"But they have overlooked a few things in Afghanistan:" An Analysis of the Integration of Biometric Voter Verification in the 2019 Afghan Presidential Elections

Kabir Panahi and Shawn Robertson, *University of Kansas;* Yasemin Acar, *Paderborn University;* Alexandru G. Bardas, *University of Kansas;* Tadayoshi Kohno, *University of Washington;* Lucy Simko, *The George Washington University*

https://www.usenix.org/conference/usenixsecurity24/presentation/panahi

This paper is included in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Open access to the Proceedings of the 33rd USENIX Security Symposium is sponsored by USENIX.

"But they have overlooked a few things in Afghanistan:" An Analysis of the Integration of Biometric Voter Verification in the 2019 Afghan Presidential Elections

Kabir Panahi
University of Kansas

Shawn Robertson
University of Kansas

Yasemin Acar
Paderborn University

Alexandru G. Bardas
University of Kansas

Tadayoshi Kohno
University of Washington

Lucy Simko
The George Washington University

Abstract

Afghanistan deployed biometric voter verification (BVV) machines nationally for the first time in the critical 2019 presidential election. Through the leading authors' unique backgrounds and involvement in this election, which facilitated interviews with 18 Afghan nationals and international participants who had an active role in this Afghan election, we explore the gap between the expected outcomes of the electoral system, centered around BVVs, and the reality on election day and beyond. We find that BVVs supported and violated the electoral goals of voter enfranchisement, fraud prevention, enabling public trust, and created threats for voters, staff, and officials. We identify technical, usability, and bureaucratic underlying causes for these mismatches and discuss several vital factors that are part of an election.

1 Introduction

Democracies today often involve technology in elections, e.g., to record votes, register voters or verify identity, transmit votes, and report results. Although computer technology is not *inherently* part of the electoral process, its use confers both massive benefits and potential vulnerabilities that must be carefully managed to preserve the integrity of the electoral process and to maintain public trust. The compromise or misuse of any technology involved in conducting an election has the potential to violate democratic goals and lead to political instability or an illegitimate government.

There has been significant work in the security and privacy community regarding electoral technologies, notably, about their hardware and software security properties (e.g., [71,79]), and about usability issues in practice (e.g., [51]), more details in Section 2. However, substantial questions remain about the use of (in)secure and (un)usable technologies in practice in electoral systems, especially in non-Western contexts.

In this work, we begin to fill a gap about the design and use of voter-facing technology in a non-Western context, following technical computer (in)security from its non-technical causes to its non-technical consequences in Afghanistan's 2019 presidential election. Before the 2019 presidential election, Afghanistan had experienced decades of armed conflict, political instability, and changing regimes, including civil war, the rise and fall of the Taliban, and fighting between the government and insurgent groups [36, 61]. Each election from 2004–2018 was marred with allegations of widespread and systemic fraud and disenfranchisement—multiple voting, ballot stuffing, and manipulation of voters or ballots [38, 42, 46, 73]. In 2009, for example, 1.3 million ballots were discarded as fraudulent, and after the 2014 presidential election, European Union election observers wrote that, after an audit by the United Nations and the US, "large scale fraud had been committed" [38]: some polling stations reported no data [38], while others reported orders of magnitude more votes than voters [42]. This combination of the electoral, political, and societal context made it particularly difficult, in 2019, to achieve a legitimate and trustworthy election in a young democracy that was simultaneously building or acquiring key physical institutions and infrastructure while facing significant domestic or international threats [94, 101].

To mitigate the systemic fraud in prior elections, the Afghan government deployed **biometric voter verification (BVV)** machines in the 2019 presidential election—the first time voter-facing technology had been employed in much of the country—requiring voters to pre-register before the election (without biometrics) and have their fingerprints and faces biometrically captured on election day (for post-processing deduplication) before casting a paper ballot. This process promised to enforce one vote per voter while making voting accessible to all [32]. Given Afghanistan's at-the-time fragile political state after decades of war and terrorism, many Afghans hoped the 2019 election would be a step towards political stability and further economic development. However, 2019's election day brought technical issues with voter verification and vote collection, causing disenfranchisement [27, 66], disputed votes, and political instability [2].

This research, led by a former Afghan Independent Election Commission (IEC)[1] employee, has the unique opportunity to study the deployment and use of these BVV machines during the 2019 Afghan presidential election. We focus on the introduction of BVV as the central and new element of the 2019 Afghanistan election, and as a critical electoral technology whose misuse or compromise led or could have led to technical security issues, voter disenfranchisement, fraud, and political instability. We explore the new technical ecosystem surrounding BVV as well as how it fit within Afghanistan's social, political, and environmental contexts, given that in hindsight we know that the electoral system did *not* function as intended. We ask: what happened, and *why*? What can we learn about technology, policy, and elections? We center our research around the research questions below, categorized in three broad topics:

- **The Biometric Voter Verification (BVV) ecosystem:** What were the goals when BVV was adopted? How was BVV integrated in the electoral process? In what ways did BVV machines work well, and what issues did they face?
- **Consequences:** What were the *consequences* of the BVVs on the electoral system? To what extent did the BVV ecosystem enable or prevent a democratic election?
- **Causes for issues and design alignments between BVVs and the electoral system:** *Why* (technically, politically, and administratively) was the BVV ecosystem designed, implemented, and deployed the way it was?

We address these topics through 18 semi-structured interviews with key international and Afghan election workers, a unique look into both technical issues and non-technical causes and consequences of those issues. Importantly, although our participants' expertise and direct experience with the election is a huge asset for our study, we are inherently limited by lack of direct access to other primary sources, such as BVV devices themselves, or their original design specifications. However, our interviews are informed by the first and second authors' own expertise: the first author is Afghan and worked for the Independent Election Commission during the 2019 election, and the second author is a member of the US armed forces, with a tour of duty in Afghanistan. We deeply reflect on our methodological decisions, our positionality as researchers, and the ethical implications of conducting this research in Section 3.

Through our interviews, we find three thematically emergent electoral goals for biometric voter verification to support—voter enfranchisement, fraud prevention, and maintenance and increase of public trust—and ground this research about biometric voter verification technology in a discussion of *how and why* it both supported and violated these goals in Afghanistan in 2019. Deciding *whether* these goals are met is *not* our aim as we analyze the complexity of our expert participants' knowledge and opinions. For example, some felt the BVVs enabled fraud—if poll workers allowed it—by using multiple fingers of the same voter. Other participants said the very existence of biometric technology deterred fraud. Both views can be true: BVVs may have enabled fraud in some ways, and prevented it in other ways.

We also find there were a number of technical mishaps and usability problems that caused cascading issues resulting in voter disenfranchisement. Some technical issues seem—from our perspective—straightforward, such as the fact that election workers had to set the time and date manually on the devices, leading to errors that contributed to 102,012 votes recorded as "out-of-time" and disputed for weeks [3]. Other technical issues seem less straightforward, yet extraordinarily impactful—such as the fact that the devices were not built to the usability requirements of the poll workers.

Contributions Through the expertise of the authors and qualitative analysis of interviews with experts involved in the 2019 Afghanistan election, our data offers insight to the computer security research community into the technical design alignments and misalignments of biometric voter verification, as well as their human causes and consequences. We hope that publishing these results will aid designers and practitioners of future electoral systems (technically and administratively). As we discuss in detail in Section 11, while it is unlikely that there will be a new election in Afghanistan in the immediate future, electoral systems in other countries may share societal, environmental, technical, and adversarial characteristics that mean that they can learn from how and why the use of biometric voter verification both supported and violated electoral goals in Afghanistan in 2019.

2 Related work

Use of biometric technologies in elections Fourty-eight countries have used biometrics in elections in the last 10 years [60], most commonly using fingerprints for voter registration, verification, or identification [106]. Fingerprints are focused on due to their high accuracy [103], uniqueness [93], and difficulty to falsify [25], with even identical twins having distinct fingerprints [62]. Adopting face matching along with fingerprint recognition can further increase biometric systems' accuracy [54]. However, the effectiveness of face matching is contingent upon the quality of the photographs and other checks [106]. Fingerprint verification accuracy is generally measured by equal error rate (EER), a comparison of false rejection and false acceptance rates [63], with the best algorithms having EERs below 0.1% and common algorithms having rates below 1% [22, 107]. Efforts to develop fingerprint biometrics for elections [6, 52, 64, 78, 98] continue to advance but differ significantly from Afghanistan in the

[1] During the Islamic Republic of Afghanistan (2004-2021).

use of Biometric Voter *Registration* [43]. Typically, biometric verification at the polls involves checking the voter's identity against a pre-existing database that includes previously collected biometrics [23]. However, Afghanistan used Biometric Voter *Verification* (BVV) technology to collect biometric data at the polls to later identify duplicate voters, and did not collect biometrics during voter *registration*. We explain the role of BVV in Afghanistan further in Section 6.

Other works related to biometric technology in elections have focused on the social, political, and economic challenges and implications of the use of biometric technology, specifically in non-Western countries [34, 37, 43, 45]. With a focus on Ghana's 2012 election, Debrah et al. found biometric technologies can benefit an election if the technologies are "robust ... [enough] to surmount election management challenges" [35]. Our work builds on this by exploring how election management challenges affected biometric technologies in Afghanistan.

Technical evaluations of election technology Foundational work in the security and privacy community has analyzed the security of various voting machines, finding potentially exploitable vulnerabilities, and usability issues [21, 39, 50, 71, 95, 95, 104, 105]. Both Wolchok et al. and Kohno et al. found issues caused by both the proprietary nature of the systems and an over-reliance on poll workers, both with regards to tasks and trust [71, 104]. Both recommend paper audit trails along with digital records and a move towards more open development. Halderman summarizes the importance of the technical security of voting machines: "*e-voting systems need to be engineered to a level of security quality far greater than that of typical information technology systems, on par with other kinds of critical infrastructure*" [50].

Other work has proposed design principles for voting machines to align with the Help America Vote Act [55]. Gritzalis proposed 15 voting system design principles aligned to US constitutional requirements to ensure that e-voting is free, equal, and secret while simultaneously being transparent and subject to public scrutiny [48]. Similarly, Molnar et al. proposed simple, reliable, and cost-effective ballot storage that is also tamper-evident, history-independent, and subliminal free [79]. Both works propose that voting machines must include audit-ability and traceability without compromising voter confidentiality or being so complex as to exclude voters.

Perceptions of election technology security Prior work has also examined user perceptions of both the security and usability of e-voting. Bederson et al. proposed that usability must be high priority and even 10% of a population having significant concerns about an election technology is unacceptable [17]. Furthermore, Oostveen and Besselaar found that trust in the machine itself is not enough and the people must trust both the officials running the election and the developer of the technology [82]. Expanding on this, de Jong et al. as well as Karola et al. cite the importance of experts' trust and evaluations as a factor in voters' confidence [33, 75]. More recently, Pomers et al. found that both voters and poll workers were more likely to be concerned with usability than with confidence in the system. Interestingly, however, they also found that poll workers were far more likely to be concerned with a lack of training [85]. Our paper builds on these important works about technical security properties of voting machines and perceptions of electronic voting by studying both in practice in Afghanistan in 2019.

Evaluations of electoral ecosystems Complementary to literature about technical security and privacy guarantees of voting machines, and user perceptions thereof, are holistic evaluations of *entire* electoral ecosystems. Bader examines the 2011 Russian legislative election and technology in elections known or perceived to have significant fraud. He found that technology reduced fraud not because of the inherent security, but because it automated vote counting and reduced human involvement [15]. Halderman evaluated challenges during the (US) Antrim County 2020 elections, finding significant failures in pre-election testing and poll workers erasing memory cards, cross-culturally echoing our findings (Sections 7 and 10) [51]. Halderman proposes that both usability and insufficiently defensive software design are at least partially to blame. Both Bader and Haldermann were specifically interested in the validity of the results of the elections and the impact of technology, whereas we are focused on the extent to which the technological processes including procurement, training, and use supported election goals including transparency, credibility, and fairness.

There are also significant works about the 2019 Afghan election, including many that focus on the political ramifications of the results and delays [1, 28, 30]. Johnson examines the 2019 presidential elections, proposing that the biometric technology could have made it simpler for a technologically savvy party to overcome another [66]. A thorough report by the US Special Inspector General for Afghanistan Reconstruction finds that the hasty implementation of technology may have exacerbated fraud and malpractice [94]. While both of these efforts address similar challenges that we identify, neither deeply examines the BVV and its impacts as they relate to the trust and transparency expectations for secure technology in an election. Furthermore, neither effort uses qualitative assessments or draws their conclusions and recommendations from this methodology.

3 Methodology

In order to explore the integration of BVVs into the 2019 Afghan election, we conducted semi-structured interviews with 18 participants familiar with them.

Participant selection and recruitment The lead author worked for the Independent Election Commission (IEC) during the election and leveraged his former professional contacts for recruitment. We recruited 18 individuals engaged in the 2019 Afghan election as part of Afghan civil society (3), the IEC (11), media (1), NGOs (2), and politics (4) (some had multiple affiliations). Four participants had expertise in IT; 13 were Afghan. Participants were ethnically diverse, with all three major Afghan ethnic groups represented. Not all Afghan participants were from Kabul; eight spoke Dari natively, and five spoke Pashto natively (all spoke Dari colloquially). One participant was recruited through another author's network as a member of the US military. The authors contacted potential participants over telephone, email, and E2EE messengers. At the conclusion of each interview, the interviewer asked for referrals to other potential participants.

Interviews We conducted semi-structured interviews from February 2022 until October 2022, with 11 interviews in Dari and 7 in English. The first author conducted all the interviews; the second author participated in four. Before each interview, we sent detailed information about the study and ourselves to participants (Appendix A). At the start of each interview, as part of our informed consent process, we went over the information that we had sent over email, and discussed risk mitigation, the interview medium (end-to-end encrypted video/audio), our data security protocols (encrypted external hard drive only accessible by the interviewers), and any of their safety concerns. Our first question during this consent process was whether they feel safe doing the interview. Our Institutional Review Board (IRB) waived documentation of consent because it would have created additional risk for participants.

We also emphasized that they were free to skip topics or questions. Additionally, we asked permission to record and told them they could ask us to stop recording at any point. Upon their confirmation, we began recording. Our interviews covered the following:

1. Experiences and challenges with **BVV adoption**
2. Political, administrative, legal and social **influences on and consequences of adoption**
3. **Security & privacy issues** during the election with BVVs
4. **Trust** in the electoral system (both personal and public)

We developed our interview protocol through several rounds of revision and a feedback session with an external expert on the 2019 elections who also has expertise in social science. Questions were open-ended (Appendix B has the full protocol) and interviews lasted 60 to 90 minutes. We stopped interviewing when interviews produced no new data, defining thematic saturation [47]. Thematic saturation has limitations in the context of qualitative work [83], and it is indeed possible that if we had not used thematic saturation as a measure of "doneness," or if we had defined it differently, our data could include more or different themes. The external expert later became a participant in the study, and thus knew the protocol in advance; the interview was structured such that knowledge of subsequent questions would be unlikely to influence responses to earlier questions.

Analysis Throughout data collection and analysis, we regularly discussed interviews and wrote memos. The lead author, a native Dari speaker, translated and transcribed all interviews. We then conducted thematic analysis, beginning by open coding and discussing broader themes [40]. The codebook iteratively coalesced through multiple rounds of discussions, open, and axial coding [20].[2] Then, two researchers independently applied the codebook to each transcript and checked their shared understanding, resolving disagreements and updating the codebook. They also regularly talked with a third researcher about their understanding of the codes and emergent themes. They iteratively applied the codebook until no new codes emerged and no new code applications occurred.

Ethical considerations Because the Taliban have threatened leadership of the former Afghan government [57], there is potential for harm to our participants, as well as ourselves and our loved ones, and any future elections that use a similar system. The rest of the team followed the lead of the first author regarding his own safety. However, the team worked with him to consider the possible risks and mitigations. The lead author feels that publishing this work will not substantially *add* to any potential harm he may face. Likewise, the lead author (and team) weighed the potential benefits and risks with this research and concluded that the potential benefits of an eventual publication outweighed the potential risks.

In accordance with the Menlo report, we attempted to maximize benefit and minimize harm, and protect and respect everyone involved with and/or affected by our research [16]. We obtained Institutional Review Board (IRB) approval from our institution. We did not pay participants in order to avoid creating institutional records, following the lead of prior work [31].

All interviews were conducted on Zoom. Despite known security flaws (as with many platforms), Zoom employs E2EE, and participants used their own trusted devices. Most importantly, participants—experts in their own safety within the context of the political situation—felt comfortable using the technology; this follows a standard of safety in prior work [11, 26, 31, 49].

We contacted approximately twice as many individuals as participants; of those who did not participate, some expressed safety concerns due to still being in Afghanistan. Once participants expressed safety concerns, we thanked them for the consideration and ended the conversation.

[2] Codebook available at https://osf.io/2ZQC8/

We present little demographic and recruitment information, and we redact information in quotes when participants discussed their specific role in the election. In doing so, we strove to make it extremely unlikely our participants will be identified from the data in this paper. Additionally, due to the nature of our contribution—i.e., the fact that they were largely discussing either *personal* anecdotes and perceptions, or publicly known events—we do not think that this publication will increase the harms they already face.

We disclosed our findings to the BVV vendor after acceptance and before publication, to enhance the security and usability of future products. We omit the name of the vendor, instead describing them as a European company, to avoid placing undue blame on them as opposed to other decision makers who are not named. We do not attempt to attribute fault to any one party, as an undesirable feature may either be a flaw in specification or implementation, and from our perspective, we cannot know the difference.

Methodological limitations Our research faced significant challenges due to the political shift in Afghanistan in August 2021 [88], when the Taliban took control of the country and disbanded the IEC [84], hindering our access to key IEC authorities, many of whom were either inaccessible or unwilling to participate due to safety concerns or perceived irrelevance to their field. Additionally, the IEC website, which contained valuable information about the election, was taken offline.

The validity of our study depends largely on the credibility of the participants' recollection and the precision of public sources of information; however, recall bias diminishes when participants recall specific events [19,81]. Additionally, different methodologies entirely could have produced new theories or richer results.

Researcher positionality Some of the authors have unique backgrounds that have enabled them to conduct this research. The first author, an Afghan native, was the Director of Information Technology (IT) for the IEC during the 2019 elections. The second author is a member of the US armed forces with tours of duty in multiple theaters, including Afghanistan. The first author's expertise and professional network enabled us to effectively conduct this research by recruiting participants that were directly involved with the adoption and implementation of the BVV technology in the 2019 election. Additionally, the first author's depth of knowledge and experience on this topic made this research possible by enabling deep and detailed conversations about advanced election mechanics with experts. The second author's experience, specifically in Afghanistan, offered valuable geopolitical insights that enriched our interview questions and perspectives.

In conducting our interviews, we were cognizant of the complex interplay of power dynamics, cultural sensitivities, and personal relationships. No researchers interviewed anyone over whom they had current or previous power. Our team's diverse backgrounds—spanning various cultural, linguistic, and professional domains—equipped us to navigate cultural, gender, age, nationality and other dynamics, and we sought to make participants comfortable, with some dynamics mitigated by pre-existing personal relationships.

The other authors have prior experience in security and privacy and HCI research, as well as specifically working with non-WEIRD and vulnerable populations. Some are American, including the senior author, but none have specific professional or personal experience or knowledge regarding Afghanistan. It is, however, relevant to acknowledge that our role as citizens of the country that had a presence in Afghanistan for two decades has certainly affected our development of this research. We have, accordingly, followed the lead of the Afghan first author regarding Afghan politics and history. Additionally, while we acknowledge the significant role the US and other nations have had in Afghanistan, including in the 2019 elections, the focus of this paper is *not* about their influence or the ramifications of it. We focus on telling this story from the Afghan perspective, though the international involvement is an integral part of that story.

4 The 2019 Afghan presidential election: adversarial actors and threats

The zeitgeist prior to the 2019 presidential election created significant threats. Understanding adversarial actors and the threat model under which the 2019 election was planned and conducted is critical to understanding *how* and *why* the electoral system operated (or failed to operate).

Adversarial actors There were significant adversarial actors in the 2019 election including the Taliban, individual politicians, internal threats, as well as foreign actors. The Taliban have historically opposed democratic processes [53], particularly elections [44]. They threatened and killed voters, staff and stakeholders during and after each election, and also attempted to destroy infrastructure [13,58,97]. In an election, political candidates can sometimes evolve into potentially adversarial actors. In previous elections, political candidates were accused of committing fraud including direct interference with the electoral process [9,56,89]. Such accusations continued into the 2019 election [76]. Additionally, there were nonspecific reports of foreign actors [4] with intention to carry out cyber-attacks on the IEC network, also echoed by four participants. While we consider international adversaries out of scope for this paper, their potential interference in an election cannot be ignored [90].

Threats to or during the 2019 election Threats during the election include voter de-anonymization, physical harm to both voters and officials, data compromise, as well as fraud

and corruption. We consider all of these, digital or not, computer security threats due to their influence on how people built and interacted with (or declined to use) the electoral system technology, and because they may occur due to misuse or compromise of computer systems.

Data compromise Adversaries may attempt to compromise data in order to identify voters or remove, add, or change votes. P7 explained: "*suppose adversaries gain access to confidential election-related data, they could sabotage the whole operation and undermine the credibility of the election and harm voters.*" Though our dataset (and news) does not indicate any systemic data compromise in the 2019 elections (contrary to prior elections [38, 67]), participants told stories of small scale data compromise, such as individuals voting multiple times, or data being deleted (discussed in Sections 7 and 8), as well as instances from the past elections.

Voter de-anonymization, physical violence and harm The Taliban disrupted polling with explosions [7], spread violence by threatening to amputate the fingers of voters who participated in the 2019 election [92], and seized BVVs in a potential attempt to realize this threat [68]. While no evidence points to the Taliban actually identifying voters whose biometric data was present on seized BVVs, these threats discouraged voters from voting [68]. As P13 noted, "*during the 2019 election, the Taliban seized some BVVs to identify participating voters. They destroyed the devices when found data is encrypted, which led to the invalidation of votes.*"

In addition to violence against voters, there was violence (and threats of violence) against election workers at all levels, from temporary field workers, to high-ranking officials [68]. Five participants told ten stories of either themselves, other election officials being marked for assassination via social media. Additionally, nine participants reported threats to themselves or their employees. Adversaries also attacked or threatened to attack either the devices or the BVV operators (poll workers) directly. P11 disclosed, "*Several biometric operators who received training were absent on the election day. When reach them out, they said that terrorist groups had identified and threatened them with fatal consequences if they took part in the election process.*"

Infrastructural damage Fourteen participants noted that infrastructure—electric, cellular, internet, and roads—were key supporting components of BVV, and therefore, were sources of vulnerability. Eight participants discussed adversarial attempts to undermine infrastructural integrity, including compromising, damaging and destroying telecommunications, transportation, and electrical infrastructure. P3 explained that "*the insurgent groups... threatened telecommunication companies to shut down their antennas on the election day otherwise they would destroy all their cell towers.*"

5 Electoral goals

Having first discussed Afghanistan's technical, environmental, political, and social contexts, and the threats and adversarial actors active during the election (Section 4), we can now turn to *electoral goals*, which are set *within* and *because of* the aforementioned contexts. This section overviews electoral goals with regards to the integration of BVV technology in the election as viewed by our participants; we return to these goals, and how they were both supported and violated by the implementation of the electoral system, in Sections 7 - 9. These goals are qualitatively drawn from our data and derived from our thematic analysis rather than prescribed by prior research; we do so because our participants discussed electoral goals throughout the interviews, and we find them a useful lens through which to understand biometric voter verification technology in 2019 Afghanistan.

Electoral goal 1: Everyone eligible to vote can cast a vote (enfranchisement). Voters must be able to safely participate and cast votes in the election, and must not be prevented from voting by the electoral system. Votes must also be accurately and securely stored, counted, and transmitted. Voting must also not put anyone at risk of harm, i.e. from the Taliban. Seventeen participants discussed voter enfranchisement, its importance to the election, or the role that it plays with regards to the end state of a successful election.

Electoral goal 2: Each voter may cast at most one vote; no non-voters may cast votes (anti-fraud). Due to Afghanistan's history with systemic and widespread election fraud, preventing, deterring, and detecting fraud was the impetus for the BVVs, in line with the United Nations' specification of a free and fair election [99]. Biometric technology promised to allow each voter to vote once and *only* once. Every respondent discussed fraud, with 15 participants specifically talking about fraud and anti-fraud measures related to the 2019 elections, while the other three respondents discussed the impact fraud and corruption had on the legitimacy of past elections.

Electoral goal 3: Increase public trust in the electoral system. A third goal of the biometric voter verification system was to build public trust in the electoral process—after decades of elections marred with fraud and instability—by providing undeniable accuracy and transparency. Seventeen of our participants highlighted the importance of trust, accuracy, and transparency in the relationship between the public, the election, and technology.

6 Biometric voter verification in Afghanistan

To achieve the goals described in Section 5—voter enfranchisement, anti-fraud, and public trust in the electoral system—despite the history of fraud and the challenging political, social, environmental, and technical contexts (Sections 1 and 4), Afghanistan's **Independent Election Committee (IEC)** partially tested a **Biometric Voter Verification (BVV)** system

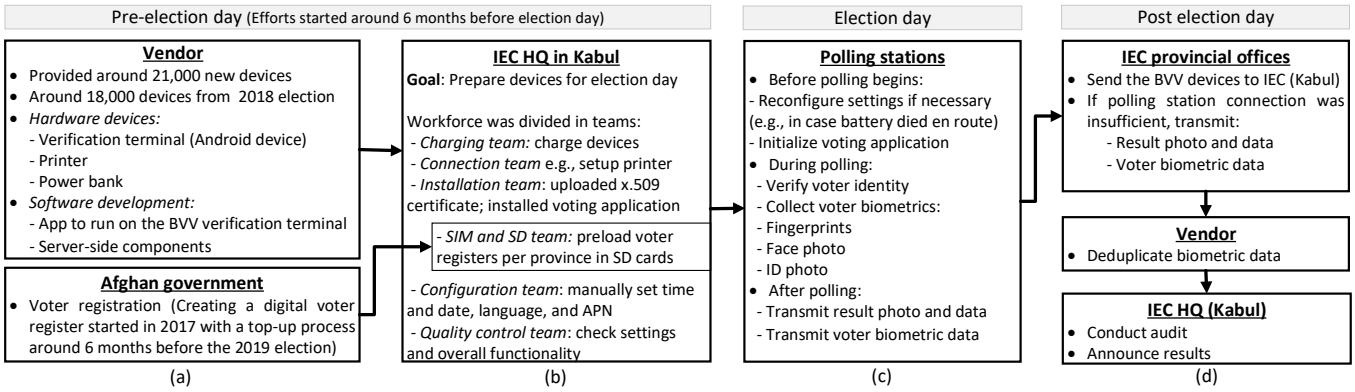

Figure 1: Integration of Biometric Voter Verification (BVV) into the Electoral System – A high-level overview of the BVV ecosystem at several key stages before, during, and after election day.

in the 2018 parliamentary election [45]. The following year—the 2019 presidential election—the IEC were mandated by law to deploy biometric voter verification for all voters [4].

The BVV used in the 2019 Afghan election included a *verification terminal* (a hand-held Android-based device with a camera and fingerprint sensor), a *sticker printer*, and a *power bank*. The printer generated QR codes that were attached to ballots. In this paper, we refer to the Android device as the BVV, and the printer and power bank perform supplementary tasks.

As a basis for understanding how BVVs supported and violated electoral goals, it is important to first understand how the devices were *supposed* to work in the electoral system, as well as what *actually* happened. The following subsections explore the consequences of the sometimes substantial gap between expectation and reality, referring to Figure 1, which summarizes the *intended* BVV development and function. While we cite public data for much of this section, we have also relied upon the first author's professional knowledge as former IEC Director of IT in 2019.

6.1 Pre-election period: Voter registration, BVVs sent to Kabul

Voter registration In Afghanistan, voter registration was historically inconsistent and error-prone because the country did not have a reliable national identification system to connect a person to a fixed address. The first voter registration process was conducted in 2004, giving 12 million people voter cards that included their name, province, and an optional photo. However, it was difficult to track the cards, and faced issues of over-registration and people registering for others [96, 108]. By 2014, the number of distributed voter cards exceeded the estimated number of eligible voters by at least 7.5 million [102].

The IEC therefore started registration anew in 2017, discarding the old registry entirely. From 2017 to 2018, the IEC registered 9.6 million voters (approximately a quarter of Afghanistan's entire population [24]). They used stickers on **Tazkiras** (national IDs) to hold voter information.

> **Reality: The voter registration database was flawed, meaning that not all who wished to cast votes could**. The new registry did not include voter photos and had errors, such as spelling issues with names (P4), duplicates if someone had more than one national ID, and missing voters [94]. Additionally, in 2019, the IEC announced that 400,000 "ghost voters" had been removed from the voter list due to duplication [66]. Nonetheless, nine participants noted that some of these removals led to voter disenfranchisement.

BVVs arrive in Kabul As shown in Figure 1(b), after the vendor had delivered the BVVs to Kabul, the devices required some setup, including charging the BVVs and power banks, installing a certificate from a server in the IEC data center, setting the time and date, installing the *voter verification application* developed by the vendor (via USB), and loading the proper province's voter registration data on SD cards.

The BVVs were then transported to polling centers, e.g., schools. Each polling center had multiple polling stations (booths), with one polling station per 300 registered voters, split by gender. Each polling station was allocated a single BVV, with one extra BVV sent to the entire polling center as a backup. In total, there were 39,000 BVVs deployed to 26,580 open polling stations out of total 29,586 polling stations [2].

> **Reality: Issues with device setup led to voter disenfranchisement**. Some BVVs arrived without charge [65]; others arrived with incorrect time and dates and were not fixed by poll workers [2]. These issues led to voters being unable to vote (on devices without charge) or cast votes being disputed [4].

6.2 Election day: Casting votes

Poll workers, temporary field employees, operated BVVs at each polling station. Before polling began, the poll worker

would activate the BVV app by scanning a QR code on the printed voter list.

When a voter arrived, the poll worker would enter the voter ID number in the BVV to check that the voter is registered for that polling center. Upon successful verification of the voter's ID, the poll worker would direct the voter to a specific polling station to cast their vote. BVVs captured the following information from each voter:

- **Fingerprints** of both index fingers
- A **photograph** of the voter's **face**, taken against a specific backdrop to confirm the location
- A **photograph** of the voter's **Tazkira (national ID)**, including the voter registration confirmation sticker from the most recent round of voter registration

A QR code (produced by the sticker printer) linking to this information was printed on a sticker and affixed to the back of the voter's ballot paper by the poll worker. Additionally, this sticker would contain polling center code as well as date and time of voting.

Moreover, poll workers had an *override* option available as part of BVV app to use at their discretion (P15), but any votes where voter verification was overridden were supposed to get checked by the vendor.

> **Reality: Technical, usability, and database issues prevented some voters from casting votes**. While many voters did cast votes, many encountered issues, from the poll workers incorrectly operating BVVs and either disallowing them to cast votes or deleting their votes, to voter registration that was tied to a different location, to technical issues with the BVVs leading their votes to be disputed or discounted [94]. (We discuss these issues through Sections 7, 8, and 9).

6.3 After election day: Results transmission, counting, and reporting

After election day, the process of reporting results began, including transmission, counting, and fraud detection.

Summarizing results at the polling station After polling closed, poll workers counted all completed biometrically validated ballots, and marked totals on a paper result sheet including the number of votes, used ballots, and votes for each candidate. During this process, several election observers and candidate agents watched, and all signed the paper to indicate the results sheet was accurate. Then, the poll worker took a photo of the results sheet using the BVV, and additionally entered the data from the results sheet into the voting app on the BVV itself. Thus, there were three copies of the summary data on the results sheet: the original paper copy, a photograph of the paper copy, and manually entered text in the BVV application. These three copies were necessary because "*there had been chances that this [results] form would be manipulated in transit. Capturing the result information digitally on the polling station would enable us to detect fraud*" (P2).

Transmission of results and voter biometric data After poll workers had tallied results and triplicated the data, the BVV devices, equipped with SIM cards, were supposed to transmit both biometric and result data using the cell network. Paper ballots and physical BVV devices were transported to provincial offices and on to Kabul.

> **Reality: Some BVVs were unable to transmit data due to a lack of sufficient cellular connection**. Additionally, the Taliban threatened telecommunication companies not to allow their antennas to be used on the election day [18]. Thus, instead, all BVV devices were transported to provincial offices and then to Kabul for data synchronization, though there were technical issues with data transfer [10] which led to political disputes [91].

Checking for fraud at polling station, in transmission, and amongst Kabul staff In order to account for manual error in results tabulation *as well as* adversarial staff members and poll workers or observers, there was a complex system using multiplicative data entry and comparison. Recall that poll workers and observers jointly produced three copies of a results summary: on paper, a photo of the paper on the BVV, and manually entered data on the BVV. To check for fraud at polling stations and in transmission, two randomly assigned staff members first compared the photograph of the results sheet and the data on the BVV; if the two did not match, a separate team corrected the digital file to match the photo, and noted the operators and polling stations involved (a process known as double-blind auditing). Separately, three staff members entered results summary data from each *paper* result sheet (in triplicate to account for manual errors and detect fraud, both at the polling station and amongst the data enterers). Finally, both sets of digital results summary files were compared programmatically. Flags anywhere along this process indicate that the polling station (and/or staff members) must be separately audited through a recount.

Checking for duplicate voters and final vote count Parallel to the above was the deduplication of voters, carried out by the vendor. After the biometric data from the BVVs was transmitted to the servers, the vendor identified duplicate voters based on fingerprints, face photographs, and voter IDs. Following deduplication, IEC removed all the duplicate votes in a special audit program (using the identifier in the form of a QR code to match them) and recounted the remaining votes. Finally, IEC announced the final result of the election as 923,592 (50.64%) for Ashraf Ghani, and 720,841 for Abdullah Abdullah (39.52%), with other candidates trailing [91]. Results were announced five months after the election, in stark contrast to the IEC's planned results timeline of 21 days [12].

7 Support and violation of electoral goal 1: Voter enfranchisement

Due to the gaps between the *design* of the BVV ecosystem, and the *implementation* and *reality* on election day, we are now poised to return to the three election goals from Section 5 and discuss, in depth, the specific technical issues that caused cascading security, privacy, safety, and election legitimacy issues. Throughout this section and the following two, we explore precisely how and why the BVV ecosystem both supported and violated the goals of **voter enfranchisement** (here), **anti-fraud** (Section 8), and **public trust in the electoral system** (Section 9). Our aim is not to judge whether each goal was achieved—and indeed, our participants, electoral experts themselves, often did not agree on high level questions of success or failure. Instead, we argue that through understanding the *technical factors* (including database, hardware, software, and usability issues) that led to both support and violation of the electoral goals, our results can help inform designers and implementers of future electoral systems. We note no factual contradictions between participants, but a healthy contrast in opinions about the support and violation of electoral goals, perhaps driven by participants' diverse professional backgrounds.

We begin with the ***electoral goal 1: Voter enfranchisement***: that everyone eligible to vote is able to cast a vote, that casting a vote has no repercussions for their or others' physical safety, and that their vote, once cast, is properly counted.

7.1 Supported: Voter participation and safety

1,929,333 votes were successfully cast on election day (86,226 later discounted as fraudulent) [14]. Although this number is substantially lower than votes cast in prior elections, votes *were* cast, and *some* of the lower voter turnout could have been to factors unrelated to the BVVs [94]. Four participants felt the very presence of BVVs increased voter participation because it felt safer, e.g., P16, who said that the use of BVVs "*encouraged other areas ...and different population groups to come and... vote for their president because they were hearing that it was safe... because of technology.*"

7.2 Violated: Some voters did not vote due to misalignments with cultural values or concerns about safety

There were multiple reports of people being unable to vote [7], and some constituents declined to vote because they feared for their physical safety. As discussed in Section 4, the Taliban threatened to amputate voters' fingers. In some instances, voters believed that the data recorded by the BVV could be traced back to them. P11 explained that "*people were told that if you participate in the election and register your biometric identities, later the Taliban will access to the database and identify your participation in the election and will cut your fingers. This created a big fear among the public not to participate in the election.*"

Some women could not vote due to the biometric verification process—taking pictures of voters' faces—did not align with their family's cultural values. P11 explained that "*in the conservative and male-dominant society like Afghanistan, men didn't allow their wives or daughters to be photographed.*" P13 added that "*introducing biometrics without having an adequate and proper awareness program in a conservative society was a cultural shock for them.*" Although many Afghan women *did* vote, it is notable that this technology precluded some from voting *by design*.

7.3 Violated: Some voters could not cast votes due to technical issues with BVVs

Distinct from people who *could* have voted but did not are those who *tried* to vote but could not due to technical issues. In addition to the issues with BVVs detailed here, inconsistencies in the voter registry (Section 6.1) meant that some voters were turned away, e.g., in P12's location at least, "*from every three voters, two voters were not in the list, despite they all registered and had valid voter stickers.*"

Unauthoritative timestamps resulted in votes being thrown out When voters cast votes, they were recorded, by the BVV, with the BVV's current timestamp, and any votes recorded before or after the official election operating time interval were supposed to be thrown out as fraud or potential fraud, as per Afghanistan's electoral laws [80]. However, recall that the time and date was set manually by central election workers, and again by some field workers if necessary. Seven participants mentioned that the manual process of setting the date and time resulted in some BVVs having timestamps with the wrong month (P8), entirely incorrect years (P2), or mixed up AM and PM (P2). P2 explained that as required by electoral law, "*those irregular voting were considered as fraud... Some devices dates were setup wrongly in 2029, so we can't say that it is fraud but likely mistake of the person who configured the device*" (P2). P2 continued, explaining that "*there were about 112,000*[3] *voters affected by the device timing issue*" (P2). These votes were part of the set of disputed votes in the post-election period; some were eventually counted [14].

Hardware design issues: power and climate Because "*in most of Afghanistan we didn't have electricity*" (P9), it was critical that the BVVs arrived with enough battery power to last a full day of voting. Four participants, however, said that devices sometimes arrived without charge at the polling centers. Despite devices being charged in Kabul before being shipped to polling centers, "*sometimes those machines, they*

[3] Official sources put the number of out-of-time votes at 102,012 [14].

charged it but they didn't turn it off... [so] sometimes when they opened it [at the polling centers], there was not enough charge" (P9). Sometimes, the battery did not last the entire day, and the devices were slow to charge: "*The BVV's battery couldn't last a full day of continuous use, and while poll workers used power banks, these also charged the device very slowly*" (P15). Complicating matters further, P18 recalled that BVVs became substantially slower in the heat, problematic given some provinces are extremely hot and lacked air conditioning in polling stations. P18 estimated that each voter took approximately three minutes in the extreme heat. At three minutes per vote, in the 10 hour voting period (7am to 5pm), a maximum of 200 people would have been able to vote. Because each polling station had a single BVV, and one polling station had 300 registered voters assigned to them, one third of the registered voters would have been unable to vote. Indeed, P18 said,"*if all the voters had participated in the elections, we would not have been able to collect the votes in the schedule set by the Election Commission, and election would turn to an uproar!*" P18 attributed this slow speed directly to "*the excessive hotness*."

7.4 Violated: Usability issues led to poll workers' mistakes and uncounted votes

Usability issues plagued the BVVs, with poll workers at times struggling to operate the devices due both to training and usability, preventing potential votes. Training did not sufficiently prepare poll workers to use the BVVs, as P12 observed: "*the biometric [poll] workers were not prepared and didn't have the enough knowledge to operate with the BVV devices*." Indeed, nine participants discussed how insufficient training and interface design left poll workers without clear procedures in case of device malfunction. P18 said that "*when several BVV devices stopped working... we did not know what to do... We asked the polling workers to put the memory of the failed device in a new device and resume polling, which later created a big challenge in data integrity.*" Understandably, poll workers who did this were trying to preserve the votes already cast, but likely were unaware that if the SD card was ever removed, a "security" feature of the BVV recorded this, and all votes previously cast on that SD card would not be counted. Corroborating this, P2 remarked, "*there were quite a number of biometric devices ... that displayed zero votes while transferring data to the server; however, there is evidence that people have come and voted in that station.*" We note that a technical design which requires the hardware to be paired and allows users to easily swap SD cards is a data integrity violation, similar to issues from the US 2020 election [51].

These technical oversights not only jeopardized data integrity but were further exacerbated by device usability. Eight participants described the usability of BVVs as complex. P11 noted "*even trained, educated biometric operators struggled with the biometric devices on election day due to the technology's complexity*." The insufficient information provided in the training was compounded by some poll workers' lack of formal education. The United Nations (UN) estimated that approximately 43% of Afghan adults were literate in 2018, a substantial increase over a decade prior [100], with more access to formal education and higher literacy rates in cities such as Kabul, and less in rural areas (education was open to all until 2021 [8]). Five participants mentioned this as an issue. P11 stated, "*The people in the villages were not educated enough to operate with the biometric device, so it was a big challenge.*" Also, P7 noted that "*most biometric workers in remote areas lacked sufficient education or learning skills, and some were too old to grasp the biometric device*."

8 Support and violation of electoral goal 2: Anti-fraud (only one vote per voter)

In tandem with the goal of every eligible voter being *able* to cast a vote was the goal for every voter to cast *only one* vote. Electoral fraud was rampant through Afghanistan's prior decades of elections, and the *deterrence*, *detection*, and *prevention* of fraud was thus a paramount goal in the design of the 2019 election.

8.1 Supported: Deterrence

Fifteen participants said the very existence of BVVs deterred fraud, e.g., P10: "*Afghan citizens knew that this biometric system was put in place ... from that perspective, it was successful ... [in] deterring people from trying to vote multiple times.*" Our data shows that BVV awarded fraud deterrence as the extent of fraud compared to historical numbers of fraudulent votes, e.g., ballot stuffing [42] in past elections, was trivial. P5 noted, "*In earlier elections, we have witnessed agents from warlords and gangsters forcing polling staff to do ballot stuffing in favor of their candidates, but BVV worked as a deterrent for the warlords this time.*"

8.2 Violated: Alleged duplicate votes

Although the BVV ecosystem *did* likely deter, prevent, and detect fraud attempts, it also malfunctioned in ways that may have allowed vote manipulation, though we cannot know the extent.

The IEC mandated that voters register and vote with both index fingers [59]. However, only *valid* fingers were registered, putting the onus on poll workers to ensure voters did not enter a second vote with a different finger because "*there was no mechanism to deny registering the rest of fingers*" (P17). Voters may have been allowed to vote with multiple fingers (and thus cast multiple votes) for multiple reasons, for example, if poll workers were fatigued or simply did not notice which finger the voter used, or if they were physically intimidated or threatened, or if they misunderstood their role (recall

from Section 6 that poll workers could manually override the voter verification process). We thus reemphasize that the technical and user interface designs—through mismatches with poll workers' abilities and understanding of technology, as well as with their intentions—may have allowed poll workers outsized power over the election outcome.

It is also possible that poll workers could also *intentionally* have enabled multiple votes. For example, P11 heard that "*some polling voters moved the biometric verification devices to unknown places on the election day and have attempted to register even their foot's toes in order to print the barcode and vote in the favor of their favorite candidate*." P3 explained that, politically, poll workers were valuable, and "*the candidates ... tried to influence the polling staff who were supposed to work with the biometric devices on the election day by any means of force, threatening, and/or bribe*."

8.3 Supported: Detection of fraudulent votes and vote manipulation

Through the parallel result audit process performed in Kabul (Section 6) and the deduplication of voter biometric data done by the vendor, thousands of votes were marked as suspicious (indicating vote manipulation by staff or in transit), and 86,226 determined, by the vendor, to be duplicate votes [94]. Both are design features of the BVVs: recall from Section 6 that the audit in Kabul was done through triplicate reporting of results (on paper, as a photo on the BVV, and as manually entered data on the BVV). As the deduplication of voter biometric data was also reliant on the BVV device and broader systems, we would be remiss to not discuss the details of biometric deduplication. P10 points out that biometric comparison involves setting a somewhat arbitrary (and likely unbiased) threshold for similarity that determines the number of duplicate fingerprints in the dataset: "*we have no way to fine-tune the system because the fingerprint is divorced from the identity of voters, so we can't go back and find out that our system really detected duplicates or did it just detect people with similar fingerprints.*" The breakdown of the votes invalidated by the vendor is reported as follow: 5,822 votes for having duplicate fingerprints, 47,527 for duplicate faces, 37,006 for duplicate voter numbers, and 5,141 for being uploaded twice, for a total of 86,226 duplicate votes being invalidated (numbers add up to more than 86,226 because 9,270 duplicates matched "multiple criteria") [3].

9 Support and violation of electoral goal 3: Increase public trust in the electoral system

Finally, we address the third overarching electoral goal: increasing public trust in the electoral system itself. Without public trust in the electoral system, the results of the election—and the new political leaders—may not be accepted [69].

We find that public trust was both supported and violated by technical design and implementation of the BVVs. We also find that the support and violation of other electoral goals—voter enfranchisement and anti-fraud measures—affected public trust: 13 participants expressed that experiences and stories of voter disenfranchisement decreased public trust.

9.1 Violated: Lack of public understanding about technical properties

Misinformation about the technical capabilities and (non)guarantees of the BVVs was widespread. Some participants attributed the public's misunderstanding to Afghan officials: P14 said that the "*IEC didn't have enough public awareness programs about the technology and how technology can commit transparency in the election... If you don't have enough knowledge about something you can't trust it.*"

9.2 Violated: Political instability fueled by slow data transmission

Substantial design and implementation issues slowed the transmission of data from BVV devices to servers, contributing to a period of political instability during which the two main candidates argued about who had won, before results were official. Preliminary results were promised in 21 days [87], but it actually took five months [86]. Here, we explore technical issues that contributed to these slow results.

Disputed votes caused by technical issues with BVVs One of the main issues during this period of political instability was the number of disputed votes, publicly reported as approximately 300,000 [94]. Some were cast at the wrong time, or even the wrong date (in the past or future), as discussed in Section 7.3. Others were from polling stations that had a suspiciously high discrepancy between votes cast and voter biometric data collected (should be 0 difference; a very small difference did not trigger a recount) [66].

While recounts on certain polling stations were conducted, the debate around whether to count suspicious votes continued. Significantly, many more of these votes were from the rural districts [66]. While we absolutely cannot speculate about the legitimacy of these votes, we observe the following: all BVVs were configured centrally (Figure 1(b)), including the time and date, but this was a manual process and some were likely misconfigured due to human error. We speculate that batteries in some devices draining on their way to the polling stations (either due to faulty batteries or not being turned off) resulted in a loss of setting, and that poll workers in the field had to reset the time and date for the devices that arrived without the proper time and date.

Poll workers did not promptly tabulate and send results Some poll workers did not follow the prescribed procedures to digitally enter votes and send results to the headquarters using BVV devices after polling concluded. P3 recalled a poll worker who "*did not take the photograph of the result form following the polling process as they were supposed to, which created a big technical challenge in the transmission of data.*" Participants mostly attributed this misuse to poor training and insufficient usability—a mismatch with the digital literacy skills of the workers. P14 recalled that, for some, this caused "*two hours of delay to configure and test the device.*" These issues echo problems that led to political disputes due to the improperly collected votes and voter data—that is, the BVVs did not match poll workers' technical experience.

The BVVs required connectivity that was not available in many rural polling centers In order to meet election timelines [87], the BVVs were designed to transmit results utilizing the cellular infrastructure. However, internet did not exist in many of the rural provinces to cover the polling centers. Indeed, 14 interviewees said that the BVV required infrastructure (e.g., cellular, electrical, internet) was not present.

P14 stated that *"the technology was not compatible with the local conditions of Afghanistan.... Many polling centers didn't have internet coverage in [the province of] Panjshir, so it created a challenge to transmit data over the internet on time from the polling centers."* Additionally, internet and cellular connectivity are dependent on electrical infrastructure. P16 explained: "*some of the challenges that we faced was just giving them enough fuel to run their generators to run their electricity so that they can have the free flowing internet to have communication equipment.*"

9.3 Supported: Improvement over the past

While the BVV ecosystem was certainly flawed, as discussed in other sections, 16 participants actually considered it, *on the whole*, a major step forward—especially with regards to reducing the electoral fraud that plagued prior elections. P6 observed that the 2019 election presented "*a lot of challenges but compared to the 2014 presidential election, there was a big improvement in terms of technology.*" P17 also generally observed that, in their opinion, "*technology is particularly important in improving the election transparency.*"

10 Underlying causes for malfunctions of the BVV ecosystem

Through the preceding discussions of support and violation for the overarching electoral goals (voter enfranchisement, anti-fraud, public trust), we have explored a variety of technical functionality, database, and usability issues. However, our expert participants went beyond specific technical malfunctions and mismatches, discussing the influence of non-technical administrative processes and roles on the *selection*, *design*, and *implementation* of the BVV ecosystem. Through this section, we identify how bureaucratic decisions that may seem non-technical can lead to design decisions and technical implications that have devastating consequences for security, privacy, safety, and election legitimacy. P17 explained: "*No doubt that the technology is particularly important in improving the election process; the selection of technology is more critical. Wrong selection of technology without consideration of the societal and political factors of a country may jeopardize the entire process.*"

Politicians and decision-makers were not well-informed about biometric and electoral technology Participants expressed that the election leadership were not always able to make informed decisions because they lacked foundational technical knowledge and appropriate technical counseling. P7 described that "*they thought that technology can make magic and can miraculously solve all the problems*." In a particularly egregious example, P10 recalled a meeting with an official who thought the BVV would know who they intended to vote for: "*he said, 'go to the thing, and you put your fingerprint on it, and the machine will already know how to vote'... in his mind he jumbled together biometrics and electronic voting and mind-reading, all of those system that somehow did magic for him.*" More generally, P9 explained that "*they thought if we look at the other countries, if we use technology in the election, maybe it will increase transparency and it will increase the speed of tally, votes and everything. But they have overlooked a few things in Afghanistan*."

The power imbalance between the vendor and the IEC regarding control of data Seven participants expressed that the vendor had too much power over electoral data, and the Afghan agency deploying the system (the IEC) had too little power (though we note that some of our participants are former IEC employees, and none represent the vendor). This control was not limited to the development of the software and hardware and deduplication of voters—P6 described that the vendor was also responsible for "*the configuration of the server [and had] access [to the] data*." P6 pointed out that this control was "*a ... national security issue because the election of a country was being managed by a company* outside *of the country.*" Control of electoral data being outside the country could either benefit or harm the security of the data, depending on the adversarial actors; P6 was "*not comfortable ... that a technology vendor, a commercial company has so much influence over the election technology.*" Compounding these issues was limited communication with the vendor during the actual election period: "*the company agreed to provide 24 hours service seven days a week*" (P15) but "*IEC and [the vendor] were communicating effectively with each*

other through emails only three days a week due to time and calendar differences between Afghanistan and [Europe]. If a technical problem would have arisen on Thursday, IEC had to wait four days until Monday to get a response..." (P4).

The lack of a consistent and pervasive national census obstructed the design of the electoral system Five participants explained how the absence of a national census inhibited the design and implementation of the BVV ecosystem. P8 said: "*if we want to change the election, we need to have an infrastructure in place, clear statistics, clear census in the country, without a clear census we can't have elections in Afghanistan.*" They went on to explain that one of the challenges in conducting such a census was political in nature, rather than purely logistical: "*the reason that we don't have census because there is a political aspect to it as well, because over the years many ethnic groups tried to have these narrative of majority, minority things ... so if we have a clear census that might change their narrative.*"

Vendor selection was influenced by politics Nine participants said that political parties had an inappropriate role in the selection of the vendor. P2 described that rather than a bidding process with multiple vendors,"*the choice of the vendor was initially proposed in a meeting during 2018 by Central Statistics Office and political parties seemed to agree with it.*" The incumbent "*supported this idea*" because the person suggesting it "*was from a trusted circle of the president*" (P17). P12 described the process as corruption: "*technology could work better if the corruption in the government was not a big issue. The president selected a company to implement biometric technology in Afghanistan that had no working background in the election area.*" While there may have been reasons "*due to shortage of timing [they] opted to go with the same vendor in 2019*" (P2), P7 felt that the vendor was selected without sufficient research, as an abuse of power: "*They have misused their power to impose the technology on IEC without researching it from all aspects.*" P8, P15, and P18 also said that the vendor was insufficiently familiar with both Afghanistan and electoral technology.

The limited timeframe to implement and deploy BVVs allowed bugs, design misconfigurations, and procedural errors to go unnoticed Ten participants discussed how the short amount of time between the 2018 and 2019 elections precluded thorough testing of the technology itself. P17 said "*the devices and the rest of the system arrived [from the vendor] exactly 28 days before the [2019] election.*" P17 continued, explaining how the short timeline led to usability issues that eventually violated electoral goals: "*We did not even have enough time to train staff to configure and prepare the devices to dispatch them to the provinces*" (P17). P15 estimated that six months would be appropriate for a testing period (rather than the 28 days that the IEC had with the updated devices): "*I wouldn't say it was fault of the IEC because I've seen a process of testing, auditing and certification. It takes at least six months. The commission didn't have this six months*" (P15).

11 Discussion and conclusion

Our findings show computer systems, database, and usability issues that marred the 2019 Afghan election, driven in part by administrative, political, and bureaucratic issues. Still, there was no consensus among our participants on whether the election was a "success" or "failure," or even whether the addition of the biometric technology was a "success" or "failure." Although our research uncovered flaws that disenfranchised voters and, to a lesser extent, allowed fraud and decreased public trust in the democratic system itself (Sections 7- 9), *some* participants felt there was a sense of *good enough for now*, given the history of extensive fraud.

While our research provides unique and broad visibility into the procedures and practices of adopting new election technology, we cannot say whether the integration of the biometric voter verification technology in the 2019 Afghan election was indeed "good enough for now" or "successful." Instead, we hope our research can provide a foundation for future conversations *before* a new election technology is adopted. It is unlikely that Afghanistan will hold elections while the Taliban are in power [74, 84], and thus the most direct application for our recommendations—for usable, trusted, safe, and secure elections *in Afghanistan*—is *currently* irrelevant, and so we cannot speculate about the context during Afghanistan's *next* election. However, biometric technologies are being increasingly adopted in electoral systems [5] and so it is important to understand how, why, and *whether* such a technology can be appropriate for any given country's democratic processes. Here, we offer high level recommendations to practitioners and designers of elections. These lessons echo general best practices, but, to use P9's words, it is absolutely critical to not "*overlook a few things*." That is, practitioners should draw lessons from our work based on the cultural, religious, environmental, historical, infrastructure, technical, political, societal, and adversarial characteristics that their country shares with Afghanistan:

- **Plan ahead:** It is important to ensure enough time for testing, evaluation, and modification of technology, as well as for training workers and physically deploying the technology. Election workers in Afghanistan had less than one month to deploy the technology, and the usability mismatch between some poll workers and the BVV technology suggests that training was insufficient (although we strongly recommend designing *first* to minimize usability gaps, and *second* to then fill those gaps with suitable training, aligning with human-centered design principles [29, 41, 77]). Our data also reveals other issues that might have been revealed

with more thorough time for evaluation cycles. Because testing, especially *in situ*, is certainly not an easy task, nor is it always possible, given that delaying an election is often not possible, we particularly emphasize its importance and the potential that sufficient time to test, certify, evaluate, modify, deploy, and integrate technology has to positively impact the credibility and integrity of an election.

- **Have full visibility and be cognizant of biases:** Our research demonstrates the impact limited technical knowledge has on the ability of decision makers to make informed decisions, e.g., the belief in Afghanistan that technology will create a trustworthy and trusted election, the IEC's forced reliance on the vendor for technical support, etc. It is important to have full visibility, understanding, and awareness. For example, it may benefit decision makers to have access to the underlying code, understand the abstract details of its functionality, be aware of any vulnerabilities and consequences that technology may have. Fulfilling this recommendation may be extraordinarily difficult given the limitations of human expertise and technical resources, but a decision-making team that holds the appropriate technical, legal, political, and sociological knowledge is critical to making both high and low level electoral technology design decisions. When decision makers don't have such expertise, we encourage hiring third party experts as guides, as well as independent testing and certification. Additionally, while it is impossible to be completely apolitical, decision-makers must be aware of their own biases, define goals ahead of time, and select the best technology for those goals [70].

- **Consider the context:** Our research demonstrates the impact of designers not fully accounting for the local deployment context. Consequently, it is important to understand and anticipate the specific challenges, cultural values, infrastructural limitations, and user educational level and expectations prior to deploying election technology. Our data shows numerous misalignments with local context, from the very use of facial biometrics disenfranchising some women, to the expectation that the BVVs would use the cell network to transmit data when there was no cell network present at some polling stations. While other work in this field has explored the importance of local context on the adoption and use of technology [31], our work additionally shows how it can be rife with tensions: for example, the very use of biometrics enfranchised some voters and disenfranchised others. We recommend, thus, that designers deeply understand the complexities of local cultural, environmental, social, political, and infrastructure context, and minimize tensions through design. Some tensions may be impossible to resolve fully through design, and hence it may be helpful to use ethics modeling to comprehensively surface and then navigate those tensions [70].

These recommendations apply to everyone working on an election—but we observe that they are most important for decision-makers with the power to affect vendor selection, to allow sufficient time for design, implementation, and deployment, and to gather complete contextual information. Having sufficient time, visibility, and context are important not only for a trust*worthy* election but also for a trust*ed* election.

Accordingly, once irreversible decisions are made, practitioners with less power over electoral design may find themselves working in suboptimal conditions, yet may still be able to both adhere to the above recommendations, and make further decisions within their purview. For example, a developer or manager with subject matter expertise may learn that designs do not adhere to cryptographic best practices, and should be able to affect change through the proper channels.

We strongly encourage practitioners to systematically consider how the application of certain design decisions *at scale*, *within the threat model of an election*, and *within the specific local context* affect the security properties of the "general case" of any given design decision. We include the following topics as starter conversations, inspired by speculative conversations within our research team during this work: linking biometric data to votes with sufficient theoretical and practical anonymity guarantees given the adversaries and size of the dataset; resiliency to network failure, disruption, and nonexistence; supply chain control and hardware security; poll worker training, manual labor, and repetitive processes as a source of potential error or insecurity.

Epilogue We conclude this paper with the *aftermath* of the 2019 election. By August 2021, following the U.S. military's exit after 20 years of presence in Afghanistan, the government collapsed and the Taliban took over Kabul [72], which consequently resulted in the dissolution of the IEC and its entire framework [84]. We cannot know what would have happened if the technology in the 2019 election had fully supported the electoral goals. Yet, achieving these goals might have paved the way for a different trajectory for the Afghan society.

Acknowledgements

We are grateful to Dalton Brucker-Hahn and Kailani Jones for their guidance in interview protocol development, and to Jeremy Epstein, Collins Munyendo, Alison Simko, and Karl Weintraub for their feedback on a draft of this paper. We also thank our anonymous reviewers and shepherd for their thoughtful and constructive comments. This work was supported by the National Science Foundation (NSF) Awards 2143393 and 2205171. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

References

[1] A. Y. Adili. Afghanistan's 2019 elections (31): A review of the disputed presidential election and its aftermath. [link], (09/2020).

[2] A. Y. Adili. Afghanistan's 2019 Election (24): Disputed recount, threats not to accept results, and some interesting new data. [link], (11/2019).

[3] A. Y. Adili and J. Bjelica. Afghanistan's 2019 Election (23): Disputed biometric votes endanger election results. [link], (11/2019).

[4] A. Y. Adili, J. Bjelica, and T. Ruttig. Afghanistan's 2019 Election (21): BVV devices and a delay in announcing preliminary results. [link], (10/2019).

[5] O. S. Afolabi. Biometric technologies, electoral fraud and the management of elections in Nigeria and Zimbabwe. *Strategic Review for Southern Africa*, 42, 2020.

[6] S. Agrawal, P. Majhi, and V. Yadav. Fingerprint recognition based electronic voting machine. In *STET-2014*, 2014.

[7] Al Jazeera. Afghanistan presidential election: All the latest updates. [link], (09/2019). Web Archive version from 3/7/2021 on 8/19/2023.

[8] Al Jazeera. Taliban says women banned from universities in Afghanistan. [link], (12/2022).

[9] A. V. Alambra. Top UN envoy: interference by officials in electoral process must stop. [link], (07/2009).

[10] S. Amiry. IEC: 85% biometric data processed, 1.7m votes so far. [link], (10/2019).

[11] M. M. Archibald, R. C. Ambagtsheer, M. G. Casey, and M. Lawless. Using Zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. *SAGE International Journal of Qualitative Methods*, 2019.

[12] Ariana News. IEC national tally center starts functioning. [link], (10/2019).

[13] Associated Press. Taliban attack kills 8 election officials in Afghanistan. [link], (06/2019).

[14] A.Y. Adili. Afghanistan's 2019 Elections (29): A statistical overview of the preliminary results. [link], (02/2020).

[15] M. Bader. Do new voting technologies prevent fraud? Evidence from Russia. In *EVT/WOTE*, 2014.

[16] M. Bailey, E. Kenneally, D. Maughan, and D. Dittrich. The Menlo Report. *IEEE S&P*, 10(02), 2012.

[17] B. B. Bederson, B. Lee, R. M. Sherman, P. S. Herrnson, and R. G. Niemi. Electronic voting system usability issues. In *ACM CHI*, 2003.

[18] J. Bjelica and T. Ruttig. Afghanistan's 2019 election (11): A first look at how e-day went. [link], (09/2019).

[19] N. M. Bradburn, L. J. Rips, and S. K. Shevell. Answering autobiographical questions: The impact of memory and inference on surveys. *Science*, 236(4798), 1987.

[20] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 2006.

[21] K. R. Butler, W. Enck, H. Hursti, S. E. McLaughlin, P. Traynor, and P. D. McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting Systems: Reflections on Project EVEREST. volume 8, 2008.

[22] R. Cappelli, D. Maltoni, et al. Fvc-ongoing: On-line evaluation of fingerprint recognition algorithms. In *International Biometric Performance Conference*. NIST, 2010.

[23] S. Chatterjee, I. S. Jogalekar, and K. Lavanya. E-voting: Portable fingerprint-based biometric device for elderly and disabled people. In *Cyber-Physical System Solutions for Smart Cities*, pages 132–142. IGI Global, 2023.

[24] CIA. Afghanistan. [link]. Accessed : September 18, 2023.

[25] S. A. Cole. Is fingerprint identification valid? Rhetorics of reliability in fingerprint proponents' discourse. *Law & Policy*, 28(1), 2006.

[26] D. Conway, R. Taib, M. Harris, K. Yu, S. Berkovsky, and F. Chen. A qualitative investigation of bank employee experiences of information security and phishing. In *SOUPS*, 2017.

[27] C. Cookman. Afghanistan presidential election 2019. [link], (08/2020).

[28] C. Cookman. *Assessing Afghanistan's 2019 Presidential Election*. United States Institute of Peace., 2020.

[29] S. Costanza-Chock. *Design justice: Community-led practices to build the worlds we need*. The MIT Press, 2020.

[30] T. Dadabaev. Afghanistan in 2019: Trump's "walk away" strategy and the future of post-election afghanistan. *Asian Survey*, 60(1), 2020.

[31] A. Daffalla, L. Simko, T. Kohno, and A. G. Bardas. Defensive Technology Use During the 2018-2019 Sudanese Revolution. *IEEE S&P*, 20(2), 2022.

[32] M. S. Darnolf. Reducing voter fraud in Afghanistan. Technical report, USIP, 2017.

[33] M. De Jong, J. Van Hoof, and J. Gosselt. Voters' perceptions of voting technology: Paper ballots versus voting machine with and without paper audit trail. *Social Science Computer Review*, 26(4), 2008.

[34] M. Debos. Biometrics and the disciplining of democracy: technology, electoral politics, and liberal interventionism in Chad. *Democratization*, 28(8), 2021.

[35] E. Debrah, J. Effah, and I. Owusu-Mensah. Does the use of a biometric system guarantee an acceptable election's outcome? Evidence from Ghana's 2012 election. *African Studies*, 78(3), 2019.

[36] M. A. Dinakhel, S. Z. Bakhshali, and I. Ali. An Overview of Political Suppression of Legal Political Parties in Afghanistan: 1940-2010. *Khairulummah*, 2(02), 2023.

[37] J. Effah and E. Debrah. Biometric technology for voter identification: The experience in Ghana. *The Information Society*, 34(2), 2018.

[38] European Union Eleciton Assessment Team. Islamic Republic of Afghanistan: Final Report: Presidential Election. [link], (03/2014).

[39] A. J. Feldman, J. A. Halderman, and E. W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. Center for Information Technology Policy, Princeton University, 2006.

[40] J. Fereday and E. Muir-Cochrane. Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme devlop. *International Journal of Qualitative Methods*, 5, 2006.

[41] B. Friedman. Value-sensitive design. *Interactions*, 3(6), 1996.

[42] C. Gall. In Afghan Election, Signs of Systemic Fraud Cast Doubt on Many Votes. [link], (08/2014). The New York Times; accessed through web.archive.org.

[43] A. Gelb and A. Diofasi. Biometric Elections in Poor Countries: Wasteful or a Worthwhile Investment?: Biometric Elections in Poor Countries. *Review of Policy Research*, 36, 2019.

[44] A. Giustozzi. The Taliban and the 2014 presidential elections in Afghanistan. *Conflict, security & development*, 16(6), 2016.

[45] A. Goldstein. Flawed biometric rollouts in emerging economies: Evidence from Jamaica, Afghanistan, and Kenya. *Breakthroughs in Digital Biometrics and Forensics*, 2022.

[46] J. Goldstein. E.U. confirms wide fraud in Afghan presidential runoff election. [link], (12/2014). The New York Times; accessed through web.archive.org.

[47] J. Green and N. Thorogood. Analysing qualitative data. *Principles of social research*, 2005.

[48] D. A. Gritzalis. Principles and requirements for a secure e-voting system. *Computers & Security*, 21(6), 2002.

[49] M. Gutfleisch, J. H. Klemmer, N. Busch, Y. Acar, M. A. Sasse, and S. Fahl. How Does Usable Security (Not) End Up in Software Products? Results From a Qual Interview Study. In *IEEE S&P*, 2022.

[50] J. A. Halderman. Practical attacks on real-world e-voting. *Real-World electronic voting: Design, analysis and deployment*, 2016.

[51] J. A. Halderman. The Antrim county 2020 election incident: an independent forensic investigation. In *USENIX Security*, 2022.

[52] K. Hasta, A. Date, A. Shrivastava, P. Jhade, and S. Shelke. Fingerprint based secured voting. In *IEEE ICAC3*, 2019.

[53] C. Hirschkind and S. Mahmood. Feminism, the Taliban, and politics of counter-insurgency. *Anthropological Quarterly*, 75(2), 2002.

[54] L. Hong and A. Jain. Integrating faces and fingerprints for personal identification. *IEEE transactions on pattern analysis and machine intelligence*, 20(12):1295–1307, 1998.

[55] HR 3295 - 107th Congress (2nd Session). Help America Vote Act. [link], (01/2007).

[56] C. B. Hull. Analysis: Are lawmakers or lawbreakers winners of afghan poll? [link], (09/2010).

[57] Human Rights Watch. Afghanistan: Taliban Threaten Revenge Killings. [link], (03/2022).

[58] Human Rights Watch. Afghanistan: Taliban's Criminal Attacks on Election Activities. [link], (09/2019).

[59] Independent Election Commission of Afghanistan. IEC Decision for Using BVV Devices, 2018. Web archive version: [link].

[60] International Idea. ICTs in Elections Database: Is the biometric data used in voter identification at polling stations? [link]. (9/2023).

[61] A. Jackson and F. Weigand. The Taliban's war for legitimacy in Afghanistan. *Current History*, 118(807), 2019.

[62] A. K. Jain, P. Flynn, and A. A. Ross. *Handbook of Biometrics*. Springer Science & Business Media, 2007.

[63] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Transactions on CSVT*, 14(1), 2004.

[64] A. Jamkar, O. Kulkarni, A. Salunke, and A. Pljonkin. Biometric voting machine based on fingerprint scanner & Arduino. In *IEEE ICCT*, 2019.

[65] W. Jin. Why are Afghan election results delayed again? [link], (11/2019).

[66] T. Johnson. The 2019 Afghan Presidential Election: An Assessment of Problematic Processes and Results. *Afghanistan*, 4.1 (2021), 2021.

[67] T. Johnson and R. J. Barnhart. An Examination of Afghanistan's 2018 Wolesi Jirga Elections: Chaos, Confusion and Fraud. *Journal of Asian Security and International Affairs*, 7(1):57–100, 2020.

[68] A. Karimi. Surveillance in Weak States: The Problem of Population Information in Afghanistan. *International Journal of Communication*, 13, 2019.

[69] N. Kerr and A. Lührmann. Public trust in manipulated elections: The role of election administration and media freedom. *Electoral Studies*, 50, 2017.

[70] T. Kohno, Y. Acar, and W. Loh. Ethical Frameworks and Computer Security Trolley Problems: Foundations for Conversations. In *USENIX Security*, 2023.

[71] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *IEEE S&P*, 2004.

[72] Z. Laub and L. Maizland. The U.S. War in Afghanistan. [link], (09/2022).

[73] F. Lehoucq. Electoral Fraud: Causes, Types, and Consequences. *Annual Review of Political Science*, 6(1), 2003.

[74] C. B. Lombardi and A. F. March. Afghan Taliban Views on Legitimate Islamic Governance. [link], (02/2022).

[75] K. Marky, P. Gerber, S. Günther, M. Khamis, M. Fries, and M. Mühlhäuser. Investigating State-of-the-Art Practices for Fostering Subjective Trust in Online Voting through Interviews. In *USENIX Security*, 2022.

[76] M. Mashal. Afghan Vote Crawls Toward Crisis, With No Results After 2 Months. [link], (11/2019).

[77] A. Mathie and G. Cunningham. From clients to citizens: Asset-based community development as a strategy for community-driven development. *Development in practice*, 13(5), 2003.

[78] K. Memon, D. Kumar, and S. Usman. Next generation A secure e-voting system based on biometric fingerprint method. In *IPCSIT*, 2011.

[79] D. Molnar, T. Kohno, N. Sastry, and D. Wagner. Tamper-evident, history-independent, subliminal-free data structures on prom storage–or–how to store ballots on a voting machine. In *IEEE S&P*, 2006.

[80] National Legislative Bodies/National Authorities. Afghanistan: Election Law (2016) [Afghanistan]. [link], 2016.

[81] J. S. Olson and W. A. Kellogg. *Ways of Knowing in HCI*, volume 2. Springer, 2014.

[82] A.-M. Oostveen and P. v. d. Besselaar. Security as belief user's perceptions on the security of electronic voting systems. In *Electronic voting in Europe-Technology (ESF TED)*. Informatik eV, 2004.

[83] M. O'Reilly and N. Parker. 'Unsatisfactory Saturation': a critical exploration of the notion of saturated sample sizes in qualitative research. *SAGE Qualitative Research*, 13(2), 2013.

[84] C. Poalzai Ehsan. Taliban says 'no need' for Afghanistan's election commission and peace ministries. [link], (12/2021).

[85] J. Pomares, I. Levin, and R. M. Alvarez. Do Voters and Poll Workers Differ in their Attitudes Toward E-voting? Evidence from the First E-election in Salta, Argentina. In *USENIX EVT/WOTE*, 2014.

[86] E. Popalzai, M. Popalzai, and I. Kottasová. 5 months later, Ashraf Ghani declared winner of Afghanistan's presidential election. [link], (02/2020).

[87] RadioFreeEurope/RadioLiberty (REF/RL). Afghan Presidential Election Results Announcement Delayed. [link], (10/2019).

[88] D. Rajmil, L. Morales, T. Aira, and M. C. Valles. Afghanistan: A Multidimensional Crisis. *Peace Review*, 34(1), 2022.

[89] Reuters Staff. Afghanistan sacks 12 election officials amid fraud investigation. [link], (02/2019).

[90] K. P. Riehle. Winners and losers in Russia's information war. *Intelligence and National Security*, 36(7), 2021.

[91] T. Ruttig. Afghanistan's 2019 Elections (30): Final results ... and parallel governments? [link], (02/2020).

[92] A. Q. R. Sediqi. The Taliban cut off his finger for voting. He defied them again. [link], (09/2019).

[93] M. Sharif, M. Raza, J. H. Shah, M. Yasmin, and S. L. Fernandes. An overview of biometrics methods. *Springer Handbook of Multimedia Information Security: Techniques and Applications*, 2019.

[94] Special Inspector General for Afghanistan Reconstruction. Elections: Lessons from the U.S. Experience in Afghanistan. [link], (02/2021).

[95] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman. Security Analysis of the Estonian Internet Voting System. In *ACM CCS*, 2014.

[96] A. F. Tookhy. Legislature and legislative elections in Afghanistan: An analysis. [link], (07/2020).

[97] A. Tuerk. Afghan Polls Close As Voters Face Taliban Threats. [link], (09/2019).

[98] B. U. Umar, O. M. Olaniyi, L. A. Ajao, D. Maliki, and I. Okeke. Development of a fingerprint biometric authentication system for secure electronic voting machines. 2019.

[99] UN Human Rights Committee. CCPR General Comment No. 25: Article 25 (Participation in Public Affairs and the Right to Vote), The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service, (07/1996). Rev: [link].

[100] UNESCO. The right to education: What's at stake in Afghanistan? A 20-year review. Technical report, (09/2021). Report at [link].

[101] USAID. USAID Support for Afghanistan's 2014 Elections: Rapid Assessment Review, (08/2015).

[102] M. van Bijlert. What to Watch in the Elections (1): Voter Registration. [link], 2014.

[103] C. L. Wilson, R. A. Hicklin, M. Bone, H. Korves, P. J. Grother, B. Ulery, R. J. Micheals, M. Zoepfl, S. Otto, and C. I. Watson. Fingerprint vendor technology evaluation 2003: Summary of results and analysis report, 2004. US Department of Commerce, NIST: [link].

[104] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp. Security analysis of India's electronic voting machines. In *ACM CCS*, 2010.

[105] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman. Attacking the Washington, D.C. Internet Voting System. In *Financial Cryptography and Data Security*, 2012.

[106] P. Wolf, M. Saneem, and T. Zorigt. Introducing Biometric Technology in Elections, 2017. Full report available at [link].

[107] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli. Security and accuracy of fingerprint-based biometrics: A review. *Symmetry*, 11(2), 2019.

[108] M. Yard. Civil and voter registries: Lessons learned from global experiences. *Report of the International Foundation for Electoral Systems (IFES). Washington, DC: IFES*, 2011.

A Appendix – Consent information sent to participants before interview

We are academic researchers in security and privacy from the United States of America that want to understand the role of technology in the Afghan election system. We are not working for any government entities. Specifically, we want to understand where technology proved useful and where it fell short during the elections in Afghanistan. We want to understand the technology needs of election systems. Our goal is to present these technology-related needs to our community. This enables our community to work on providing better technological solutions for elections. Information about the research project/study:

- Our ultimate **purpose** is to develop better technical tools and communication mechanisms for elections.
- This is a **research** project conducted at the [Institution & PI].
- Activities and **procedures** to be followed:
  - **Duration**: Around one hour (an interview in English or Pashto about technologies used in the Afghan elections)
  - Audio recorded interview: YES or NO (it's your choice)
  - Recording the interview is OPTIONAL and you can ask us at any time to stop the recording. If you desire, your entire recording will be deleted at that point.
  - Name and specific personally identifiable information will not be recorded.
  - Recording the interview will allow us to focus only on talking with you, and having your exact words will greatly increase the quality of the data (recordings will not be shared outside the research group).
  - Recording will be hosted on the infrastructure of the [Institution name]. Access will be restricted to the research team and the recordings will be password protected.
  - Only the researchers that are part of this study will transcribe the interviews.
  - To mitigate future **risks**, your identifiable information will not be used or distributed for future research studies even if your identifiable information is removed.
  - It is possible, however, with internet communications, that through intent or accident someone other than the intended recipient may see your response.
  - In case you want to withdraw from the interview, your recording and the corresponding interview notes will be removed from our records.
- Publications will NOT include personally identifiable info.
- We will give you the option to review a draft of our research paper before it is published. Though we will remove all information we see as identifying, you may ask us to remove any additional information you feel may identify you.
- This study is **voluntary**: You have the option to refuse to answer any question. You have no obligation to participate and you may discontinue your involvement at any time.
- Although participation may not **benefit** you directly in the first instance, the information obtained from the study will help us gain a better understanding of how to develop better security and privacy solutions for election systems.
- Even though personally identifiable information will be removed, information about protests may be considered sensitive and, if this information is released and tied back to an individual, it could damage that individual's financial standing, employability, reputation, or cause social stigmatization or discrimination.

Participation in this effort indicates your willingness to take part in this study and that you are at least 18 years old. Should you have any questions about this project or your participation in it you may ask [PI name] [Institutional email]. If you have any questions about your rights as a research participant, you may call the Human Research Protection Program at [phone #] or [email].

Audio recording: YES NO

B Appendix – Interview protocol

Our semi-structured interviews varied slightly based on each participant's background. While all participants were asked questions in line with their expertise, participants with a comprehensive background of IT were queried more extensively to get more technical details. The interview protocol was influenced significantly by [31].

Consent Process:

- Introduction to researchers and research objectives.
- Oral overview of the consent form, covering:
  - Expected interview duration.
  - Voluntary nature of interview recording.
  - Ask to stop the recording at any point.
  - Assurances of anonymity and data protection.
- Any question, before we start the interview?

Preliminary Remarks (Post-Consent):

- Remind participant on maintaining their anonymity and confidentiality to share any stories freely with us.
- Confirm with participant to start the interview.

Interview Sections and Questions: Our question were structured into specific sections to comprehensively cover various aspects of electoral technologies. Each section was designed to include questions addressing security and privacy, and we encouraged participants to share their personal experiences and stories. Depending on their responses, we further explored each subsequent section. We also tried to skip some sections if participants didn't have any information on that or preferred not to answer.

Experience and Challenges:

- Which elections did you participate/have role in?
- What technologies did you experience during the 2019 election?
- How did you see technology being used during the election?
- What was your perspectives on adoption of biometrics technology in the 2019 election?
- What did you see as the challenges/benefits of technologies in 2019 Afghan election?

Perceived Political Influence:

- 2019 Afghan election had a lot of political tension, how, in your opinion, did the technology used in the 2019 election impact the political tension?
- Do you have any story that politics influenced selection or use of technology in the election 2019 to share with us?
- What impact, in your opinion, can political parties have influence on the improvement/impediment of electoral technology?
- If you could change the election process, how would you?

Societal and Administrative Impact:
- How did you see influence of non-technical staff, officials, stakeholders, observers in selection or use of technology?
- What organizations impacted the selection of technology?
- How did you see sharing information about election technologies with public during the 2019 election?
- What technology did you use to receive public information concerning the elections and its technologies?
- If social media was used, what type of information were posted about technology and infrastructure?
- How did you see the influence of social media on the election process and its technologies?

Relation to Training:
- Did you receive any training for using technology in the election?
- If yes, how did you use that training in the 2019 election? Was the training helpful or unhelpful? Why?

Trust Factors:
- What technologies are you aware of that were used in the Afghan elections prior to 2019?
- Did you see any improvement in the 2019 technical electoral systems in compare to technologies used in the past?
- Did you trust or distrust technology used in the election? Why?
- Did people trust the electoral technologies?
- Did technology improve credibility of the 2019 election?
- How can technology improve the credibility of future Afghan elections?

Voter Registration:
- What do you know about voter registration and voter lists?
- What technology were used in the voter registration? Was it effective? Why?
- What security approaches were in place to protect voter's data against manipulation?

Biometric Voter Verification:
- What brand, type, and model of biometric voter verification devices were used in the 2019 election?
- What hardware technology was used on the server-side?
- How the data were transferred from BVV devices to the Server?
- How does IEC check the integrity of data among BVV devices and the server while transferring the data?
- What procs were used to securely transfer the data to the server?
- How is the data stored on the BVV device and the server? What format? what type? Was it encrypted? What was the overall size? Who accessed the data?
- What security mechanisms were adopted to protect the voters' biometric data?
- How did the deduplication work?

Result Tabulation and Audit:
- What was the process to tabulate the result during the 2019 election (With all technical and security details)?
- What technologies are used during the result tabulation?
- How did you eval. the result tabulation process in the election?
- Were you involved in the audit process during the 2019 election? If yes, what IT systems were involved during the audit process? How did you see the process?

Result Transmission and Reporting:
- What data and how transmitted from the polling centers/stations particularly from places with no internet coverage?
- Who was permitted to transmit the data? How was the data received in the server side? What security factor was involved during transmission?
- What was the process for reporting results?
- What security procedures were leveraged to avoid data manipulations by attackers after the data was posted on the website?

Advanced Technical:
- What IT infrastructures were used in the headquarter and provinces in the 2019 election to deploy BVV?
- What election-related data do you define as confidential?
- What procedure did the IEC use to keep the confidential systems/data safe and secure?
- What backup mechan. does the IEC pactice to prevent data loss?

Security and Privacy:
- Have you noticed any fraudulent cases during the 2019 election?
- How did technology help in dtection/prevention of fraud?
- Did technology create any threat for your your colleagues during the 2019 election?
- What cybersecurity threats remained potential in 2019 election? Do you have any story about a cyber-attack that you would like to share with us?
- What security procedures/equipment were in place to prevent cyber or physical attacks on the infrastructure level?
- What was the influence of military groups against the Afghanistan gov. on the IT infrastructure in the 2019 election?

Conclusion:
- Is there anything else that you would like to add to this interview?
- Do you have any question for us?
- Could you refer us to other individuals who had a role in the election that may be interested in an interview?

C Appendix – BVV Ecosystem

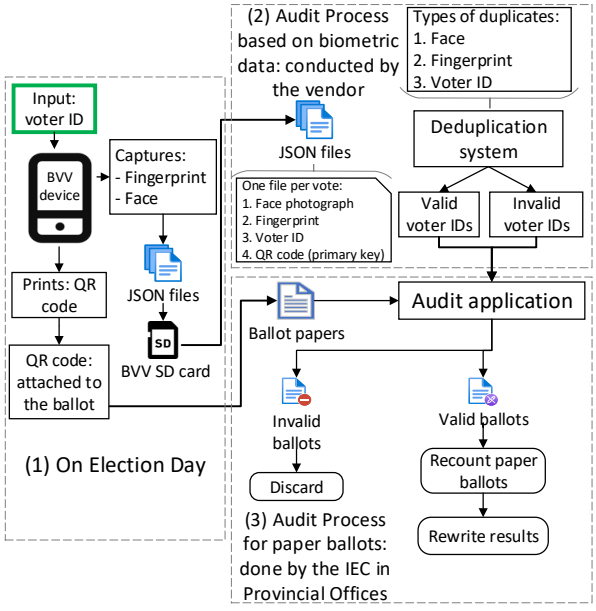

Figure 2: Biometric Voter Verification (BVV) Workflow