INTERNATIONAL IDEA
INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

Introducing Biometric Technology in Elections

Introducing Biometric Technology in Elections

Lead author: Peter Wolf
Case study authors: Abdul Alim, Brown Kasaro, Mohammed Saneem, Pontius Namugera and Tamir Zorigt

International IDEA
Strömsborg
SE–103 34 Stockholm
Sweden
Telephone: +46 8 698 37 00
Email: info@idea.int
Website: ‹http://www.idea.int›

Cover design: Kristina Schollin-Borg
Design and layout: International IDEA

ISBN: 978-91-7671-205-4

Created with Booktype: ‹https://www.booktype.pro›

Contents

Preface

Voter registration remains one of the most complex and contested parts of the electoral process. In countries where there is no trustworthy population census and no reliable identification documents, voter registration is even more complicated. Existing registers are often of poor quality, thus opening up avenues for manipulation and putting pressure on electoral management bodies to establish more reliable registration systems. In such a situation, it is often assumed that biometric technology can provide the required solutions.

The drive towards biometrics has been facilitated by its largely apolitical nature. In many cases, there is broad agreement on the need for its application, not least because investing in high-tech solutions allows stakeholders to demonstrate their commitment to resolving registration problems. That said, expectations regarding biometric solutions may also be exaggerated, and the introduction of new biometric technologies can create a new set of challenges.

The aim of this Guide is to improve understanding of biometric technologies among key electoral stakeholders, including electoral management bodies, governments and decision-making bodies, and civil society, including voters.

While some voter registration problems can indeed be addressed by biometrics, manipulation and malpractice can never be prevented by technology alone. Costs and sustainability are another concern.

We hope that this Guide will act as a useful resource for electoral authorities considering introducing biometric technologies in elections, and as a motivation for improvement, where needed, for those who have already done so.

Yves Leterme
Secretary-General, International IDEA

Acknowledgements

We would like to thank all those who contributed to the content of this Guide, and in particular the lead author, Peter Wolf, of the Electoral Processes Programme at International IDEA. We would also like to thank the authors of the country case studies: Abdul Alim, Brown Kasaro, Mohammed Saneem, Pontius Namugera and Tamir Zorigt.

Jorge Valladares and Gregory Kehailia, both working with International IDEA in Myanmar, contributed important comments and suggestions. Abdurashid Solijonov, of International IDEA's Electoral Processes Programme, extracted maps and statistics from International IDEA's ICTs in Elections Database.

In June 2016, in Pretoria, South Africa, International IDEA hosted a workshop on biometric voter registration practices in Zimbabwe. Special thanks go to the presenters at the workshop for their additional comments and input, including Granville Abrahams, Senior Manager, Election Commission of South Africa; Liberman Bhebhe, Executive Director, National Youth Development Trust Zimbabwe; Tawanda Chimhini, Executive Director, Elections Resource Centre Zimbabwe; Ellen Dingane, Programme Coordinator, Zimbabwe Electoral Support Network; Idrissa Kamara, Democracy and Electoral Assistance Unit, African Union Department of Political Affairs; Qhubani Moyo, member of the Zimbabwe Election Commission; Chidi Nwafor, Director at the INEC Nigeria (on whose presentation the Nigeria case study is based); and Nicholas Matatu and Adebayo Olokoshi of International IDEA.

This report is based on data collected up to November 2016. The data and maps are continuously updated in International IDEA's ICTs in Elections Database.

Abbreviations

AFIS	Automatic fingerprint identification system
AES	Automated election system (Mongolia)
BVR	Biometric voter registration
BVV	Biometric voter verification
BVVS	Biometric voter verification system
DDCM	Direct data capture machines (Nigeria)
EMB	Electoral management body
EC	Election Commission (Bangladesh)
ECU	Electoral Commission of Uganda
EVR	Electronic voter register
FAR	False accept rate
FEO	Fijian Elections Office
FRR	False reject rate

FRS	Facial recognition system
GEC	General Election Commission (Mongolia)
GASR	General Authority for State Registration (Mongolia)
ICT	Information and communications technologies
NID	National identity card (Bangladesh)
NIRA	National Identification and Registration Authority (Uganda)
NSIS	National Security Information System (Uganda)
PERP	Preparation of Electoral Roll with Photographs (Bangladesh)
PVC	Permanent voter card (Nigeria)
PVRIS	Photographic Voter Registration and Identification System (Uganda)
SCR	Smart card reader (Nigeria)
UNDP	United Nations Development Programme
WSQ	Wavelet scalar quantization

Introduction

Voter registration is one of the most important activities that an electoral management body (EMB) needs to conduct, but it is also one of the most costly in terms of both time and resources. A credible voter register confers legitimacy on the electoral process, helps prevent electoral fraud and ensures that every eligible voter can vote in an election and that they can do so only once.

An inaccurate voter register can cause problems in the electoral process by raising doubts about the election's inclusiveness and outcome and by opening up avenues for fraud and manipulation. Many countries that face challenges in creating an accurate voter register are considering reforming their voter registration systems through the introduction of biometric technologies. Such reforms are aimed at increasing trust in the electoral process by enfranchising all eligible citizens and, at the same time, reducing various forms of electoral fraud, such as voter impersonation and multiple voting.

This Guide provides an overview of key concepts and considerations for all stakeholders involved in discussions about the application of biometrics in elections, both for voter registration before an election and for voter verification at polling stations on election day.

The Guide is structured as follows. Chapter 2 describes the development, uses and application of biometrics worldwide. Chapter 3 presents systems options and considerations, while Chapter 4 discusses some of the limitations of biometric technologies in elections. Chapter 5 explores some new developments in biometric technologies. Chapter 6 outlines factors to consider when adopting biometrics, and Chapter 7 points to some alternatives to biometrics.

Following the Conclusion, which also includes recommendations, the Guide presents case studies from six contexts where biometrics have been introduced: Bangladesh, Fiji, Mongolia, Nigeria, Uganda and Zambia.

1. The use of biometrics in elections

Background

Biometrics involves the measurement and analysis of unique physical or behavioural characteristics, especially as a means of verifying and identifying an individual. The broad range of biometric characteristics that can be measured includes fingerprints, palm prints, retina and iris scans, voice patterns and DNA profiles (Bolle and Pankanti 2004).

In a biometric *verification* system, an individual claims an identity, for example by providing a name and date of birth. The individual's biometric features are captured and compared to previously captured and confirmed biometric features of that individual. Such a one-to-one comparison determines whether the individual is indeed who they claim to be.

In a biometric *identification* system, the individual does not need to claim an identity. His or her biometric features are captured and compared to the features of all previously captured biometric features stored in a biometric database. This one-to-many comparison seeks to determine who the individual is.

The application of biometrics as such is not new. The first fingerprint catalogues of known criminals were established in the second half of the 19th century for the use of police investigators and criminal courts (National Institute of Justice 2011). The second half of the 20th century saw further advances in the development of automated biometric identification systems (Jain, FlynRen and Ross 2008). In recent years, the application of biometric technologies has expanded rapidly in diverse fields such as access control, border security, citizen registration, passports and identification cards, and elections (Das 2016).

In the late 1990s and early 2000s analogue technologies were used to capture biometric voter registration data. For example, Polaroid cameras were used to capture facial images of registrants, and registrants' fingerprints were recorded using ink and paper. This information was attached to paper registration forms and later scanned and digitalized at data centres (EISA 2010). Now, such analogue systems are obsolete, and biometric data are largely captured using electronic registration kits, including digital cameras and digital fingerprint pads. The number of countries adopting biometrics in elections has steadily increased to over 50, with significant differences between regions: while there are virtually no users in Europe, about half of the countries in Africa and Latin America use this technology in elections (see the International IDEA ICTs in Elections Database for more information).

Capturing, processing and storing biometric data

The most commonly captured biometric features for electoral purposes are fingerprints for automatic fingerprint identification systems (AFISs), facial images of voters for facial recognition systems (FRSs) and sometimes also scanned signatures. Iris-recognition systems are a relatively new option and not yet widely used for electoral purposes.

All biometric data is first captured by a camera or sensor as an image. This image is then further processed into a biometric template. Matching algorithms used for verification and de-duplication are based on comparing these biometric templates.

While collecting data in the form of biometric templates is enough for matching algorithms, these templates can be proprietary to the system vendor. Biometric templates cannot be transferred back into the original images. To avoid vendor lock, it is advisable to store both the captured images and the templates in the registration database. Wavelet scalar quantization (WSQ) is a common format for storing fingerprint images. In case of a change of vendor, this technology makes it possible to re-create new templates based on existing images without repeating the registration exercise.

Application of biometric technologies in elections

In elections, biometric technology can be used in one or more of the following processes:

Biometric voter registration (BVR)

For voter registration, biometric data for each eligible voter is captured using biometric registration kits. The resulting voter register contains biometric data such as fingerprints and facial images in addition to biographical and personal

data, such as an individual's name, date of birth, national ID number, address and assigned polling station.

In countries where voter registers are derived from civic or population registers and where those registers already contain biometric data, this data can very likely also be used for electoral purposes, thus greatly simplifying the establishment of a biometric voter register.

A biometric voter register is a precondition for the following applications.

Biometric voter ID cards

Once a biometric voter register has been established, some of the captured data can be printed and/or stored electronically on voter ID cards. A voter's photo is usually printed on their ID card. Sometimes, cards also include an image of a fingerprint and the voter's signature.

Voter ID cards can also store biometric information in digital format on a microchip, magnetic strip or barcode included on the card.

Biometric de-duplication

A biometric voter register allows for more efficient detection and deletion of duplicate registrants. Biometric de-duplication is usually conducted by matching fingerprint data, often in combination with facial-recognition systems. De-duplication is often the main reason for the establishment of biometric voter registers, especially when many citizens have no reliable identification documents, when no reliable civic registration exists or when the quality of alphanumeric data in the voter register is poor.

Biometric voter verification (BVV)

In order to *prevent identity theft* and *multiple voting*, biometric technology can be used at polling stations to confirm the identity and eligibility of voters. Electronic verification is usually conducted by devices such as electronic poll books that capture voters' fingerprints and check them against the fingerprints stored in the voter registration database for the polling station. Alternatively, fingerprints can be checked against fingerprint data stored digitally on a voter identification card.

A simpler way of utilizing biometric data at polling stations is the inclusion of voters' photos on the printed voter list to enable polling staff to visually check the identity of voters.

When to use biometric voter registration

All the above tasks can also be conducted without capturing biometric data. Simpler and cheaper computers and databases can be used to capture and process biographical voter data (e.g. name, date of birth, ID numbers, addresses, constituencies) only.

Whether or not biometric data adds real value depends on the context in which the technology is used. Biometric technology may lead to significant improvements when:

- citizens do not have reliable and trusted identification documents that can be used for voter registration;
- there is a need to issue voter ID cards or if voter ID cards need to include biometric details about the voter;
- multiple registration is a major problem and/or when multiple registration cannot be reliably detected based on high-quality biographical data in the voter register;
- multiple voting and voter identification at polling stations are major problems;
- photos or other biometric features are required on voter lists at polling stations, where it is difficult to establish the identity of citizens based on reliable identification documents; and
- voter registers cannot be extracted from reliable and trusted civic or population registers.

The use of biometrics worldwide

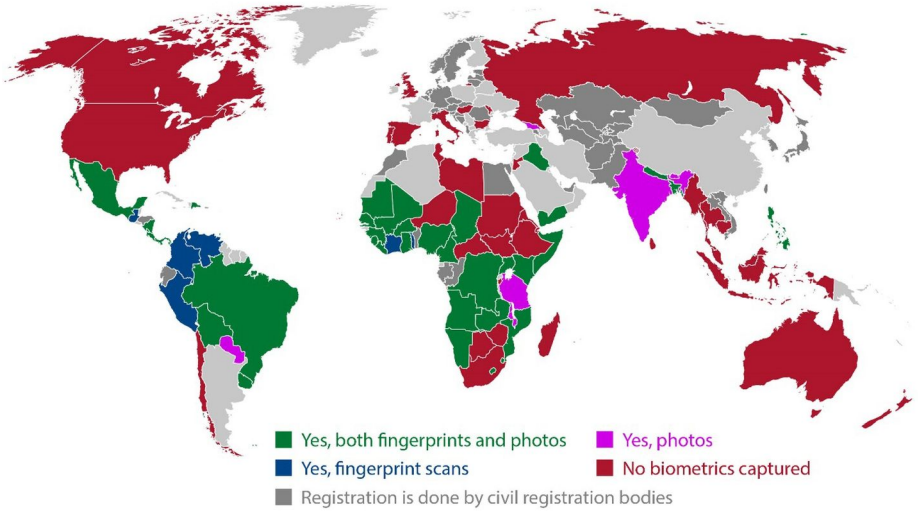
Biometric voter registration

According to International IDEA's ICTs in Elections Database, as of 2016, 35 per cent of over 130 surveyed EMBs were capturing biometric data as part of their voter registration process. Biometric technology is widely used in the registration process, especially in Africa and Latin America (see Figure 1). In 32 per cent of surveyed countries, voter registers are based on civil registers. In many cases, civic registration systems contain biometric data that can be used for electoral purposes.

Biometric voter verification and identification

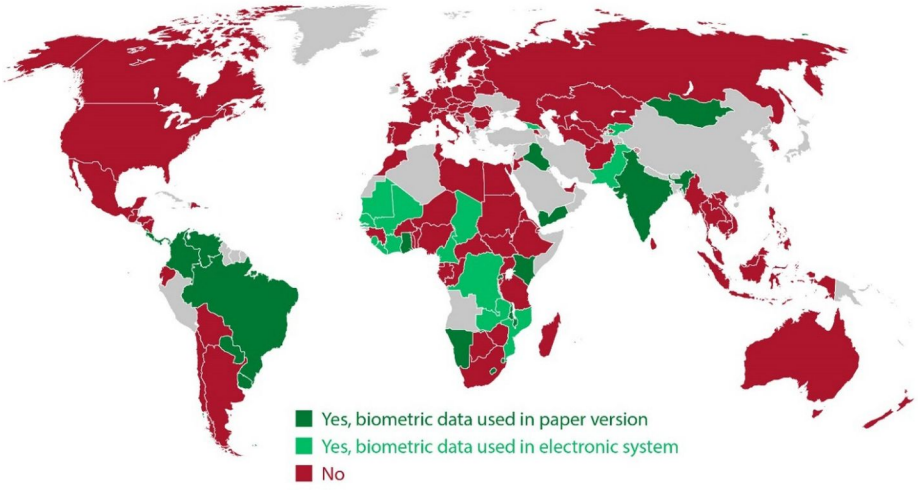
Twenty-five per cent of the surveyed EMBs use biometric information to identify voters at polling stations. However, in many cases this does not involve electronic biometric identification, but rather a manual check of each voter's photograph on the voter list. Only 9 per cent of the surveyed countries utilize an electronic biometric voter identification system. In some of these cases, fingerprint scans are only conducted in selected precincts and not the entire country (see Figure 2).

Figure 1. EMBs conducting biometric voter registration



Source: ICTs in Elections Database, <https://idea.int/data-tools/data/icts-elections>, September 2016.

Figure 2. Use of biometric data at polling stations

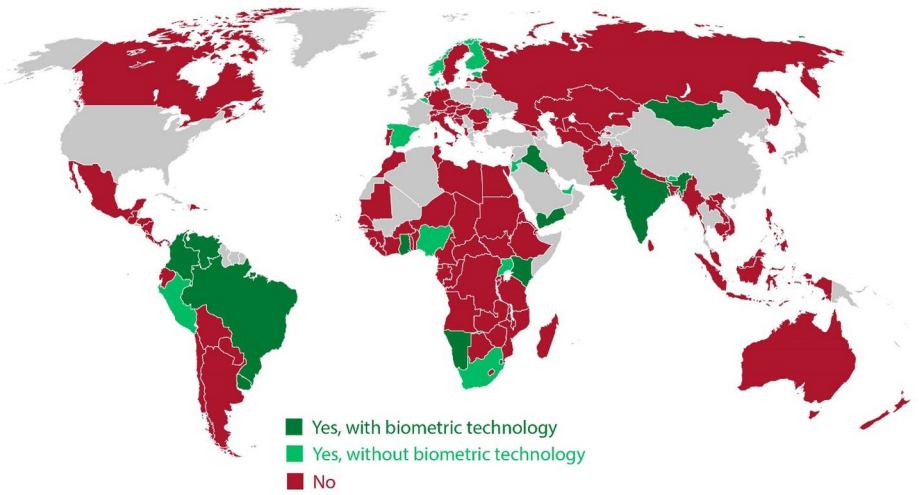


Source: ICTs in Elections Database, <https://idea.int/data-tools/data/icts-elections>, September 2016.

Electronic voter identification

Of the countries that have electronic voter identification devices at polling stations, most of them do not utilize biometric scanners: 23 per cent of the surveyed EMBs use electronic identification devices at polling stations but 60 per cent of those devices have no biometric capability (see Figure 3).

Figure 3. Electronic voter identification at polling stations



Source: ICTs in Elections Database, <https://idea.int/data-tools/data/icts-elections>, September 2016.

3. System options and considerations

Biometric technology can be implemented in many different ways and adjusted and selected to best fit a country's needs and existing infrastructure.

Is there a real need for biometrics?

The following questions may help assess the value of biometric technologies. The more of these questions that are answered in the affirmative, the stronger the case for using biometric technologies becomes. However, only the most complex biometric systems will be able to cover all these functionalities.

- Is a new registration system the only reliable option for creating a credible voter list? Could such a list be derived from other registers?
- Is there a need for better de-duplication of local or national voter lists?
- Is there a need for more reliable identification of voters through printed photos or signatures on paper voting lists at polling stations?
- Is there a need for more advanced electronic and/or biometric identity checks at polling stations on election day, for example to verify voter eligibility and to prevent impersonation and multiple voting?
- Is there a need to issue new, more reliable voter ID cards?
- Should voter ID cards include biometric features, such as a photo, signature or fingerprints?

Should it be an EMB-driven registration process or should it be based on population/civil registries?

Biometric registration is a costly and time-consuming exercise, especially if conducted for the sole purpose of creating a voter register. Extracting voter registers from any existing population registers, civil registers or national ID-card databases is much more efficient and can lead to substantial cost savings. Therefore, the following questions may help assess whether the use of civil registers should be considered as an option:

- Is there a civic or population register in electronic format from which voter registration data could be extracted?
- Is the data in the register reliable, comprehensive, accurate and up to date?
- Is the data in the register sufficient for electoral needs, for example to assign voters to polling stations? If not, how much effort would be required to add any missing data?
- Is the government body in charge of the voter register trusted enough to be the main source of information? If not, can the EMB put in place oversight measures to guarantee the quality of the voter list?
- If biometric data is needed for voter identification at polling stations, does the register contain such data in a suitable format?

Even if biometric data cannot be obtained from other government bodies, it may be worth investigating whether biometric equipment and infrastructure used by another government body may be used for voter registration.

Mongolia

In Mongolia, the General Authority for State Registration (GASR) prepares laptop computers for polling stations to which it exports all available biographical and biometric data on eligible voters. The Working Group on Automated Election System Certification, in which the General Election Commission (GEC) participates, is in charge of supervising and certifying the export process. All of this system's hardware, software and data are maintained by the GASR, and the GEC is not involved. For more details see the Mongolia case study.

System architecture

Centralized voter registration database

Biometric registration can, in principle, be conducted at the local constituency level. This would, however, only produce limited benefits. While biometric voter verification could be conducted, de-duplication would remain restricted to the local level. Multiple registrations throughout the country (or even in neighbouring constituencies) could not be detected.

In most cases, biometric voter registration therefore entails the establishment of a central, national voter registration database and the creation of related infrastructure for data transfer and communication.

Online versus offline systems

All voter registration centres and voter verification systems at polling stations would ideally be connected directly to a centralized voter register.

An online registration system has many benefits:

- up-to-date information is always available at the local and central levels;
- duplication checks can be conducted directly at the point of registration. Voters can be informed immediately, and the issue can be addressed on the spot;
- there is no need for the physical transfer of data from registration and verification kits to central databases; and
- there is no need for manual backups of databases on local registration and verification kits, as all data can be restored immediately on the server.

In many cases, however, infrastructure and connectivity restrictions will not allow for reliable online access throughout the country, and offline systems need to be deployed. In this case, offline registration systems:

- need to be individually configured with all necessary data before deployment;
- need physical storage media (e.g. hard disks, USB memory) that are transferred regularly to exchange data with the central registration database;
- need stable data backup procedures to avoid the loss of local data;
- can only perform local eligibility and duplicate checks and require related procedural safeguards;

- cannot immediately confirm successful registration, and only preliminary registration confirmation can be issued to registrants;
- need reliable synchronization of central and local database systems to detect any lost registration data (e.g. lost or stolen flash drives or corrupted media during transfer).

Similar considerations should be taken into account for voter identification systems. If polling stations have stable network connections, the configuration of equipment can be more uniform and data backups are less important. However, fallback systems should be in place in case of network outages.

Online voter verification systems have the additional advantage that voters can (legal framework permitting) be allowed to vote at any polling station, as their eligibility can be checked at every location.

Initial, continuous and periodic registration

When introducing a new registration technology, it is important to plan not only for the initial establishment of the new registration system but also for maintaining and updating the voter register, either periodically or continuously.

Periodic voter registers are discarded after an election and compiled from scratch for the next election. Considering the complexities of collecting biometric data and the capabilities of registration databases, this is usually not the most efficient method of maintaining biometric registers. One of the advantages of periodic registers is that they do not require procedures for removing deceased voters or for updating voter addresses.

Continuous registers are regularly updated rather than compiled from scratch. For a continuous register, the system needs to include features for address and other data changes, re-registration, the removal of deceased voters as well as the addition of new voters. With continuous registers, the entire electorate only needs to be enrolled once. After that, the resources (number of registration kits, registration staff time) required for updating will decrease significantly.

Fiji

In Fiji, electronic voter registration is carried out using laptop computers, handheld webcams and mobile fingerprint readers. Initially, Fiji purchased 384 registration kits to register around 500,000 voters. Currently, the EMB maintains 30 kits for the purposes of updating existing records and registering new voters. For more details see the Fiji case study.

Zambia

The Electoral Commission of Zambia (ECZ) updates the permanent register, which contains records on some 6.7 million registrants, before every general election through mobile registration campaigns. The registration campaign in 2015 lasted 90 days and utilized 2,000 biometric kits to capture data from 7,700 registration centres. The biometric kits operate offline. For more details see the Zambia case study.

One registration kit per precinct or roaming equipment

For a swift registration process, registration kits are ideally permanently deployed at registration centres close to voters. Simultaneous deployment to all registration points speeds up the initial registration process, as registration takes place at the same time in all precincts.

In order to save on costs, roaming registration kits have been used in many countries. The kits are deployed to several locations for a few days each. This reduces the number of required registration kits and the related costs. As registration at one location is only possible for a shorter period of time, the accessibility of the registration process is more limited, and the overall registration process and the creation of a full national register will take longer.

Which biometric data should be captured?

Fingerprints

Automatic fingerprint identification systems can be based on scanning a single fingerprint for each registrant. This is the fastest and simplest procedure. However, only capturing one fingerprint increases the possibility of fraud, as the same person may register multiple times by using different fingers.

Capturing more than one fingerprint for each voter reduces the potential for fraud, and increases the amount and quality of available fingerprint data. In this way, false match rates can be greatly reduced.

In recent years, 10-fingerprint scanners have become more common. They scan all 10 fingers in three steps (four fingers on the left hand, four fingers on the right hand and both thumbs)

Facial images

Many digital voter registration kits capture a photo of the voter. This photo can be printed on voter ID cards or voter lists, and processed into a biometric template for facial-recognition systems.

Utilizing facial recognition in addition to fingerprint recognition can further increase a system's accuracy. However, this requires high-quality photographs taken in good lighting conditions and images with a neutral facial expression. Getting such high-quality pictures, especially in a field environment, is very difficult.

Facial-recognition systems should therefore only be used in addition to fingerprint recognition systems.

Signatures

While electronic signature pads are able to capture signatures, this is not very common in voter registration. A person's signature may intentionally or unintentionally vary significantly, which makes reliable electronic matching difficult. Images of voter signatures can still be useful to print on voter ID cards, for example for visual comparison against the signature on the voter list.

Iris scans

Iris-recognition systems are a relatively new development and have rarely been used in elections; Somalia is the only country currently using such a system for election purposes, in Somaliland. Iris recognition has several advantages over fingerprint recognition: the eye and the iris are better protected physically than fingerprints, and an iris scan can be taken from a distance without contact with any equipment, making dirt and physical wear less of an issue. On the downside, recognition rates depend on lighting conditions, and the cost of iris-scanning technology is still comparatively high.

Issuing voter ID cards

Biometric registration kits can also be used to print voter identification cards, even directly at the registration point. This can be especially useful when many voters do not have access to other identification documents. Voter ID cards also provide voters with proof of successful registration. Important considerations for voter ID cards include the following:

- Does a voter ID card need to be issued at all? Printing cards will require additional resources (printers, blank cards, ink). Printers often turn out to be the most difficult piece of hardware to maintain.
- Should biometric features be printed on voter ID cards?
- Should voter ID cards contain digital information in machine-readable formats (chip, magnetic strip, barcode)?

- Should ID cards be issued right away after registration? This provides immediate proof of registration and eliminates the need to deliver the ID card to the voter. However, it can lead to confusion and discrepancies when the voter's record is changed or deleted during data processing, de-duplication and compilation of the final voter list (see the Zambia case study).
- Should voter ID cards only be issued after the final voter list has been compiled? In this case, voter IDs are only issued to confirmed registrants, and IDs can possibly be printed in a more centralized way. Since all registrants need to be contacted a second time for ID card distribution, this requires another time- and resource-consuming process, and some voters will likely not obtain their voter IDs.

De-duplication procedures

De-duplication of large biometric registers requires substantial computational and human resources. The ICT resources required are particularly high in the beginning when an entire register has to be cross-checked. At that stage, each registrant's biometric data has to be compared to the data of all other registrants. Later on, when only relatively few new registrants are added, the computational effort decreases. In some countries, such as the Democratic Republic of the Congo, purchasing all the required de-duplication ICT resources was not feasible, and the process was thus outsourced to international commercial providers.

Even though much of the de-duplication work can be conducted automatically, human adjudication is required in unclear cases. Related procedures need to be developed, and staff must be available and trained accordingly. If the process is outsourced, it should be clarified who can conduct manual adjudication.

Nigeria

For the 2015 general elections in Nigeria, the EMB decided to optimize the registration process by using permanent voter cards and smart card readers. The card technology chosen included a contactless chip card that was difficult to counterfeit or tamper with that would last for up to 10 years. This smart-card-based system stores voter information such as biographical data, biometrics and a facial image. For more details see the Nigeria case study.

4. Limitations of biometric technologies in elections

Biometrics confirm identity, not eligibility

While biometrics *can* be used to verify the identity of voters, they *cannot* be used to verify their eligibility. Whether a registrant is underage, is a citizen or is eligible to vote in a certain constituency cannot be checked biometrically. These checks will always need to rely on other means of verification and documentation.

Biometric technology alone does not guarantee comprehensive or inclusive voter registration.

Comprehensive voter registration can only be achieved when citizens are aware of registration processes, when they have reasonable opportunities and easy access to the process and when there are no registration barriers such as high costs, time-consuming procedures, difficult-to-reach registration centres and short registration deadlines.

When a new registration system—biometric or other—is introduced, it is always a challenge to reach all eligible citizens. Any new system risks yielding lower registration rates during the initial registration drive.

When low registration rates and incomplete registers are a problem, biometric systems alone will not provide a solution, and analysing weaknesses in the overall registration process is at least as important as technological upgrades.

Failure rates

It is sometimes assumed that biometric systems always work correctly and without failure. In reality, biometric technologies and related matching processes cannot be expected to work with 100 per cent accuracy.

The following performance metrics are important for understanding the types and frequency of mistakes that can occur:

- Failure-to-capture rate: the number of cases in which biometric data cannot be read from an individual. This is relevant at the time of voter registration.
- Failure-to-enrol rate: the number of cases for which the data can be read biometrically, but the quality is too poor to create a usable biometric template and database entry. This is relevant at the time of voter registration. A registration system should immediately alert the operator if it is not possible to create a database entry.
- False match rate (sometimes also called the false accept rate): the probability that a system will match the wrong database entry to a biometric input.
  In deduplication, this can lead to the detection of false duplicates; for voter verification at polling stations, it can lead to the wrong voter record being matched after a fingerprint scan.
- False non-match rate (sometimes also called the false reject rate): the probability that a system will not detect a match between a biometric input and a related database entry.
  In deduplication, this can lead to undetected duplicates; for voter verification at polling stations, it can lead to a registered voter not being recognized by the fingerprint scanner.

Failure rates depend on many factors, including:

- the quality of equipment used;
- the amount of biometric data captured. The more data captured, the better the results. For example, systems utilizing all 10 fingerprints have lower failure rates than those scanning only one; systems that match both facial features and fingerprints are more accurate than those that are only based on one metric;
- environmental conditions such as temperature, humidity, dust or dirt on the scanner, and lighting conditions;

- individual physical characteristics such as injuries, physically damaged fingerprints, registrants with calloused or dirty fingers; and
- the type of biometric data in question. Typically, facial-recognition systems have higher failure rates than fingerprint matching systems. Iris-scanning systems are in turn more reliable than fingerprint-based systems.

While failure rates may be low, it is important to recognize that failures are inherent to biometric technologies. When utilizing biometrics, such failures should be expected and accommodated. Automated biometric identification systems often need to be complemented by human adjudication mechanisms. Fallback procedures should be in place to make sure that voters are not disenfranchised where biometric identification is not possible due to technical limitations.

Biometrics does not prevent all forms of manipulation and mistakes

Biometric voter registration can prevent some types of electoral fraud. In a context where electoral fraud is common, however, new kinds of manipulation may occur.

Where exceptional procedures make it possible to skip biometric enrolment, for example in cases where enrolment is difficult or impossible, such exceptions may be exploited. Any such exceptions should be documented and investigated if they are very common in certain areas.

It is also important to make sure that biometric data is captured from the correct registrants. Sometimes, the wrong person's fingers are scanned, intentionally or by mistake, and even attempts to fraudulently capture biometric data from images are not unheard of.

In areas where attempts to deny registration are common, care must be taken to prevent or compensate for the intentional damage or destruction of registration kits aimed at delaying or cancelling the registration process.

5. Implications of new biometric technologies

Impact on registration, voting procedures

Introducing biometric technologies may result in significant changes in the way voter registration is conducted. Such changes may require a review of existing registration procedures and an agreement on necessary fallback mechanisms:

- What happens if a citizen cannot be enrolled successfully in the biometric voter registration (BVR), possibly as consequence of the failure-to-capture or failure-to-enrol rate, as explained earlier?
- What happens if a citizen's eligibility cannot be confirmed through a biometric verification process on election day (possibly as a consequence of the false match rates or FNMR, as explained earlier)? Should there be supplementary lists or alternative means of identification?
- If a voter's eligibility can be confirmed through the biometric voter verification system (BVVS), is there still a need to provide other proof of identity, for example if a voter does not bring an ID card, is a fingerprint scan sufficient?
- What are the backup procedures in case of complete system failures? Should alternative manual processes remain in place, and if so, when should they be used?

Avoiding negative impacts on voters and disenfranchisement

Biometric technologies, especially when introduced, may have a negative impact on the electorate and even lead to the disenfranchisement of some groups of voters. This should be avoided as far as possible. Some registration barriers to consider include:

- Accessibility for citizens: will registration and identification be at least as efficient and accessible with technology as they were without? Will some citizens, for example the disabled, find it more difficult to register?
- Queues: capturing and matching biometric data takes time and can delay registration and identification processes. Will the amount of available (and affordable) equipment be sufficient to avoid long queues and waiting times, which may discourage citizens from registering and voting?
- Cultural barriers: are there religious beliefs or cultural objections that may prevent some citizens from providing biometric information? Are these real objections or just misinformed assumptions that can be addressed through information campaigns?
- Rumours: is there potential for rumours that may discourage citizens from registering or voting? Increased voter information campaigns may be a remedy where there are false assumptions such as that the use of biometrics is endangering the secrecy of the vote, that biometric equipment transmits disease or a fear that biometric data will be used against people.
- Simplicity: is the proposed system unnecessarily complicated and difficult for voters to understand?
- Violence and intimidation: is there a risk of some actors resorting to violence against individuals, sabotaging equipment or intimidating voters when fraud is eliminated through new technologies?

Data protection

Voter registers contain the personal data of millions of citizens. Protecting the privacy of this data, both legally and technically, is of the utmost importance. This is true of biographical data and even more so for the unalterable, personal characteristics stored in biometric systems. Data in central registration databases needs to be protected, as does data in biometric registration and verification kits deployed throughout the country.

Regulation is required regarding the purposes for which biometric data can be used and the individuals to whom this data can be disclosed. Citizens whose data is collected should be able to obtain information about how this data will be used, and they should have an opportunity to access their data and correct any inaccuracies.

Whether the required data protection legislation is already in place or whether data protection needs to be specifically regulated for the use of biometrics in elections should be assessed in a review of the legal framework.

Owners of biometric databases need to make sure their procedures adhere to data protection regulations, and they have to take steps to ensure that biometric registration data is technically secure against potential misuse and unwarranted disclosure.

As biometric templates are often proprietary, the use of inadvertently disclosed templates is limited. The disclosure of original biometric image data has great potential for misuse and creates a risk of identity theft that is not limited to elections.

Transparency

Using biometrics for voter registration and identification does not eliminate the need for transparency measures related to voter registration. Building stakeholder trust in biometrics and avoiding incorrect perceptions requires continuous engagement. Information about the systems in use should be provided from inception to implementation and use.

It is advisable to explain from the very beginning why biometric solutions are proposed and how they can be expected to improve the electoral process, as well as what they cannot achieve. Platforms should be provided to discuss concerns that will surely arise. Beyond the provision of such information, it is also recommended that interested stakeholders be allowed to follow the selection and implementation of biometric systems.

Even with biometrics in place, the public display of voter lists remains an important transparency mechanism, both as a general confidence-building measure and to increase the quality of the register by encouraging widespread checks and reporting of mistakes.

Once electronic voter registration databases are in place, it is not difficult to give citizens the ability to check their registration status online, for example through websites, mobile applications or SMS-based systems.

The provision of electronic versions of the full voter register to selected stakeholders, such as political parties, is another common transparency measure. However, it needs to be clarified who is granted access to this data, in what format the data is provided and what the data can be used for.

6. Factors to consider when introducing biometrics

There are many recent examples where the introduction of electoral technologies created serious problems, including delays and disenfranchisement of voters. Such cases are often due to poor planning and short implementation timelines. Difficulties can be expected to arise when rolling out new registration systems in less than a year, especially on a national scale.

Key stages for introducing biometric technologies

Needs assessment

This stage is for developing a clear understanding of goals and stakeholder expectations: can they realistically be met? What is the level of stakeholder support?

To understand what is needed, any assessment should also include a review of existing procedures to identify shortcomings: which, if any, biometric solutions have the most potential for improvement? What problems is the biometric technology supposed to address?

Feasibility studies

At this stage, system options and alternatives are considered: which ones are the best fit in terms of costs, infrastructure and sustainability? Will there be any negative impact on voters? If so, how can it be mitigated? This phase also includes a demonstration and evaluation of solutions available on the domestic and international market and the development of technical specifications for the most suitable system.

Securing funding

The use of biometric technology for elections requires substantial funding. This stage assesses whether the required funding for a biometric system can be secured in the short term for the initial rollout of the system as well as in the long term for future elections. It also needs to ensure that the required funding will be available on time so that financial matters do not delay project implementation.

Reviewing legislation

Electoral laws, registration and voting procedures need to be reviewed and probably updated. Attention should be paid not only to new regulations, but also to existing legislation that has to be adhered to or that may become obsolete through the use of new technologies. Data protection legislation requires specific attention, as biometric voter registration databases store sensitive personal information about millions of citizens.

Pilot projects, mock registration exercises

New technologies are best piloted in smaller elections before a full national rollout. Such a gradual introduction makes it possible to gain important experience and makes it easier to maintain the old system as a fallback option.

Procurement

The time it takes to procure, produce and import new voting technologies is often underestimated. When procurement takes longer than anticipated and the election day is set, there is often not enough time for the system rollout.

Distribution of equipment, installation, testing

It is essential to allow sufficient time for proper system installation and testing under field conditions. Many technology failures are rooted in insufficient testing due to time pressures.

Recruitment and training of voter registration staff

For the successful deployment of technology, well-trained staff are essential. While expertise at the central level may already be available, many registration staff usually need to be recruited in the field.

Voter information

A well-informed electorate is essential for a successful and smooth registration process, for widespread participation, and ultimately for achieving high registration rates and thus an inclusive voter register.

Timelines

How long the introduction of biometric technologies takes greatly depends on the exact context, legal framework and needs. However, comparing various country experiences, it is recommended that initial preparations begin at least 18 to 24 months before an election. A typical timeline could be:

- six or more months for procurement, tendering, vendor selection and contracting. As these initial steps often take longer than planned, ample time buffers are recommended;
- two to four months for the production and delivery of equipment, testing and deployment;
- one to six months for the field registration process. Obviously, increasing the number of registration kits will speed up the registration process, but this will also increase related costs;
- two to three months for data processing, de-duplication, and establishing and displaying preliminary voter lists, adjudication of appeals;
- two to three months for printing voter ID cards, and printing and distributing voter lists, finishing about one month before the election.

Uganda

In Uganda, countrywide enrolment of all citizens was initially conducted for four months with approximately 8,000 enrolment kits and two operators per kit. During this period, a total of 16.7 million people were enrolled. The exercise was extended for an additional five months at the subnational level to allow those who had missed out on the mass enrolment exercise to register.

Furthermore, in 2013, the Ugandan Government announced that several institutions, including the Electoral Commission, had all requested resources for registering citizens. This level of duplication prompted the Cabinet to formulate a multi-institution registration task force under the leadership of the Ministry of Internal Affairs. Subsequently, a mass enrolment strategy was developed and implemented whereby participating institutions contributed and shared resources.

For more information see the Uganda case study.

Costs

Biometric technologies come at a significant cost. *Initial* costs could be between EUR 2 and EUR 10 per registered voter, depending on the solution. Beyond initial purchases, equipment will also need to be maintained, upgraded and/or replaced between elections. Total costs will depend on the processes covered, the equipment and biometric features used, available infrastructure and the need for backup power, as well as additional communication links. Costs will also depend on whether voter ID cards are issued, and on whether registration or voter verification (or both) are conducted at polling stations.

The financial impact of a biometric voter registration and identification system can be greatly reduced if registration data can be extracted from other existing population registers. The sustainability of a biometric system may also be improved if the same equipment can be utilized both for voter registration before election day and for identifying voters on election day. Both options should therefore be included in feasibility studies.

Staffing needs

One of the keys to the successful implementation of technology is having well-trained staff who know how to operate deployed systems. Operating biometric registration kits in the field requires hiring a large number of operators and supervisors. Operators need basic computer literacy for data entry and handling the registration hardware. Supervisors need more advanced skills to train operators and for troubleshooting. On average, an EMB might require two operators per registration kit and one supervisor for every 7–10 deployed kits. More ICT-experienced staff will be needed at data processing centres, possibly provided both by the vendor and the EMB. While vendors can usually provide experts required for operations, expertise within the EMB is important for oversight of the system deployed, as well as avoiding vendor lock.

Bangladesh

In Bangladesh, the EMB used 309,000 enumerators, 104,000 computer operators, 62,000 supervisors, 6,000 officers, and technical experts and support staff for countrywide registration of over 80 million voters over a period of 11 months. More than 10,000 laptops with webcams and fingerprint scanners were procured and distributed across the country. For more details see the Bangladesh case study.

7. Alternatives to biometric technologies

Given the significant and long-term investment required to use biometric technologies in elections, governments and electoral authorities should be aware that biometric technology is not necessarily the only option for improving voter registration. Improving existing registration systems and procedures can, depending on context, be a more efficient solution for typical problems such as multiple registrations, inaccurate data, multiple voting, low registration rates and poor public perception of the voter register.

Multiple registration and mistakes

Multiple registration can be the result of attempted fraud, but is often caused by mistakes during data entry or data processing. Voters may register more than once by mistake or fail to de-register when changing their residence. Records may also be duplicated when merging databases from different registration centres.

In case of problems with multiple registration, the following measures can be considered in addition to, or instead of, biometric de-duplication:

- Reviewing registration and data-processing procedures for weaknesses and sources of errors and mistakes.
- Where an electronic voter registration database exists, many duplicates can be detected without biometrics by matching biographical, alphanumeric data (e.g. names, dates of birth). Fuzzy matching procedures can be used to compensate to some extent for data entry mistakes and typos.
  This has limitations, however, when people share the same name and date of birth, when some voters do not know their exact date of birth and

registration offices use an estimate instead (often 1 January of their birth year) and when voters have multiple names and they intentionally or unintentionally change their name between registrations.

- The public display of preliminary voter lists and the sharing of electronic versions of the voter list with relevant stakeholders, and encouraging review and objections in case of mistakes are powerful measures for assuring the quality of the voter list and building trust at the same time.

Multiple voting

Biometric technology can significantly decrease opportunities for multiple voting. During registration, biometrics can be used to detect and prevent multiple registration, and biometrics used in polling stations can clearly establish a voter's identity and thus mitigate the risk of impersonation, identity theft, the misuse of records of deceased voters, carousel voting and ballot-box stuffing. Alternative non-biometric measures include marking voters' fingers with indelible ink or the use of photo voter lists without full-scale biometric processing.

Low registration rates

Biometric technology alone cannot solve problems related to low voter registration rates. Identifying and eliminating any registration barriers, increased voter information and encouragement to register are at least as important as technical upgrades aimed at increasing the comprehensiveness of a voter register.

An important consideration is whether a new biometric system will make it more difficult for voters to register or stay registered, for example when not enough registration points or equipment can be provided. Insufficient registration equipment may cause limited time windows during which voters can register, long queues and waiting times, or it may require voters to travel long distances to register.

Damage to public perception

Positive public perception of the quality of the voter list is essential. Using biometric technologies is a very visible and high-profile measure that demonstrates commitment to improving voter registration. However, if biometric registration is not feasible, any alternative measures and related analysis also need to be widely publicized to increase stakeholder trust and confidence in them.

8. Conclusions and recommendations

This Guide provides an overview of issues decision-makers should consider when adopting biometric technologies in the context of elections, namely: their real added value; the context in which they are applied; mitigation of side effects, in particular disenfranchisement; the cost-efficiency of the technology and the time frame in which it is adopted.

This leads to several recommendations and lessons for governments and election officials to consider in assessing the adoption of biometric technologies.

Recommendations

1. Capturing stakeholder expectations and analysing existing voter registration problems are essential for understanding if, how and which biometric technology can address them.
2. Biometric technology is very efficient for reducing or eliminating multiple registration and multiple voting, as well as producing high-quality, tamper-resistant voter ID cards.
3. Low registration rates will not be improved by using biometric technology. Additional measures such as providing voter information about the registration systems in place, removing any registration barriers and introducing an inclusive registration process are essential regardless of whether a biometric system is used.

4. Biometric technology cannot be expected to operate entirely without the risk of failure. Fallback procedures should be in place to prevent disenfranchising voters and creating unnecessary registration barriers.
5. Biometric technology may malfunction, especially in difficult physical and environmental conditions, or where the necessary infrastructure is limited. Piloting, testing and fallback options in case of failure are essential.
6. Biometric technology is expensive, and alternative solutions should be considered. Technology costs are related not only to the initial procurement and rollout, but also to long-term ownership and maintenance.
7. If a decision to introduce biometrics has been taken, sufficient funding needs to be secured in a timely manner.
8. In contexts where citizens already have reliable and trusted identification and/or where multiple voting and impersonation are minor problems, the added value of biometrics in elections is likely limited.
9. Biometric technology should only be introduced where an appropriate legal framework and registration procedures are in place.
10. A common reason for the failure of new technologies is insufficient time for project implementation. The gradual introduction of technologies over several electoral cycles is safer than an immediate full-scale rollout nationwide.

Case studies

Case Study 1. Bangladesh

Abdul Alim

Biometric voter registration (BVR) in Bangladesh was first initiated in 2007 following the postponement of the ninth parliamentary elections that were originally scheduled to be held on 22 January 2007. One of the reasons for the postponement was the poor quality of the voter list, which contained approximately 12.2 million names that were on the list either in error or were duplicates (Alim 2014). After the election was postponed, a new Election Commission (EC) took office in accordance with a presidential decree. Once in office, the High Court ordered the EC to update the existing voter list based on the enfranchisement of adult citizens. In order to implement the court's order and to prepare a credible voter list, the new EC conducted stakeholder consultation meetings and appointed a technical committee to carry out a feasibility study. In the end, it decided to prepare a voter list through BVR and to provide voters with national identity (NID) cards.

The initiation and implementation of BVR faced significant legal, logistical, administrative, political, environmental and social challenges. In particular: (a) there was no legal framework for the collection of automatic fingerprint identification system (AFIS) data or for the production and distribution of NIDs; (b) time was very limited, as the election was postponed and there was pressure to hold it as soon as possible; (c) the EC needed a significant amount of money and technical expertise and logistics for the BVR process; (d) stakeholders, especially political parties, were concerned about the BVR process and methodology; and (e) it was very difficult to reach about 75 per cent of the country's 80 million voters, as they lived in remote, rural areas, often without electricity and far from the nearest road.

In order to mitigate these challenges, the EC drafted a law and sent it to the caretaker government, which approved it with slight modifications and issued it as an ordinance, as there was no parliament at the time. To mobilize resources, the EC and the government turned to their development partners, in particular the United Nations Development Programme (UNDP), for technical assistance, as well as for support with resource mobilization and procurement. This resulted in a new project, called Preparation of Electoral Roll with Photographs (PERP), which was signed by the EC and the UNDP on 27 August 2007. The key objectives of this three-year project were the collection of AFIS data from more than 80 million voters and the distribution of NIDs. The project also received financial support from Denmark, the European Commission, the Republic of Korea, the Netherlands, Norway, Switzerland and the United Kingdom. All of the procurement was carried out by the UNDP under the PERP project, as the UNDP administered the project. Vendors were mostly international, but in a few cases, local agents supplied goods.

Concerned about the quality of the work being carried out and in an effort to ensure that every adult citizen from every corner of the country, including rural and remote areas, was registered, the EC signed a memorandum of understanding with the armed forces, given the latter's operational capacity, skilled staff and status as a government institution. The armed forces immediately set up a Central Coordination Committee that involved both the military and civil bureaucracies, which resulted in a successful civil–military partnership.

The EC managed to overcome scepticism on the part of political parties at the outset of the project. Although most parties generally favoured the BVR system in principle, they had reservations about the process, and in some cases believed it was being conducted to delay the elections. In particular, many parties were unhappy that an extended registration process would delay the election date far beyond their preferred time frame. After drafting its BVR methodology, the EC prepared a roadmap for the completion of registration and announced a date for the election. These were shared with every political party and, in the end , the parties expressed their satisfaction with how the BVR process was conducted.

Before implementation was completed, the EC undertook a successful pilot programme. For countrywide registration, 309,000 enumerators, 104,000 computer operators, 62,000 supervisors, and 6,000 officers and technical experts and support staff were recruited and trained. Over 10,000 laptops with webcams and fingerprint scanners were procured and distributed across the country.

The initiation of the BVR process encouraged people to register, as most Bangladeshis had never before had an official identification document, and the opportunity to obtain an NID was a powerful incentive to register. The EC conducted a massive awareness-raising campaign, involving civil society organizations, that encouraged people to register. This worked as a strong motivating factor for citizens to take part in the process.

In order to oversee progress, a National Steering Committee headed by the EC was formed. The committee was comprised of two election commissioners, representatives of the armed forces and officials from the EC, the government and the UNDP. The committee not only supervised the implementation, but also provided overall guidance to the Central Coordination Committee.

Success and sustainability

The EC registered 80.5 milion voters and distributed NIDs to them in just 11 months. In 2008, just before the ninth parliamentary election, the International Foundation for Electoral Systems conducted a statistical evaluation of biometric electoral rolls, commissioned by the UNDP, and confirmed that: (a) the data was captured with a high degree of accuracy; (b) there were no discernible differences by gender in the accuracy of the list; (c) the high accuracy rates were geographically uniform; and (d) nearly all eligible voters were on the list. On 29 December 2008, the postponed parliamentary election was held, and it was subsequently assessed as the 'best election in the country's history' by observers from the International Republican Institute (IRI 2009).

In order to maintain the voter list through the use of BVR technology and to continue issuing NIDs, the EC undertook several critical measures following the election. In its Five-Year Strategic Plan (2011–16), the EC established a strategic goal of 'maintaining a correct electoral roll' and established server stations at the *upazila* (an administrative term for a geographical region in Bangladesh), district and regional levels with the aim of decentralizing the service. In addition, the EC initiated a new project with financial support from the World Bank to issue smart cards to all registered voters. After some delays, the EC is planning to issue smart cards to about 100 million voters starting in late 2016. This project is known as the Identification System for Enhancing Access to Services and has a budget of USD 196 million.

Case Study 2. Fiji

Mohammed Saneem

Background

Biometric voter registration was introduced in Fiji in 2012 following the promulgation of the 2012 Registration of Voters Act. According to the Act, the Office of the Supervisor of Elections (as it was known then) was required to electronically capture biometric and biographical details for anyone applying to register to vote and, upon acceptance of their registration, to immediately issue a voter card.

In elections prior to 2012, the Office of the Supervisor of Elections would register voters through house-to-house visits, and the data would later be entered into a central database. Numerous flaws were identified in this system, and the 2006 general election observer reports by the European Union (EU) election observer group and the Commonwealth observer group noted the need for an annual update of the voter register and the establishment of a permanent and public voter database, which would improve the quality of the voter list.

The EU observer group noted the inefficiency of the 2006 voter register, which included the misspelling of voters' names, incorrect constituency allocations and the failure to register a great number of voters. The failure to correctly register voters deprived them of their right to vote.

Therefore, in 2008 the Fijian Government initiated a scoping and assessment exercise to determine the requirements for the implementation of electronic voter registration (EVR). A public tender process followed the scoping and assessment findings. Subsequently, an international vendor was engaged to design Fiji's EVR system. The vendor produced the hardware and software, which included

biometric technology, and provided the support and training required for the implementation phase.

In 2014 an Electoral Act was promulgated, and the Office of the Supervisor of Elections, which was responsible for registering voters and maintaining the database, was renamed the Fijian Elections Office (FEO).

Brief description of the new system

In order for a person to register as a voter in Fiji, they have to be a citizen and 18 years of age (prior to 2012, the voting age was 21). The 2012 Registration of Voters Act also made registration voluntary (it was previously compulsory). Applicants must also register in person. Each new voter is assigned a unique voter registration number.

Electronic voter registration is carried out using laptop computers, handheld webcams and mobile fingerprint readers. All the equipment is properly housed in custom-made waterproof kits that make them easy to carry and store. Fiji initially purchased 384 kits, and the FEO currently maintains 30 kits for updates and new registration purposes.

The BVR system operates on an SQL server that is housed in a central location. Data collected using individual kits is transferred to a flash drive and then periodically uploaded to the server. This system allows data from remote regions to be transferred to the central server without having to physically transport individual kits, and allows the kits to be continually used for registration without any disruption.

The voter registration process in Fiji involves three steps.

1. To register, new voters must complete an application form in which they provide basic personal details such as their name as it appears on their birth certificate, address, contact details, next of kin, as well as a signed declaration that all information is accurate. A valid identification card is required from all applicants.
2. The voter must submit the completed application form to a registration official, who enters the details into the BVR software. At this stage, the registration official also photographs the applicant and captures fingerprint data from his or her left and right thumb. The applicant is also assigned to the polling venue closest to their current residential address.
3. After recording all the above-mentioned data, the registration official prints out an electronic voter registration card (EVR card as it is commonly known in Fiji) and hands it to the newly registered voter.

The FEO conducts periodic data-cleaning exercises to identify potential multiple registrations, remove deceased persons (this information is provided either through notification by next of kin or through data obtained directly from the registrar of births, deaths and marriages), record changes in the details of registered voters, and any other relevant data matching and verification that may be required.

The biometric data is mainly used to identify multiple occurrences of the same person in the register. The system is not currently designed to easily allow instant voter information updates directly on the main server.

For the above system limitation, records in the central database are matched against each other once they are collected from the field. During this stage, the biometric template of each voter record is compared with every other record. Suspected matches are identified by specialized software and then examined by trained operators. If a suspected match is confirmed to be a real match, the duplicates are removed from the central database in accordance with approved procedures.

The end result is a clean voter register in which each person appears only once and is only registered to vote at one polling station.

Registration strategy

In 2012, Fiji started registering voters from scratch. The new law also changed registration dynamics significantly. Election officials would no longer be required to make house visits, but would instead invite eligible Fijians to register. The new voter cards soon gained immense popularity and became the most widely used ID card in the country. For some Fijians, it was their only official photographic ID.

In 2012, it was estimated that by 2014 (the year of the next scheduled elections) Fiji would have approximately 620,000 eligible voters. Registration was carried out in strategically planned bursts that covered the entire country. Some permanent registration centres were also established, and registration teams were also deployed to selected overseas countries.

The FEO also carries out strategic updating of the register by conducting annual secondary school registration drives to register students who have become eligible to vote. The FEO also establishes temporary registration centres around the country to allow voters to update their details. Lost cards are also replaced at these locations. There is no cost to update one's details or replace a lost card.

At the close of registration for the 2014 general election, the FEO announced that 591,101 registered voters would be eligible to vote. Table 1 shows registration figures after the introduction of the new system.

Table 1. Voter registration in Fiji, 2012–16

Year	Number of registrations
2012	505,036
2013	28,576
2014	57,489
2015	7,422
2016	8,827 (Q1 to Q3)

Key achievements of the use of EVR system:

- historic creation of a single national register of voters, which is stored electronically;
- the FEO is able to register new voters in areas without an Internet connection;
- data-matching features of the software allow the FEO to detect potential multiple registrations and keep the register up to date and clean;
- continuous updating of the register, which is recognized as an international best practice;
- for the first time, the FEO is able to provide instant statistics on the voter list, which is useful for planning and operational purposes.
- However, there were also some challenges with BVR, including:
- staff training and quality assurance practices were developed as lessons were learned from experience, for example no guide was available for the operation of BVR systems;
- technical issues with the software that required intervention by the supplier, even after Fiji had recorded data. Ideally, the supplier should not have access to the software after supply;
- too expensive for developing countries to maintain, as there are recurring costs associated with licences for kits and so on. Laptops and other devices have relatively short lifespans, and in addition to the expense of replacing equipment, there are costs of reloading existing software onto newer machines;

- updating the voter list: there needs to be a more practical approach to ensuring that the voter list is up to date. It is essential that data on migration, deaths and so on is noted in the system to ensure that it provides accurate figures; and
- reporting interfaces and data handling need to be more properly defined. The current system requires a great deal of IT specialization and should be made more user friendly.

Conclusion

The EVR system maintained by the FEO is regarded as one of the most trusted and up-to-date databases of Fijians over the age of 18. The EVR card that is issued by the FEO is also a universally accepted ID card in Fiji.

There is still room for improvements to the biometric registration tools available on the market. It is not feasible for smaller economies to develop customized tools. There is also a need for more literature on dealing with data accuracy, data security and information accuracy management.

While Fiji has managed to maintain a secure and up-to-date register of voters, it is now feeling the pressure of changes in technology and the cost of purchasing licences to maintain its registration kits.

Case Study 3. Mongolia

Tamir Zorigt

Background

As of 2016, Mongolia has a population of approximately 3 million, including 1.9 million registered voters (International IDEA Voter Turnout Database) who are eligible to vote at nearly 2,000 polling stations. Each polling station serves up to 2,000 voters in one soum (second-level administrative subdivision), up to 2,500 voters in one aimag (first-level administrative subdivision) centre and up to 3,000 voters in one capital district. While almost half of the population lives in the capital, Ulaanbaatar, the remainder is spread throughout a vast country stretching over three time zones and partly rough terrain with limited infrastructure, particularly in about 300 remote locations where telecommunication networks are not yet available or have limited connections.

Until 2008 the voter register was compiled manually using a paper-based population register. During the regular parliamentary election held in 2008 certain mistakes and weaknesses were recorded, such as politicization, group divisions and delays in releasing the election results. Eventually, a civic protest spun out of control and led to mass unrest. The parties represented in parliament responded by agreeing to introduce automation in elections and endorsed the Law on an Automated Election System. Subsequently, information and communication technology (ICT) upgrades, including a new voter registration and voter identification system, were introduced in an attempt to restore the credibility of the electoral process.

Introducing a biometric voter registration and identification system

The introduction of biometric technology for elections was facilitated by the establishment of an electronic civil register, including a database with personal information, fingerprints and photos of all registrants.

The General Authority for State Registration (GASR) started work on the new civil register in 2011, and by the end of the year most of the country's population aged 16 and above was enrolled. Soum and district assemblies create election precincts based on the database on permanent places of residence from administrative and territorial units in consideration of GASR suggestions. A BVR compiled using this process was used for the first time for the parliamentary elections in 2012.

Preparing the voter identification system for polling stations

When a new voter register for an upcoming election is required, all necessary data is exported from the civil registry. The GASR prepares laptop computers for polling stations—one computer for every 1,500 voters—to which it exports all biographical and biometric data on eligible voters. The Working Group on Automated Election System Certification, consisting of the General Intelligence Agency of Mongolia, the Communications and Information Technology Authority and the General Election Commission (GEC), participates in, supervises and certifies the export process, system configuration, registration software and other equipment. Each laptop is complemented with a fingerprint scanner, a printer and a video projector or large monitor. All hardware, software and data related to this system are maintained by the GASR.

The GASR is in charge of the voter registration and identification process, and the GEC has no role.

Voter identification system and procedures at polling stations

The voter identification system is offline on election day and requires no network connectivity. If two computers are needed per polling station, they can be connected directly through a local area network. a voter's eligibility, his or her fingerprint is scanned.

If the fingerprint can be matched against the record of an eligible voter in the registration database, the voter's picture is shown on a large screen so that everyone in the polling station, including observers, can identify the voter. The voter is issued a paper receipt and may proceed to cast his or her vote.

If the fingerprint is not recognized, the voter's details are looked up manually in the database. If the manual search is successful, the system emits a loud beep to alert all poll workers, witnesses and observers present in the polling station. Then a picture of the voter from the registration database is shown on a large screen in the polling station so that everybody present can compare the image and the voter. The voter is then issued a paper receipt and may proceed to cast his or her vote.

If a person cannot be found in the register or if an eligible voter is found but already marked as having voted, no receipt is issued, and the person is not allowed to vote.

Impact

During the parliamentary election in 2016, 1.4 million (74 per cent) of all registered voters were identified by the voter registration system. About 70,000 (5 per cent) of these voters were looked up manually in the database either because their fingerprint could not be verified or because their biometric data was not included in the laptop computer due to the temporary change of residence of voters.

Most voters seemed to have trust in the new voter registration system, and no major problems were reported. The current system is expected to be used again for the next elections.

Case Study 4. Nigeria

Chidi Nwafor

Background

Prior to the adoption of technology for use in Nigeria's electoral process, the voter register had been compiled manually. The manual register could not be updated, was fraught with inaccuracies and was believed to be bloated with underage and duplicate registrations.

In 2002, the Independent National Election Commission (INEC) started ICT upgrades with the introduction of optical mark recognition (OMR) technology for voter registration. The register produced from this exercise was used for the 2003 elections but was discarded because of the enormous number of exceptions that resulted from forms that had not been completed properly.

In 2006 the INEC came up with the concept of an electronic voting system with four components: an electronic voter register, electronic voting machines, electronic voter authentication and electronic transmission of results, in which biometric technologies are now used for the voter register and voter authentication.

Beginning in 2006, handheld direct data capture devices were used for voter registration. Some 32,000 devices captured details that included biographical data, two thumbprints and a photograph of each registrant. These registers were used for the 2007 general elections. However, due to the irregularities associated with the registers—not the technology itself—the registers were abandoned. The irregularities arose from the late arrival of machines, which forced people to go looking for machines instead of waiting for the machines to be deployed to centres close to them, which led to double registrations and misplaced voters.

The 2011 Direct Data Capture Machines (DDCMs) Project

A new Election Commission was inaugurated in June 2010, and elections were scheduled for January 2011. At the time, problems included the need to amend the electoral law, a lack of funds and the need to balance the cost and effectiveness of the voter registration process. As a result, the development of an open-source voter registration system was deemed the most appropriate solution to respond to Nigeria's need for a simple, secure, fast and reusable process.

Two major bottlenecks were time and cost restraints for procuring the required 132,000 registration systems for 120,000 polling units. Only two months before the commencement of registration, contracts for the supply of 132,000 DDCMs were awarded to three vendors at a total cost of USD 234 million.

The open-source voter registration (Open VR) software was built using open-source technologies, and the biometric image software suite developed by the National Institute of Standards and Technology was used for the comparison and analysis of biometric data.

The DDCMs captured the biodata, photograph and all 10 fingerprints of most registrants. The resulting voter register was considered to be the best ever produced by the INEC and was used for the general elections in 2011 and 2015.

Voter accreditation at polling stations

The voter accreditation process takes place on election day to ensure that each voter is registered to vote at the polling station.

Voter accreditation had previously been performed manually, thus exposing the process to manipulation and fraudulent practices. This process was improved in 2011 with the introduction of paper registration slips and accreditation before voting, ensuring that voting commenced at about the same time at all polling stations.

Permanent voter cards

For the 2015 general elections, the INEC decided to use technology to optimize the process by introducing permanent voter cards (PVCs) and smart card readers (SCRs).

Among the different card technologies available, PVCs were chosen that used a contactless chip card, since they are difficult to counterfeit and tamper with and last for up to 10 years. The PVCs are smart-card-based and store voter information including biodata, biometrics and a photograph.

The PVC project was initiated in 2012, and cards were printed for voters still on the register after the voter register optimization process, which included data

consolidation and deduplication. A total of 73.5 million initial cards were printed at a total cost of USD 31.8 million. The unit price for the subsequent production of PVCs increased from USD 0.50 to almost USD 2.00.

Smart card readers

To take full advantage of the PVCs, it was decided to use SCRs for the identification and authentication of voters during the 2015 general elections. SCRs are used to verify that a PVC presented at a polling station was issued by the INEC and to authenticate that the bearer of the PVC is the legitimate owner of the card through fingerprint matching. Once a PVC was read and verified by the SCR, the voter identification number was stored in the reader, and repeat verification of the same PVC on that particular reader was no longer allowed.

The accreditation process was broken down into three phases: (a) identification, which involved a physical comparison of the card holder with the image displayed on the SCR when the PVC was read; (b) verification (that the card was authentic), which involved checking that the information on the chip could be read; and (c) authentication, which involved matching the fingerprint stored on the card with that of the voter.

The INEC procured a total of 182,000 SCRs for all 152,000 voting points in the country. Each SCR cost about USD 188 in 2014–15, yet a recent market survey showed an increase to about USD 300 per unit.

Equipment testing and certification

The SCRs were extensively tested by an independent assessor from the United States and certified to comply with requirements, specifications and international technical standards.

To test the system, a mock accreditation exercise was conducted in selected areas to assess the average duration of the authentication process, the ability to check all voters during accreditation hours, the lifespan of the system's power supply and the frequency of failed verifications, and the overall added value of the SCRs to the accreditation process.

Relevant findings included that verification of PVCs took less than two seconds. Authentication of fingerprints was more difficult for some voters, this process took much longer or even failed entirely in some cases. There were cases involving faulty chip encoding in the PVC, which were noticed because the voter's details shown on the SCR screen after verification were different from the voter's biodata contained on the card. Mishandled or mutilated PVCs were also observed. Interestingly, the results varied greatly depending on the location. While some states had an outstanding percentage of successful accreditations of

up to 92 per cent, other states had only around 36 per cent and a mere 3.4 per cent in one state.

These observations helped the INEC determine the guidelines for voter accreditation on election day. The difficulty of successfully authenticating some voters led the commission to decide that once a PVC was read by a card reader (successful identification), the voter should be allowed to vote even if authentication failed.

Case Study 5. Uganda

Pontius Namugera

In recent years the Electoral Commission of Uganda (ECU) has undergone a revolution of technological advancements towards the computerization of its core activities, with the aim of achieving free and fair elections. One of the ECU's core functions is to compile, maintain, revise and update the national voter register.

In 1980 Uganda had a handwritten register that could only be used once. Since 1993 the process of updating the voter register has been progressively computerized to enable easy updating, use and maintenance. During the general election of 1996 the voter register was manually compiled in handwritten notebooks. These notebooks were collected, and a central register was compiled and reproduced using typewriters and photocopiers. In 2001 the voter register was further improved by using, for the first time, computer technology to add information about voters to a Microsoft Access database, after which voter registers were printed using laserjet printers.

Uganda's first biometric voter registration

The ECU first introduced a biometric voter register in 2001 with the implementation of the Photographic Voter Registration and Identification Systems (PVRIS) project, becoming one of the first adopters of biometrics in Africa. At the time, voters were registered using a digital camera to capture a photograph of the voter, and biographical data was captured using a paper-based registration form. The project introduced the use of a photograph-based voter register at polling stations during all election activities.

Prior to the PVRIS project, the national voter register was text only and had grown to encompass a voter population of approximately 11.5 million. After the

implementation of PVRIS, the registered voter population was reduced to 8.5 million. The ECU used facial-recognition software to identify and eliminate cases of multiple registration. Data entry was conducted using high-speed scanners and optical character recognition software to interpret handwritten forms into text data before storage. The Photographic National Voter Register was first successfully used countrywide during the 2006 elections.

Despite the success of the PVRIS, a few challenges related to the voter register remained. There were some cases of multiple voting that the facial recognition system did not detect. The low quality of the images affected the results of the FRS and by 2010, images captured in 2001 had aged and could no longer be easily checked. Some voters did not have a photo because of corrupted images on the floppy drives used to store the images. Furthermore, in several cases a photo was attached to the wrong person's data.

In view of these challenges, the ECU planned to improve the method used for voter registration in preparation for the 2011 general elections. In 2010 the ECU embarked on the implementation of a BVR system. This commenced with a countrywide pilot phase during the general update of the voter register.

The BVR system was introduced by using equipment acquired by the Ugandan Government under the National Security Information System (NSIS) project, which was being implemented by the Ministry of Internal Affairs. During the implementation process, the ECU used mobile data capture units (comprising a laptop computer, camera, signature pad and other peripherals) which were integrated into a registration kit. The new system electronically captured biographical data, demographic data (each voter's assigned polling station, residential address and so on), 10 fingerprints per voter, photographs and signatures. This pilot phase added about 4.2 million new voters. The system used an FRS and an AFIS to identify and eliminate multiple registrants and produced a clean voter register of 13.9 million voters for the 2011 general elections.

Biometric Voter Registration and National ID Project

In 2013 the Government of Uganda recognized that several institutions had all requested resources for registering citizens, including the Uganda Bureau of Statistics, to conduct a population census; the Uganda Registration Services Bureau for Birth and Death and Marriages; the Citizenship and Immigration Board, for the purposes of issuing identity cards, and the Electoral Commission.

This potential level of duplication prompted the Cabinet to formulate a multi-institution task force made up of key stakeholders under the leadership of the Ministry of Internal Affairs, with the aim of:

- developing a mass registration strategy;

- creating a roadmap for a mass registration programme;
- developing a unified budget; indicating the anticipated short-, medium- and long-term savings compared to each institution independently conducting its own registration exercise;
- advising on a governance structure, as well as the roles and responsibilities of the participating institutions.

Subsequently, a mass enrolment strategy and budget were developed and approved by the Cabinet. The strategy's objectives were to:

- identify and register Ugandan citizens and issue them unique national identification numbers and national ID cards;
- register citizens 16 years of age and older for the purpose of producing a clean voter register in time for use in the 2016 elections; and
- register resident aliens and issue them alien ID cards.

This exercise was implemented using a multisectoral approach. In addition to the ECU, participating institutions included the Directorate of Citizenship and Immigration Control, the National Information Technology Authority Uganda, the Uganda Registration Services Bureau, the Uganda Bureau of Statistics and supporting agencies, including the Uganda People's Defensce Force, the Uganda Police Force and the Uganda Prisons Service.

The various institutions contributed human resources, office space, furniture and vehicles to the mass enrolment exercise, which was called the National Security Information System. Each participating institution contributed to the specification of the system during the development phase, including the mandatory data fields required by each individual institution. The ECU made sure that all data required to extract the national voter register from the NSIS was captured in the enrolment exercise.

Countrywide enrolment of all citizens was initially conducted for four months at the parish level with approximately 8,000 enrolment kits and two operators per enrolment kit. Within this period, a total of 16.7 million people were enrolled. The exercise was extended for five months at the subnational level to allow those who had missed out on the mass enrolment exercise to register.

There were different laws governing the registration of individuals for various purposes for the ECU and the other participating institutions, and there was a need to harmonize these laws, and so the 2014 Registration of Persons Bill was passed. It provided for access to, and the use of, the data collected from the mass enrolment and created the National Identification and Registration Authority (NIRA).

Extraction of data from the NIRA for the compilation of the national voter register used in the 2016 general elections

The ECU extracted data from the NIRA database to compile the national voter register. The data included all vital information required for the voter register, including biographical data, biometric data (images and all 10 fingerprints) and demographic data, including each voter's assigned polling station. Only data that met the eligibility criteria for a voter was extracted.

From the extracted data, the ECU was able to create a preliminary national voter register which was later updated and publicly displayed, after which the final voter list was produced.

The process of registering new voters is now simpler because the NIRA continuously registers citizens so as to issue them national ID cards, and the ECU extracts additional data from the NIRA whenever there is an election. The ECU does not spend any more on registration and data processing than it used to. Similarly, the acquisition and maintenance of the registration kits and the expensive hardware and software for deduplication (FRS and AFIS) is the NIRA's responsibility.

While not quantified, savings were achieved by sharing resources between participating organizations at the national level and across the country, including vehicles, office space and staff; using equipment purchased by the government to serve multiple purposes; and collecting data in the field (which is very costly) once instead of separately for each organization.

The fingerprint data contained in the ECU's biometric voter register was also used by the biometric voter verification system (BVVS) that was deployed at every polling station during the 2016 general elections.

The deployment of biometric verification devices at polling stations across the country was very successful, and it had a significant impact on the credibility of the presidential, legislative and local council elections. The BVVS was primarily meant to eliminate voter fraud originating from voter impersonation and multiple voting. Additionally, the BVVS proved effective at helping voters identify their correct polling station. Most observers of the 2016 general elections noted that the system worked satisfactorily without any technological failures.

A total of 32,334 devices were deployed to cover 28,010 polling stations, and some spares were kept in strategic locations. Most of these devices were leased rather than purchased outright. This saved the EUC approximately 25 per cent compared to purchasing the equipment.

Case Study 6. Zambia

Brown Kasaro

The introduction of biometric technology in Zambia followed electoral reforms that were instituted after the 2001 general elections. Voter registration was identified as one of the key areas to be addressed. A law requiring the Electoral Commission of Zambia (ECZ, the country's EMB) to conduct continuous voter registration was passed. The ECZ was required to come up with a new register of voters with the following the key features: the register and voter cards had to include photos of voters; voter cards were to be issued immediately upon registration; and strict checks for duplication were to be carried out.

A medium technology solution was implemented in 2005, leading up to the 2006 general elections that used optical mark recognition (OMR) technology. OMR-based forms and Polaroid cameras and ink pads were used to record details about each registrant in the field in addition to photos and fingerprints. An AFIS was also used for centralized deduplication of the database.

The biometric system and processes in place

The ECZ introduced biometric technology for voter registration data capture in 2010, leading up to the 2011 general elections. The decision was made following the demise of Polaroid technology. The ECZ had the option to replace Polaroid technology with digital photo kits (thereby continuing with OMR forms) or replace the old solution with biometric kits.

Biometric kits were chosen because the technology:

- was suited to continuous voter registration, in that the existing register could be preloaded onto kits during registration update drives;

- enhanced the accuracy of the register by facilitating data validation at the point of capture;
- enabled the ECZ to conduct registration through mobile campaigns, thereby reducing the number of kits to be procured and thus decreasing the cost of voter registration; and
- did not require changes to backend systems that the ECZ had already implemented, including the AFIS.

The ECZ updates the permanent register, which contains about 6.7 million registrants, at least once before every general election through mobile registration campaigns. These campaigns are complemented by a national voter education and publicity campaign. The last registration campaign, in 2015, lasted 90 days and used 2,000 biometric kits to capture data from 7,700 registration centres. The biometric kits operate offline. The biometric data captured are fingerprints and photos. Fingerprints are used for the AFIS deduplication process of the entire national database, while the photos are printed on both the card and in the register to help polling officials visually identify voters. Although voter cards are issued upon registration, the AFIS deduplication process is centralized.

The ECZ does not carry out biometric voter verification on polling day. Voter identification is done manually, using voter cards, national ID cards and the register for each polling station. Indelible ink is also used to deter multiple voting.

Project implementation

The ECZ received support from donors for the introduction of biometric kits in 2010 through a basket fund that was managed by the UNDP country office. The procurement of the kits was facilitated by the UNDP in close collaboration with the ECZ.

The basket fund also helped the ECZ build in-house capacity to upgrade its backend system to manage voter registration data and to prepare the registers. The ECZ maintained the AFIS that was implemented in 2005 and upgraded it through the vendor.

Projected implementation started with the procurement process in September 2009. The kits were delivered in April 2010, and the registration campaign commenced in June 2010 after staff were trained.

Synergies with national registration

To register as a voter in Zambia, a person must be a citizen aged 18 years or older who has a national identity card. National ID cards are issued by the Department

of National Registration under the Ministry of Home Affairs once an individual reaches 16 years of age.

The national registration process is still manual, thereby limiting the level of possible collaboration with the ECZ. The National Registration Department is in the process of computerizing its operations and is developing a fully biometric civil register.

Future plans

The ECZ hopes to take advantage of a full biometric national register that, once implemented, will help in preparing the voter register. Some of the possibilities being envisaged are: using a single card for voting (the national ID card) and eliminating AFIS processing by the ECZ by accessing the civil registration infrastructure.

References and further reading

ACE Electoral Knowledge Network (ACE project), ACE Encyclopaedia, <http://aceproject.org>, accessed 8 September 2016

Alim, A., *Electoral Governance and Political Parties: Bangladesh Perspectives*, PhD Thesis (Dhaka: Jahangirnagar University, 2014)

Bolle, C. and Pankanti, R., Sr, *Guide to Biometrics* (New York: Springer, 2004)

Catt, H., Ellis, A., Maley, M., Wall, A. and Wolf, P., *Electoral Management Design: Revised edition* (Stockholm: International IDEA, 2014), <https://www.idea.int/publications/catalogue/electoral-management-design-revised-edition>, accessed 1 November 2016

Clouser, M., Krimmer, R., Nore, H., Wolf, P. and Schürmann, C., *The Use of Open Source Technology in Elections* (Stockholm: International IDEA, 2014), https://www.idea.int/publications/catalogue/use-open-source-technology-elections>, accessed 1 November 2016

Coalition of Domestic Election Observers, *Promoting a Peaceful, Transparent, and Credible Biometric Voter Registration Process: Ghana's Election 2012* (Accra: Ghana Center for Democratic Development, 2013)

Das, R., *Adopting Biometric Technology: Challenges and Solutions* (Boca Raton, FL: CRC Press, 2016)

Electoral Institute for the Sustainability of Democracy in Africa (EISA), *Voter Registration in Africa* (Johannesburg: EISA, 2010)

European Union, Election Observation Mission Fiji 2006, *Final Report (*Suva: European Union, 2006)

European Union, United Nations Development Programme (UNDP) and International IDEA, *Procurement Aspects of Introducing ICT Solutions in Electoral Processes: The Specific Case of Voter Registration* (Brussels: Joint EC-UNDP Task Force on Electoral Assistance, 2010), <http://www.undp.org/content/undp/en/home/librarypage/democratic-governance/electoral_systemsandprocesses/procurement-aspects-of-introducing-ict-solutions-in-electoral-pr.html>, accessed 1 November 2017

Fijian Elections Office, Voter Registration, [n.d.], <http://www.electionsfiji.gov.fj/voter-registration/>, accessed 7 October 2016

International Institute for Democracy and Electoral Assistance (International IDEA), *Certification of ICTs in Elections* (Stockholm: International IDEA, 2015), <https://www.idea.int/publications/catalogue/certification-icts-elections>, accessed 1 November 2016

—, ICTs in Elections Database, <http://www.idea.int/data-tools/data/icts-elections>, accessed 8 November 2016

—, Voter Turnout Database, <http://www.idea.int/themes/voter-turnout>, accessed 8 November 2016

International Republican Institute (IRI), *Election Observation Mission Final Report: Bangladesh Parliamentary Elections December 29, 2008* (Washington, DC: International Republican Institute, 2009)

A. Jain, P. FlynRen and A. Ross (eds), *Handbook of Biometrics* (New York: Springer, 2008)

Knight, K. et al., *Fiji Islands General Elections 6-13 May 2006, Report of the Commonwealth Observer Group* (London: Commonwealth Secretariat, 2006)

National Instiutue of Justice, *The Fingerprint Sourcebook* (Washington, DC: National Instiutue of Justice, 2011)

Schaffer, F.C., *The Hidden Costs of Clean Election Reform* (New York: Cornell University Press, 2008)

Contributors

Abdul Alim is a democracy and elections practitioner in Bangladesh who has spent the past 17 years working for free, fair and credible elections. He is currently the Director of EWG/Elections at the Asia Foundation. He has experience in managing large election programmes with the UNDP, the Asia Foundation, the National Democratic Institute and Transparency International. He also collects data for various International IDEA databases. In 2008–12, he worked closely with Bangladesh's Election Commission and provided policy advice on various issues in conducting the successful ninth parliamentary election in a conflict political situation. Alim holds a PhD and is the author of 10 fundamental research publications mainly on electoral governance.

Brown Kasaro is an electoral technology specialist with experience in the implementation of electronic election results management systems and biometric voter registration systems, as well as the introduction of technology in election processes in general. Kasaro has over 10 years of technology leadership experience with the Electoral Commission of Zambia.

Pontius Namugera is the Director of Technical Support Services for the Uganda Electoral Commission. He holds a Bachelor of Science in Mathematics from Makerere University in Kampala, Uganda, and a Master of Science in Information Systems from Boston University in the United States. He has 14 years of experience working with election technologies, including voter registration, results transmission and implementation of large-scale IT projects. He has worked on a number of international missions in Afghanistan, Kenya and Zimbabwe.

Mohammed Saneem is the Supervisor of Elections for the Fijian Elections Office (FEO). He was appointed to his position in 2014. He is responsible for conducting national elections, as well as the registration of voters, political parties and candidates. Under his leadership, the FEO conducted the 2014 general election after a lapse of eight years and under a new electoral system. Saneem also serves as a representative to the Steering Committee of the Commonwealth Electoral Network, the Melanesian representative to the PIANZEA Advisory Group and the Association of World Electoral Bodies. He began his legal career in private practice in Fiji. Prior to his appointment as Supervisor of Elections, Saneem served as the Acting Permanent Secretary responsible for Elections and Registrar of Political Parties, and Acting Permanent Secretary for Justice, Anti-corruption and Communications. He currently chairs the National Anti-Money Laundering Council. Saneem obtained a Professional Diploma in Legal Practice and Bachelor of Law from the University of the South Pacific.

Peter Wolf is a member of the Electoral Processes Programme at International IDEA. He has focused on ICT applications in electoral processes since joining the Elections Department of the OSCE mission in post-war Bosnia and Herzegovina, where he worked on voter registration and results databases. He served as a consultant in voter registration projects in Albania, the Democratic Republic of the Congo and Iraq, and has participated in various international election observation missions, including as an electronic voting expert in France, Kazakhstan, Kyrgyzstan, Venezuela and the Philippines. He holds a Master of Science degree from the Graz University of Technology.

Tamir Zorigt is a System Security Engineer at the General Election Commission of Mongolia. On five separate occasions, he has been a member of the Working Group on Automated Election System Certification, which is mandated to certify the automated election system for use in Mongolian elections.

About International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization with the mission to advance democracy worldwide, as a universal human aspiration and enabler of sustainable development. We do this by supporting the building, strengthening and safeguarding of democratic political institutions and processes at all levels. Our vision is a world in which democratic processes, actors and institutions are inclusive and accountable and deliver sustainable development to all.

What do we do?

In our work we focus on three main impact areas: electoral processes; constitution-building processes; and political participation and representation. The themes of gender and inclusion, conflict sensitivity and sustainable development are mainstreamed across all our areas of work. International IDEA provides analyses of global and regional democratic trends; produces comparative knowledge on good international democratic practices; offers technical assistance and capacity-building on democratic reform to actors engaged in democratic processes; and convenes dialogue on issues relevant to the public debate on democracy and democracy building.

Where do we work?

Our headquarters is located in Stockholm, and we have regional and country offices in Africa, the Asia-Pacific, Europe, and Latin America and the Caribbean. International IDEA is a Permanent Observer to the United Nations and is accredited to European Union institutions.

<http://www.idea.int>

A credible voter register gives legitimacy to the electoral process and helps prevent electoral fraud. However, voter registration remains a complex and contested task. It is one of the most important activities that an electoral management body needs to conduct, but it is also one of the most costly in terms of both time and resources.

Many countries that face challenges in creating an accurate voter register are considering reforming their voter registration systems through the introduction of biometric technologies. The drive towards biometrics has been facilitated by its largely apolitical nature. Investing in high-tech solutions allows stakeholders to demonstrate their commitment to resolving electoral problems. At the same time, expectations on biometric solutions may be exaggerated.

This Guide provides an overview of key concepts and considerations for all stakeholders involved in discussions about the application of biometrics in elections, both for voter registration before an election and for voter verification at polling stations on election day.

International IDEA
Strömsborg
SE–103 34 Stockholm
Sweden
Telephone: +46 8 698 37 00
Email: info@idea.int
Website: ‹http://www.idea.int›

ISBN: 978-91-7671-205-4 (PDF)