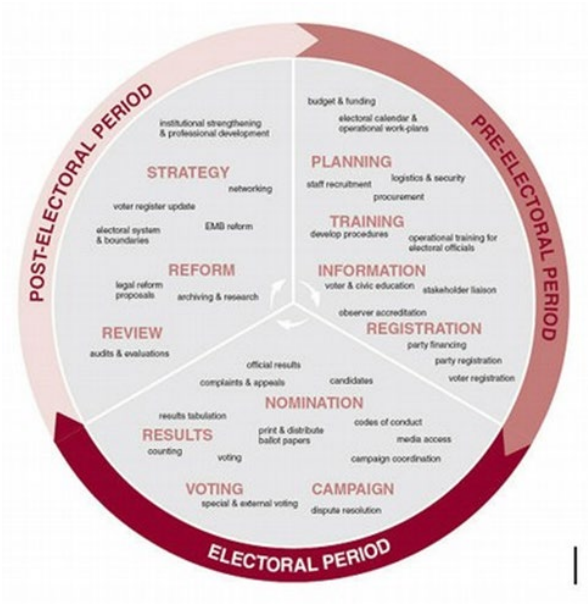

Figure. 1. The Electoral Cycle (developed by the European Commission, IDEA, and UNDP)[22]

Various crises of public trust have also led to a better understanding that the introduction of technology in elections and an increase in trust are not colinear processes [23, 24]. 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, greater damage than good may result in building trust in democratic institutions by introducing technology. The case studies add to the existing literature by showing this interaction. Very often, technology introduction is par-

tially 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, the disconnect often happens by institutional ossification rather than by design. In contrast, the overarching approach should be 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.

With this idea in mind, in this paper, we aim to respond to the question of how we can analyze the use of electoral technologies approaching the electoral cycle and its impact on the creation of trust and distrust. In this research, we approach the electoral cycle to detect and compare the touchpoints between technology and trust occurring in different stages of the electoral process and to compare them within a selection of relevant cases. For doing so, we propose an inductive approach and rely on literature and acquired in-depth knowledge from the cases to reflect on the relationship between election technology and trust. The dependent variable the paper looks at is the perceived level of trust in the countries. The cases used are Poland, Kenya, the Netherlands, and the United States. 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 organizing elections. The Netherlands and the U.S. are usually considered old democracies since they have held elections for over 100 years. Poland is a younger democracy, 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.

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 published research 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 [25]. This means that the technology to conduct the elections also varies between states and, in many cases, by local jurisdictions within a state. The dispersed 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 [26]; amongst the reasons is 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 [27] 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 [28] 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 [29–31]. 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. It 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 [32]. 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 [33]. 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 [34] and that they gained access to a municipal jurisdiction's results management system (RMS) website.

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

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 voter's intent. 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 entirely 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, using a Dominion Voting System application, Adjudication, was at the forefront of these misinformation attacks by threat actors. Many media outlets amplified the claim that Dominion changed votes through the Adjudication software. That was one of the claims that 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 [35].

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 [36–40]. 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 [41, 42]; experts agree that a full hand count tally in American elections is a less secure and less accurate method of tabulating votes [41]. 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 [43–47].

Continuing after the 2022 election and as recently 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 [48], ballot printing technology [49], and systems that are used to clean voter registration databases to prevent voter fraud [50].

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 [27], 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 trying to distrust the democratic institution. While the study and recalls show more confidence in the election machinery, the increased polarization creates chaos and sows discord in American and democratic institutions.

3.2. THE NETHERLANDS

The case of the Netherlands is an interesting one because this country 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, using 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 (DREs) in the early 1960s 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 lacked 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 led to the withdrawal of the certification of the voting computers and a return to voting with paper ballots [51, 52]. In 2008, internet voting was considered for nationwide elections for the waterboards, a form of decentralized government. 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 slight majority at that time stated that they preferred to use paper ballots, in contrast with 2006 and 2010 [53]. 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 computer is the most reliable, some of them would still prefer this. This difference in appreciation between the preferred and most reliable methods is even more significant 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, the convenience of the voting method seems to prevail over the question of trust [54].

Another area in the electoral cycle where technology is used in the Netherlands is for tabulating and calculating 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. Nearly all political parties and municipalities use the software during the election process, 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, brought to the next level in person, and manually re-entered into the system. Until the 2017 election, it was also standard procedure that a digital file of the results was transferred together with the paper print using USB sticks. Due to questions concerning the safety of that procedure, this was abandoned [55].

Just before the 2017 parliamentary elections, a news report stated that the software was unsafe and could be hacked in a way that would make it possible to change the outcome of the results. 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 [56].

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 involved in the Dutch Parliamentary Election Study stated that they felt 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 who 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 was not 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 [57].

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 the media states about the technology. Even though counting the ballots is still done by hand in the Netherlands, based on some news reports, many voters thought 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 that occurred in 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 the 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 (on average). This low average turnout [58] (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 [59], 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 [59]. The election code proposed in 2011 allowed significant vote-value disparities, conflicting with the Polish constitutional requirement of voter equality [60]. 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 [61]. A combination of legal, managerial, and trust-related issues [62] forced them 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 [63, 64].

The second example shedding light on the functioning of Polish elections relates to the problems that 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 in this election [65].

A report by Fundacja Batorego [66] describes how the problem in the IT system for calculating the results escalated and ended 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 several 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. Still, several 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 introducing 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. This followed the Kriegler report following the 2007 post-election violence, which recommended a move to a "modern, IT-facilitated process".[1] 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 introducing technology in elections would improve public trust in the election process and 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, and some ideological. Although this was essentially a government decision, it should have been made more openly and transparently. To the author's knowledge, this did not 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 typically 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 introducing the Biometric Voter Registration System (BVR) in 2013, technical expertise was also quite limited in the allocation of time. Thus, there was only a basic level

[1] Kriegler and Waki Report on 2007 Elections, pg.26

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. The 2022 EU EOM final report found that "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."[67]. 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."[68]

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 role 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 failures. Unfortunately, according to the latest international standards, this is not a valid approach, and EMBs should be considered ultimately responsible for any implementation of technology in elections [69].

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 served to raise public trust to some extent.

Throughout such technological applications 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 accountable for their specification, procurement, and implemen-

tation. 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' and '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 proposes a discussion around different elements interacting with the conceptual duality of trust and distrust and the use of electoral technologies throughout the electoral cycle. The four cases described represent four different combinations of levels of democratization and type of election management body (EMB) and, stemming from their analysis, we can detect salient trust and distrust elements and at what stages of the electoral cycle they refer to. The following table summarizes some of these elements, mostly related to challenging trust in the electoral system:

Table 1. Summary

Pre-electoral period	Electoral period	Post-electoral period
External incursions in the electoral systems in use: voter registration, verification, software, voter information, or result management (USA). Failed renovation of voting methods due to a lack of management capacity (Poland). Anomalies in the procurement of NVTs due to lack of transparency (Kenya). Limited access to information about the NVT implementation process, especially about the findings, recommendations, and subsequent changes made after the auditing process (Kenya).	Problems with the recount of pre-scored punch cards (USA). Development of software to support the management of ballot adjudication: 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 (USA). Hacker reports on the untrustworthiness of voting systems in terms of lack of transparency, verifiability and voter secrecy (The Netherlands). A failed system for result transmission pro-	Court cases to force local EMBs to get rid of their NVT and conduct hand counts (USA). Challenging of electoral results by the opposition and Supreme Court decision to re-run elections in 2017 due to technology inconsistencies and lack of capacity to ascertain the correctness of results (Kenya).

	voked a late communication of results and heightened controversy (Poland).	
General impact throughout the electoral cycle		
Targeted attacks to adjacent systems such as intrusion detection systems, ballot printing technology, and systems to clean voter registration databases to prevent voter fraud, having a spillover impact on the general perception of elections (USA) Public exposition of vulnerabilities by computer scientists and researchers that left opportunities for manipulation in election results via the NVT (USA). Deliberate use of expert knowledge on NVT vulnerabilities to spread non-grounded theories that the NVT or the companies that developed the technologies had been manipulated or perpetuated fraud in the tabulation process (USA). Doubts cast on technology for vote tabulation and calculation (The Netherlands).		

From this table, we can extract a set of findings, the first one being that trust-related issues are not only important when new technology is introduced (as in the Polish case) 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, where technologies already used in several elections are challenged and disputed for very diverse reasons, from the legitimate questioning of their trustworthiness to a strategy to undermine trust in democracy. In general, we can also find how trust and trustworthiness differ conceptually but also in relation to their impacts on trust and distrust creation. Technology systems can often be designed to be trustworthy yet still not enjoy trust. An example of this is the 2020 elections in the US. As the Center for Election Innovation and Research found: "The 2020 general election was the most secure in American history. Almost 95% of all ballots were cast on auditable paper, up from less than 80% in 2016, including all ballots in every swing state. States nationwide conducted more legitimate audits of those ballots than ever before. More pre-election litigation clarified the rules, and more post-election litigation confirmed the results, than ever before" [70]. The same can be said for the process concerning the tabulation and calculation of votes in the Netherlands. Because the electronic process was only supportive of the paper process, which was legally binding, the process itself had enough safeguards to be trustworthy, fraud would have been detected if it actually had happened. However, because of how the story was told in the media, there was a lack of trust.

Conversely, as the early stages of the Netherlands and Kenya implementation show, there can also be trust without trustworthiness, pointing in other directions than the technology in the creation of trust: it can be transmitted either from a successful and convenient previous experience, or the trust posited on the previous good work of EMBs. But distrust is also showing this capacity to stem some ancillary systems, which are attacked not because of their centrality or relevance on the actual outcomes of elections, but because of their capacity to cast doubts on the overall security of the system as a whole. The use of NVT along the electoral cycle adds new layers of complexity at different levels (e.g., technical, managerial, or procedural) that, consequently, may trigger 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 accountable for their specification, procurement, and implementation. Ultimately, such a more holistic approach could have led to less polarization and disinformation in an already polarized environment. 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 combined to decrease rather than increase trust in the electoral process. Also, it is worth noting that the number of stakeholders linked to the active provision of trust and those potentially providing distrust is unbalanced towards distrust providers. On 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 case findings, which conclude 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, proving to be a useful examination model. Additionally, trust or distrust can span multiple election cycles, such as in the U.S. case study, where the foundation for distrust in the 2020 election was laid in the early 2000s after the use of new voting technologies became mainstream. With more election management bodies implementing NVT, it provides an opportunity to explore NVTs' role in trust and distrust of electoral processes in the long term.

5. References

1. Cheeseman, N., Lynch, G., Willis, J.: Digital dilemmas: the unintended consequences of election technology. Democratization. 25, 1397–1418 (2018). https://doi.org/10.1080/13510347.2018.1470165.

2. Duenas-Cid, D.: A theoretical framework for understanding trust and distrust in internet voting. In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Germann, M., Glondu, S., Hofer, T., Krivonosova, I., Martin-Rozumilowicz, B., Rønne, P., and Zollinger, M.-L. (eds.) E-Vote-ID 2022 Proceedings. pp. 57–62. University of Tartu Press, Tartu (2022).

3. Van Dijck, J.: The culture of connectivity: A critical history of social media. Oxford University Press, New York (2013).

4. Garnett, H.A., James, T.: Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity. Election Law Journal: Rules, Politics, and Policy. 19, 111–126 (2020).

5. Kiyohara, S.: Adoption of Online Voter Registration Systems as the New Trend of US Voter Registration Reform. The Japanese Journal of American Studies. 30, 31–51 (2019).

6. Passanti, C., Pommerolle, M.-E.: The (un)making of electoral transparency through technology: The 2017 Kenyan presidential election controversy. Soc Stud Sci. 52, 928–953 (2022).

7. Everett, S.P., Greene, K.K., Byrne, M.D., Wallach, D.S., Derr, K., Sandler, D., Torous, T.: Electronic voting machines versus traditional methods. In: Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI '08. p. 883. ACM Press, New York, New York, USA (2008). https://doi.org/10.1145/1357054.1357195.

8. Germann, M., Serdült, U.: Internet Voting for Expatriates: The Swiss Case. JeDEM - eJournal of eDemocracy and Open Government. 6, (2014). https://doi.org/10.29379/jedem.v6i2.302.

9. Obinna Ibeanu, O.: Digital Technologies and Election Management in Africa's Democratisation Process More Technocratic than Democratic? , Dakar (2021).

10. Duenas-Cid, D.: Trust and distrust in electoral technologies: what can we learn from the failure of electronic voting in the Netherlands (2006/07). In: Duenas-Cid, D., Liao, H.-C., Macadar, M.A., and Bernardini, F. (eds.) 25th Annual International Conference on Digital Government Research (DGO 2024), June 11–14, 2024, Taipei, Taiwan. pp. 1–9. ACM , Taipei (2024).

11. Duenas-Cid, D., Calzati, S.: Dis/Trust and data-driven technologies. Internet Policy Review. 12, (2023). https://doi.org/10.14763/2023.4.1727.

12. Otnes, C., Lowrey, T.M., Shrum, L.J.: Toward an Understanding of Consumer Ambivalence. Journal of Consumer Research. 24, 80–93 (1997). https://doi.org/10.1086/209495.

13. Priester, J.R., Petty, R.E.: The gradual threshold model of ambivalence: Relating the positive and negative bases of attitudes to subjective ambivalence., (1996). https://doi.org/10.1037/0022-3514.71.3.431.

14. Gonggrijp, R., Hengeveld, W.-J.: Studying the Nedap/Groenendaal ES3B Voting Computer: A Computer Security Perspective. In: Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology. p. 1. USENIX Association, USA (2007).

15. Six, F.E., Latusek, D.: Distrust: A critical review exploring a universal distrust sequence. Journal of Trust Research. 1–23 (2023). https://doi.org/10.1080/21515581.2023.2184376.

16. Tomlinson, E.C., Schnackenberg, A.K., Dawley, D., Ash, S.R.: Revisiting the trustworthiness–trust relationship: Exploring the differential predictors of cognition- and affect-based trust. J Organ Behav. 41, 535–550 (2020). https://doi.org/10.1002/job.2448.

17. Belanger, F., Hiller, J.S., Smith, W.J.: Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. The Journal of Strategic Information Systems. 11, 245–270 (2002). https://doi.org/10.1016/S0963-8687(02)00018-5.

18. Appelbaum, S.H.: Socio-technical systems theory: an intervention strategy for organizational development. Management Decision. 35, 452–463 (1997). https://doi.org/10.1108/00251749710173823.

19. Licht, N., Duenas-Cid, D., Krivonosova, I., Krimmer, R.: To i-vote or Not to i-vote: Drivers and Barriers to the Implementation of Internet Voting. In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Kulyk, O., Rønne, P., Solvak, M., and Germann, M. (eds.) Electronic Voting. E-Vote-ID 2021. Lecture Notes in Computer Science. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-86942-7_7.

20. Loeber, L.: Use of Technology in the Election Process: Who Governs? Election Law Journal: Rules, Politics, and Policy. 19, 149–161 (2020). https://doi.org/10.1089/elj.2019.0559.

21. Adeshina, S.A., Ojo, A.: Factors for e-voting adoption - analysis of general elections in Nigeria. Gov Inf Q. 37, 101257 (2020). https://doi.org/10.1016/j.giq.2017.09.006.

22. ACE Project - The Electoral Knowledge Network: Electoral Cycle, https://aceproject.org/electoral-advice/electoral-assistance/electoral-cycle, last accessed 2023/05/16.

23. Duenas-Cid, D., Krivonosova, I., Serrano, R.A., Freire, M., Krimmer, R.: Tripped at the Finishing Line: The Åland Islands Internet Voting Project. In: Krimmer, R., Volkamer, M., Beckert, B., Küsters, R., Kulyk, O., Duenas-Cid, D., and Solvak, M. (eds.) International Joint Conference on Electronic Voting E-Vote-ID 2020. pp. 36–49. Springer LNCS, Bregenz (2020). https://doi.org/https://doi.org/10.1007/978-3-030-60347-2_3.

24. Oostveen, A.-M.: Outsourcing Democracy: Losing Control of e-Voting in the Netherlands. Policy Internet. 2, 201–220 (2010). https://doi.org/10.2202/1944-2866.1065.

25. Bush, S., Prather, L.: Healthy democracy requires trust – these 3 things could start to restore voters' declining faith in US elections, (2022).

26. Stewart, C.: Trust in Elections. Daedalus. 151, 234–253 (2022). https://doi.org/10.1162/daed_a_01953.

27. MIT Election Data and Science Lab: Voter Confidence. , Massachusetts (2021).

28. Senate and House of Representatives of the United States of America: Help America Vote Act of 2002. Senate and House of Representatives of the United States of America, Washington (2002).

29. Boyle, A.: E-voting flaws risk ballot fraud, https://www.nbcnews.com/id/wbna3077251, (2003).

30. Schwartz, J.: Ohio study finds flaws in electronic voting, https://www.nytimes.com/2003/12/03/us/ohio-study-finds-flaws-in-electronic-voting.htmlhttps://www.nytimes.com/2003/12/03/us/ohio-study-finds-flaws-in-electronic-voting.html, (2003).

31. Feldman, A., Halderman, A., Felten, E.: Security Analysis of the Diebold AccuVote-TS Voting Machine. , Princeton (2006).

32. Mueller III, R.S.: Report On The Investigation Into Russian Interference In The 2016 Presidential Election. , Washington (2016).

33. Brown, E., Davis, A., Swaine, J., Dawsey, J.: The making of a myth, https://www.washingtonpost.com/investigations/interactive/2021/trump-election-fraud-texas-businessman-ramsland-asog/, (2021).

34. Department of Justice, O. of P.A.: Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election. , Washington (2021).

35. Ramsland, R.: Antrip Michingan Forensic Report. (2020).

36. WAKE Technology Services: Fulton County Pennsylvania - Election System Analysis. (2021).

37. Birkeland, B.: Investigators: Mesa County Clerk Allowed Unauthorized Person To Compromise Voting Equipment, https://www.cpr.org/2021/08/12/investigators-mesa-county-clerk-allowed-election-conspiracy-theorist-to-compromise-voting-equipment/, (2021).

38. Grossi, C.M.: Investigation into Third Party Access to Vote Tabulators, https://www.michigan.gov/-/media/Project/Websites/AG/releases/2022/August/Investigation-into-Third-Party-Access-to-Vote-Tabulators.pdf, (2022).

39. Cohen, Z.: Text messages reveal Trump operatives considered using breached voting data to decertify Georgia's Senate runoff in 2021, https://edition.cnn.com/2023/04/21/politics/trump-georgia-senate-breached-voting-data/index.html, (2023).

40. Stern, G.: Nevada high court rejects plea to stop county's hand-count, https://apnews.com/article/2022-midterm-elections-voting-rights-nevada-reno-d8b026034790812e7d04621d22193138, (2022).

41. Pierce, A.: Shasta County Supervisors Opt To Hand Count Vote. Details Remain Scarce., https://shastascout.org/shasta-county-supervisors-opt-to-hand-count-vote-details-remain-scarce/, (2023).

42. Parks, M.: Hand-counting ballots may sound nice. It's actually less accurate and more expensive, https://www.npr.org/2022/10/07/1126796538/voting-explainer-hand-counting-ballots-accuracy-cost, (2022).

43. Judge Leavitt: Cnty. of Fulton v. Sec'y of the Commonwealth. (2022).

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

45. Merrill, B.: Alabama Voting Machines Challenge. (2022).

46. Prentice, P., Kirkwood, T.: Verified Petition For Relief. (2022).

47. Griswold, J.: Final agency order of dismissal. (2022).

48. Parks, M.: Some Republicans in Washington state cast a wary eye on an election security device, https://www.npr.org/2022/08/28/1119692541/washington-state-albert-sensor-cybersecurity-election-security, (2022).

49. Snow, A., Ellgren, N.: Voting snag in Arizona fuels election conspiracy theories, https://apnews.com/article/2022-midterm-elections-donald-trump-arizona-4e15278b82452878d6f6aa45b2984579, (2022).

50. Cassidy, C., Carr Smyth, J.: State voter fraud system fractures as Republicans opt out, https://apnews.com/article/voter-fraud-election-conspiracies-registration-trump-republicans-23f0a2f89b6c8b53c4c7b89e2bdc82af, (2023).

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

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

53. Loeber, L.: Voter trust in the Netherlands between 2006 and 2010. In: CeDEM11 Proceedings of the International Conference for E-Democracy and Open Government. pp. 323–333. International Conference for E-Democracy and Open Government (2011).

54. Loeber, L.: The E-voting Readiness Index and the Netherlands. In: Krimmer, R., Volkamer, M., Cortier, V., Goré, R., Hapsara, M., Serdült, U., and Duenas-Cid, D. (eds.) Electronic Voting: Third International Joint Conference, E-Vote-ID 2018, Bregenz, Austria, October 2-5, 2018, Proceedings . pp. 146–159. Springer, Bregenz (2018).

55. Castenmiller, P., Young, P.: Elections and IT; the challenge of making it work in a changed world. In: Krimmer, R., Volkamer, M., Cortier, V., Duenas-Cid, D., Goré, R., Hapsara, M., Koenig, R., Martin, S., McDermott, R., Roenne, P., Serdült, U., and Truderung, T. (eds.) Third International Joint Conference on Electronic Voting E-Vote-ID 2018 2–5 October 2018, Lochau/Bregenz, Austria, Proceedings. pp. 170–179. Taltech Press, Bregenz (2018).

56. Hofmans, T.: Kiesraad vindt geen onregelmatigheden bij gebruik van OSV-verkiezingssoftware, (2022).

57. Sipma, T., Lubbers, M., van der Meer, T., Spierings, N., Jacobs, K.: Versplinterde vertegenwoordiging: Nationaal kiezersonderzoek 2021. SKON (2021).

58. Musiał-Karg, M., Kapsa, I.: Alternatywne metody głosowania w opiniach Polaków. Postawy i poglądy względem wybranych form partycypacji w wyborach. UAM-WNPiD, Poznań (2020).

59. Stelmach, A.: Postal Voting. Poland and Solutions in Other Countries. Przegląd Prawa Konstytucyjnego. 58, 83–97 (2020). https://doi.org/10.15804/ppk.2020.06.06.

60. 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: and Cultures. 31, 704–738 (2017). https://doi.org/10.1177/0888325417717787.

61. 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. 41, 8–10 (2021). https://doi.org/10.1080/09540962.2020.1766222.

62. Musiał-Karg, M., Kapsa, I.: Debate: Voting challenges in a pandemic—Poland. Public Money & Management. 41, 6–8 (2021). https://doi.org/10.1080/09540962.2020.1809791.

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

64. Kobylski, P.: Powszechność w głosowaniu korespondencyjnym w dobie COVID-19. Wybrane zagadnienia. Studia z Polityki Publicznej. 9, 83–95 (2022). https://doi.org/10.33119/KSzPP/2022.1.4.

65. Śleszyński, P.: Hipotezy głosów nieważnych w wyborach powszechnych w Polsce po 1989 r. Social Space Journal. 2, 1–31 (2015).

66. Flis, J., Frydrych, A., Gendźwiłł, A., Michalak, B., Rutkowski, J., Rychard, A., Zbieranek, J.: Co się stało 16 listopada? Wybory samorządowe 2014. , Warszawa (2015).

67. European Union: European Union Election Observation Mission: Kenya 2022, Final Report. , Brussels (2022).

68. Supreme Court of Kenya: Presidential Election Petition E005, E001, E002, E003, E004, E007 \& E008 of 2022. (2022).

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

70. Center for Election Innovation and Research: Survey of Voter Beliefs about Election Integrity in 2020 and 2022. (2023).

About the Authors

David Duenas-Cid

David Duenas-Cid is the Associate Professor and Director of the Public Sector Data-Driven Technologies Research Center at Kozminski University (Poland). President of the Working Group on Digital Sociology at the International Sociological Association, General Chair at the E-Vote-ID Conference, Program Chair at the Annual International Conference on Digital Government Research and Mini-Track Chair on e-Democracy, e-Participation and e-Voting at the Hawaii International Conference on System Sciences.

Leontine Loeber

Leontine Loeber is a legislative lawyer and department head at the Ministry of Education of the Netherlands. Visiting scholar and researcher at the Vrije Universiteit Amsterdam. Outreach chair and member of the Programme Committee for E-Vote-ID. Member of the International Advisory Board for the Electoral Integrity Project.

Beata Martin-Rozumiłowicz

Dr. Beata Martin-Rozumiłowicz is an International Electoral Expert with two and a half decades of election observation and technical assistance experience. She's been Deputy Chief Observer on EU EOMs to Zimbabwe (2023), Kenya (2022), and The Gambia (2021/2022). Previously, she was Director for Europe and Eurasia at IFES in Washington, D.C. and also headed OSCE/ODHIR's Election Department in Warsaw, Poland. Beata has co-authored OSCE/ODIHR's new ICT Handbook and is currently working on a special edition on updating political party assistance strategies together with a number of academics and practitioners, soon to be published in Policy Studies.

Ryan Macias

Ryan Macias is the owner of RSM Election Solutions LLC, a consultancy providing subject matter expertise in election technology, security, and administration. Member of the National Task Force on Election Crises, the Advisory Group for the GCA Cybersecurity Toolkit for Elections, Programme Committee for E-VOTE-ID, Steering Committee for Center for Internet Security (CIS) Rapid Architecture-Based Election Technology Verification (RABET-V), and Board Member to California Voter Foundation (CVF).

