DO NOT MIX TRUTH WITH FALSEHOOD OR HIDE THE TRUTH KNOWINGLY.

AYAT 42, SURAH BAQARAH, AL QURAN

THE REPORT ON ELECTRONIC VOTING MACHINE (EVM) & OVERSEAS VOTING

OVERSEEING CHALLENGES, RECOMMENDATIONS & WAY FORWARD

March, 2022

TABLE OF CONTENTS

ABBREVIATIONS

ECP	Election Commission of Pakistan
EVM	Electronic Voting Machine
DRE	Direct Recording Electronic
PCOS	Precinct Count Optical Scanning
CCOS	Central Count Optical Scanning
VVPAT	Voters Verified Paper Audit Trail
EMB	Election Management Body
R & D	Research and Development
BVM	Biometric Verification Machine
NADRA	National Database and Registration Authority
E-Voting	Electronic Voting
I-Voting	Internet Voting
PMU	Project Management Unit
IVTF	Internet Voting Task Force
E2EV	End to End Verifiability
Minsait	Spanish Cybersecurity Audit Firm
COMELEC	Commission on Election (Philippines)
DDoS	Distributed Denial of Service
Forex	Foreign Exchange
CCTV	Close Circuit Television
SMS	Short Message Service
RLA	Risk Limiting Audit
CU	Control Unit
BU	Ballot Unit
CNIC	Computerized National Identity Card
SLA	Service Level Agreement
GPS	Global Positioning System
RTS	Result Transmission System
A-WEB	Association of World Electoral Bodies
NICOP	National Identity Card for Overseas Pakistanis
EPROM	Erasable Programmable Read Only Memory
ATM	Automatic Teller Machine
SEC	Superior Electoral Court (Brazil)
PST	Public Security Test (Brazil)
OMR	Optical Mark Recognition
DEFCON	Defense Condition
ECI	Election Commission of India
TSE	Tribunal Superior Electoral
Nedap	A Dutch Multinational Technology Company
ICT	Information Communication Technology

EXECUTIVE SUMMARY

INTRODUCTION

The debate on the use of Electronic Voting Machines (EVMs) in Pakistan dates back over a decade. In 2009, the Election Commission of Pakistan (ECP) commissioned a feasibility study on EVMs which recommended that "*use of electronic voting and counting technologies be pursued further, although a final decision on the national adoption of these technologies will remain pending*". Since then, the ECP has arranged demonstrations of EVMs developed by COMSATS, TIP, KRL, NIE, Smartmatic, and Indra, and, in 2012 and 2015, conducted field tests for EVMs and BVMs in Multan and Haripur respectively. ECP also acquired 150 EVMs manufactured by Smartmatic and, following promulgation of the Elections Act, 2017, piloted the machines in Peshawar bye-elections.

The issue of electoral reform resurfaced in late 2020, focusing principally on Electronic Voting Machines (EVMs) and Internet Voting (IV). In the Elections (Amendment) Act 2021, [1]ECP was required to procure EVMs for use in the General Elections. Thereafter, the ECP constituted three Committees including Technical Evaluation Committee with a mandate to provide concrete recommendations on the feasibility and roadmap for introducing EVMs in the forthcoming General Elections. The other two Committees include a Financial Committee and a Legal Committee with their own mandate. The detailed Terms of Reference (ToRs) of all three Committees are attached at **Annex-A**.

This document presents the views and findings of these Committees and gives a comprehensive account of the challenges and risks involved in adopting such a course together with presenting a detailed, research oriented roadmap based on highlighting stories from successful countries engaged in use of such technology. The report also presents findings of the Internet / Overseas Voting aspect.

[1] Elections (Amendment) Act, 2021, https://senate.gov.pk/uploads/documents/1623649621_687.pdf

WHY EVMs?

EVMs have a history of evolution internationally and various advantages which stand to benefit the polling process. EVMs counter certain forms of electoral rigging, improve efficiency of polls, and yield more accurate results. EVMs also reduce operational costs over a length of time, make elections more inclusive, and they are known to improve voter confidence in elections.

However, EVMs also bear formidable challenges: EVMs are not always transparent as they are vulnerable to hacking and malfunctions. They can be problematic to use in regions where technical literacy is low. EVMs typically have considerably high initial costs and there are sustainability concerns about deploying them in developing countries with considerable maintenance cost. There are no general standards or certifications to deploying EVMs and each country must evolve its own best practices, which require time and research. Considerable controversy persists around EVMs, even in countries like India, Venezuela, and the United States, which have been using them for decades.

Most importantly, however, EVMs require a vast supporting ecosystem, which includes issues of logistics, infrastructure requirements, procedural mechanisms, legal and political concerns, detailed cybersecurity protocols and more. The research literature identifies the ecosystem as a key overlooked factor and why election technology deployments tend to fail in practice.

Types of EVMs – A Global Perspective

Electronic voting is not a new phenomenon. The first widespread use was in the USA, in the 1960s when punched card systems were used. In this section, a summary is presented to demonstrate different voting technologies currently used in different parts of the world, including United States, India, Brazil, Philippines, and Canada.

1.1 TYPES OF ELECTRONIC VOTING MACHINE (EVM)

A) Precinct Count Optical Scanning (PCOS) Machines

PCOS Machine in Philippines, used in 2010 and developed by M/s Smartmatic

Ballot papers are marked using a pen/ marker, a digital pen or an electronic marking device. These marked ballot papers are input to the Optical Mark Recognition (OMR) based scanning and counting device. OMR is the same technology used to mark standardized tests. This can be done at each precinct, or all the marked ballots can be collected at a centralized location for the tabulation, in which case the system is called central-count voting system.

Deployment and Price Estimate: PCOS systems are deployed in Philippines, with price estimates of each unit costing around 1600 USD[2]

Pros	Cons
Marked paper ballots enable audits to be carried out	Marked paper ballots are susceptible to traditional risks, such as ballot box stuffing, and ballot destruction
Faster speed of tabulation	Numerous machine malfunctions have been reported.
Paper legacy will continue for ease of voters	Marking on a specialized ballot may be cumbersome. Requires excessive awareness
Quick declaration of results at the polling stations. It works as counting machine	Voter training and awareness required to help them mark ballots. Possibility of invalid votes remains

[2]CNN: Comelec to lease 94,000 new machines for 2016 elections, https://cnnphilippines.com/news/2015/08/13/Comelec-decision-lease-94K-new-machines.html

B) Direct Recording Electronic (DRE) Voting Technology

Brazilian DRE *First DRE in the US developed 1991 consortium of state bodies*

The machine records votes by means of a ballot display, which may be accompanied by buttons or touch screens to directly record the voter's choice, hence the name Direct-Recording Electronic voting machine. The machine records votes electronically only and no paper trail is generated. The machine may transmit individual ballots or vote totals.

Deployment and Price Estimate: It has been used in the USA and Venezuela. Currently Brazil is the country with a nationwide deployment of machines, each machine price estimated to be around USD 700[3]

Pros	Cons
Cost efficiency due to elimination of paper	Typical example of a black box that depicts lack of transparency
Eliminates, undervotes, over votes and invalid votes	No guarantee of EVM software honest or bugged and functioning properly
Quick result compilation	No paper trail for auditing

C) DRE Voting Technology with VVPAT

Indian EVM with VVPAT

[3] Brazil's electronic voting machine comes of age, https://cnnphilippines.com/news/2015/08/13/Comelec-decision-lease-94K-new-machines.html

In the direct-recording electronic voting machine, the voter has no guarantee that their vote was recorded as cast. This makes the voting process opaque and lacks the guarantees to convince stakeholders of a free and fair election. The DRE-VVPAT voting machines, along with recording the vote, produce a paper print out of the vote. This printout can be inspected by the voters, to verify their vote was cast as intended. This Voter Verified Paper Audit Trail (VVPAT) can then be inserted in a ballot box automatically, straight from the voting module or manually by the voter.

Deployments and Price: DRE-VVPATs are used extensively in the USA and nationwide in India for national level elections. The Indian model has an estimated price of US $229[4].

Pros	Cons
Voters mark their vote directly into an electronic device	Requires excessive awareness & training
No invalid votes	The paper trail is only useful when post-election audits are carried out.
Fully Auditable system	The paper trails are susceptible to destruction, ballot box stuffing.
Quick result compilation	Highly costly in terms of logistics and transportation. Storage issues and use of more human resource to handle it

D) Public Network connected DRE (Direct Recording Electronic)

Developed in US by Votronic

ExpressVote XL by Election Systems Software (ES&S)

Such machines transmit the recorded electronic ballots and transmit vote data from polling stations over a public network, such as the internet. Vote data may be transmitted as individual ballots, periodically as batches of ballots throughout the election day, or as one batch at the close of voting, and are generally tabulated centrally.

[4] https://www.eces.eu/template/default/documents/E-Voting%20in%20Nigeria%20-%20ECES.pdf

Deployment and Price: These machines have been used in Switzerland, UK on an experimental basis and no price estimates are available.

Pros	Cons
Voters mark their vote directly into an electronic device	High-end secure network is needed for safe voting and it's very expensive and always prone to hack.
No invalid vote	Lacks transparency and fragile machine is not rugged that can be used in difficult terrain such as desert, mountains and under extreme temperatures.
Quick results compilation	Lack auditability features

E) EVM with Paper Ballot

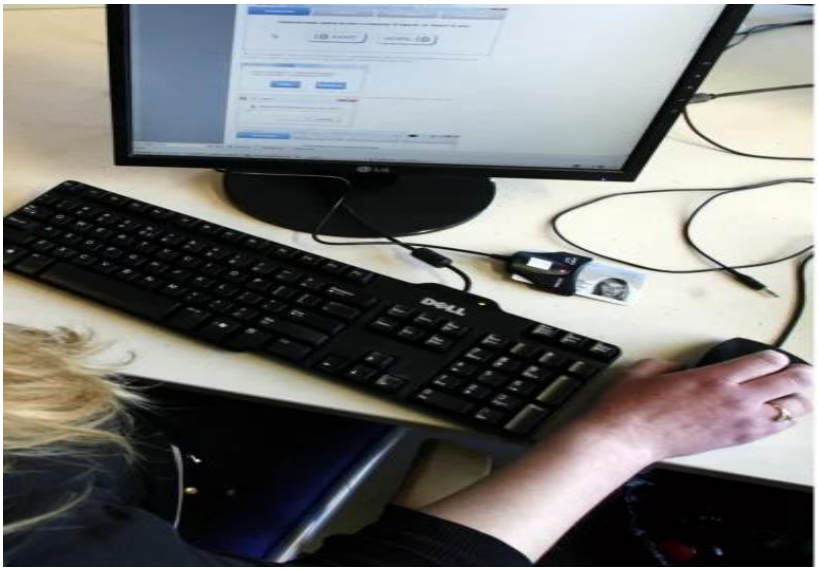
EVM in Bangladesh, assembled by Bangladesh Machine Tools Factory after importing parts

The voter marks his choice using a button on the machine, which produces a token, or a paper print out of the vote. This printed ballot is then placed in a ballot box either automatically by the voting machine or manually by the voter. At the end of polling, all of the tokens/ballots are manually counted.

Deployment and Price Estimate: These machines have been used in Belgium and Bangladesh. Bangladesh is spending $2,400 per machine.

Pros	Cons
Voters mark their vote directly into an electronic device	Manual Counting
Paper trail allows audits to be undertaken	Ballot stuffing and ballot destruction

F) Online or Internet Mode of Voting



Estonia's internet voting system in Tallinn, Feb 28, 2011

Internet voting is undertaken in an unsupervised environment. Voters submit their vote electronically via the internet, from any location in the world.

Deployment and Price: Around 7 countries in the world deploy Internet Voting in some capacity. [Discussed in detail in Section 6]. However, Estonia with a population of 1.3 million people is the only country to have nationwide deployment.

Pros	Cons
Voters mark their vote directly via the internet through any gadget	Highly susceptible to all types of Cyber attacks
Easily accessible	Not suitable in countries where internet penetration is low
No invalid votes	Voters disfranchised who are not tech savvy
No paper trail	Coercion and impersonation cannot be prevented
May increase voter turnout	Secrecy of Ballot cannot be ensured or guaranteed.
Quick result compilation	If email ID or passcode is compromised or hacked then the voting right will be transferred from legitimate voter to the unauthorized person or hacker to vote.

1.2 COMPARATIVE INTERNATIONAL PRACTICES

BRAZILIAN EVM

Brazilian EVMS were used for the first time in 1996. Key government entities like the National Institute of Spatial Research (INPE), the Brazilian Army, the Brazilian Air Force (Department of Aerospace Science and Technology – DCTA), the Brazilian Navy, and the Center of Telecommunications Research and Development (CPD) contributed to the design. The Superior Electoral Court (*TSE*) specifies the equipment specifications and issues a bid tender for companies to compete to manufacture the voting machines. A TSE team built and implemented the software that runs on the EVMs for recording and counting votes. Today, there are 550,000 EVMs available for the country's 460,000 polling stations. The current model costs US $670 and has a minimum service life of 10 years.

Features of the Machine:

The Brazilian EVM includes a voter authentication and identification unit using a biometric scanner to scan voter fingerprints, the biometric reader scans their fingerprints. The ballot casting unit is used to record the actual votes. The machine uses separate memory cards to store recorded votes, total votes, and backup data respectively. The total votes are printed on machine bulletins using thermal printers, like receipt printers used in ATMs. However, it must be noted that these machines only print the totals, once the voting time ends and not the paper trail of individual votes cast by the voters. The machines are also supported by batteries that ensure machine functionality is not disrupted in the event of a power outage. The system also has an audio output for voters who are blind or visually impaired.

Lessons learned from the Brazilian Experience:

1. According to the SEC, there are several layers of security that prevent invasion by third parties and access to information contained in the device. If an attack is attempted, it causes a reaction in the system that hangs the program and prevents it from being executed by an outsider.

2. On voting day, the balloting system is not connected to the internet or the SEC system. Consequently, there is no way to access or to invade it remotely. The equipment works only at the time and date of the elections, normally from 8am to 5pm.

3. Since 2009, the SEC has organized mandatory Public Security Tests (PSTs). The PSTs are attended by specialists, and in the presence of staff from electoral court of justice, members and representatives of political parties, journalists of Electoral Justice, members of international organizations, Brazilian Federal Police and Brazilian Army. This is an important trust-building measure that can be emulated in Pakistan.

4. Another inspection procedure carried out by the Electoral Court is to select certain EVMs on the eve of the election and proceed with a simulation of the votes at the headquarters of the regional electoral courts. According to the SEC, this happens with the participation of representatives of the candidates, with cameras filming the process, there is a verification process to ascertain the votes corresponding to those registered in the machine.

5. The possession of national capacity to produce EVMs not only reduces cost of EVMs but allows for flexibility in modifying the functionality of the machines. Brazil has constantly and easily migrated to higher models with 7 models deployed between 1996 and 2014.

6. The Brazilian Supreme Electoral Court regularly funds research aimed at improving security of elections. To illustrate this, a hacking competition was organized in 2009 to demonstrate the high security of the systems and create additional confidence in the technology. In 2011, new biometric-based voting machines were developed. The Electoral Court started implementing biometric identification in the electoral process in 2012.

7. There is a legal provision for participation of the Brazilian Bar Association, the Public Ministry and political parties in the various stages of specification and development of all computer programs used in the EVM. In addition, all technology is internally developed by the SEC.

8. **Six months before each election, the system is opened for verification to several institutions, such as political parties, the Public Prosecutor's Office, the Federal Police, universities, and professional associations. The objective is to verify the programs that will be adopted and to make it open to criticism.**

https://www12.senado.leg.br/radio/1/noticia/2020/11/16/tse-avalia-voto-online-ou-por-celular-para-eleicoes-de-2022

INDIAN EVM

The Electronics Corporation of India Ltd. (ECIL) in Hyderabad was tasked with designing and developing EVM after it was first envisioned in 1977 by the Election Commission of India, to use electronic voting machines. A prototype was created in 1979 and in Kerala's general election in May 1982, EVMs were used for the first time. The EVMs were used across the country in the General Election for the Lok Sabha in 2004.

India is currently on its third generation of EVMs, namely the M3 electronic voting machine with VVPAT capability, M1 and M2 being the older models. Trials for the VVPAT system were done in 2011 and 2012, and machines with VVPAT have been integrated into machines since 2014. The Election Commission of India uses EVM Tracking Software to safely track the inventory of election EVMs in real-time (ETS). When the machines were purchased in 1989–90, the cost per EVM was INR 50,000 (equivalent to US$660 in 2020). According to an additional order placed in 2014, the cost per unit was expected to be INR 10,500 (equivalent to US$190 in 2020).

Features of the Machine

The M3 EVM is made up of the Control Unit (CU) and the Balloting Unit (BU), which are connected by a cable (5 meters long). Up to 16 candidates can be accommodated in a Balloting Unit. If there are more than 16 candidates, ballot units can be cascaded to accommodate them. These EVMs are also supported with batteries, to ensure functioning in the case of a power outage. The Control Unit (CU) keeps track of the votes cast through the Balloting Unit. The attached printer is used to produce a Voter Verified Paper Audit Trail (VVPAT), that allows voters to confirm that their votes were cast correctly. When a vote is cast, a slip with the candidate's serial number, name, and symbol is produced on the VVPAT printer and exposed for 7 seconds through a transparent window. Following that the printed slip is automatically cut and dropped into the VVPAT's sealed dropbox. As an additional layer of security, the M3 EVMs incorporate hardware and software features that allow the pairing of a specific control unit to function only with a specific voting unit.

Lesson learned from India Experience

1. The India EVM model of 5 and 150 persons balloting per minute and per 30 minutes respectively, offer the benefits of considerably reducing the number of voters per polling unit.

2. The EVM VVPAT with documented ballots for voters enhances the transparency and credibility of the electoral process. Five copies of the results tally sheet are printed and signed by the presiding officer of each polling station and by representatives of the political parties. The five copies are assigned to specific destinations: the first is posted on the polling station to publicize the result; three are added to the polling station report and forwarded to the respective electoral registry; and the last copy is delivered to the party representatives.

3. National production of the EVM machines offers the possibility of considerable reduction in the unit prices (From $116 to $229).

4. At close of polling, the EVM is moved to the Counting Hall or Counting Centers in presence of the candidates. Thereafter, the seals, with unique IDs containing the signature of polling agents on CU, are presented to representatives of candidates before the start of counting. The date and time of counting is fixed by the ECI. Ideally, counting of votes for a constituency should be done at one place, preferably at the Headquarters of the Regional Office in that constituency. In India, the lifespan of an EVM is 15 years and votes recorded in the Control Unit (CU) can be stored up to this lifetime until, unless erased. Where a Court order for a recount is issued, the Control Unit can be reactivated by fixing the battery and the result stored in the memory is accessed.

https://www.jagranjosh.com/general-knowledge/cost-and-place-of-manufacturing-of-evm-in-india-1555398297-1
Election Commission looks to develop mobile voting technology to track down 'Lost Votes' - https://government.economictimes.indiatimes.com/news/digital-india/election-commission-looks-to-develop-mobile-voting-technology-to-track-down-lost-votes/74171792
https://www.eces.eu/en/posts/evoting-nigeria

VOTING MACHINES IN THE PHILIPPINES

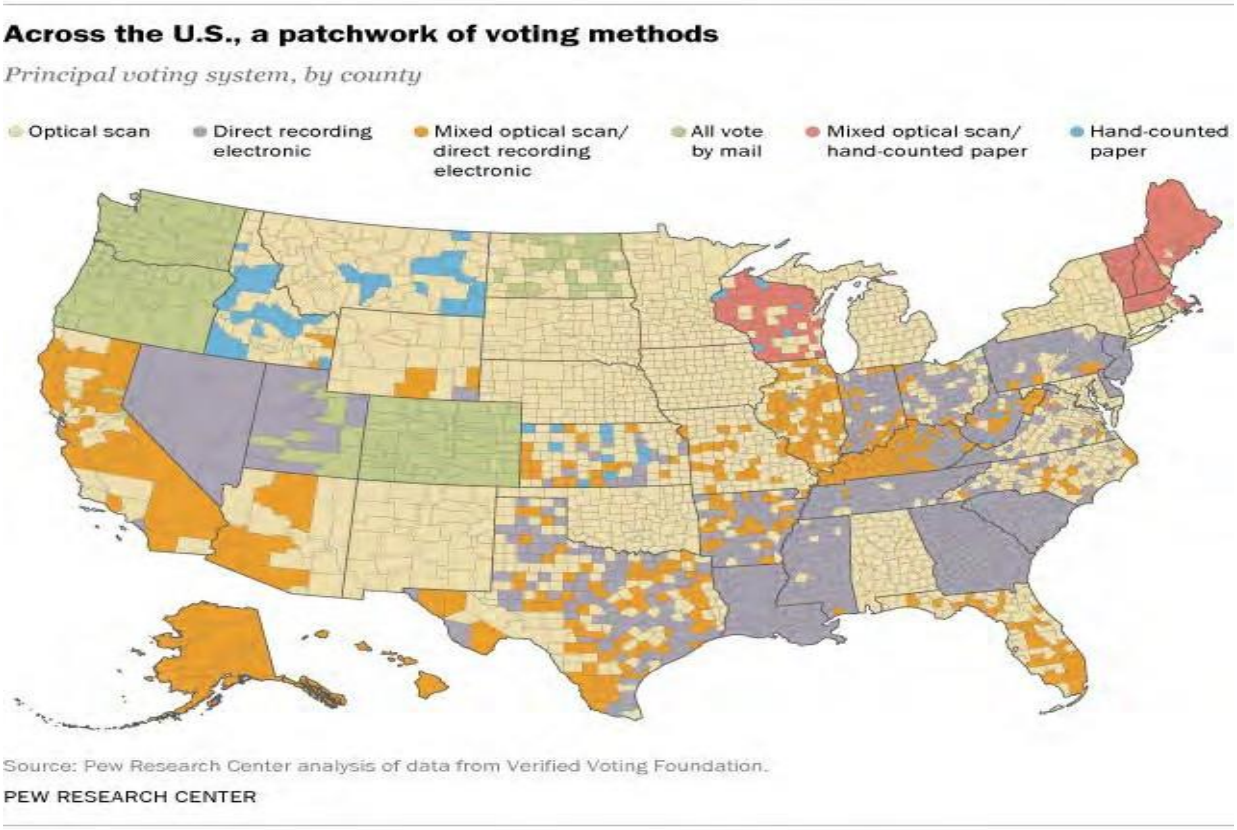
Smartmatic was chosen by the Commission on Election (COMELEC) to automate the election process in 2007. Smartmatic's voting machines were used in general elections in 2010.

For the 2016 General election, in a 7.9-billion-peso contract, the Commission on Elections leased 94,000 new optical mark recognition (OMR) equipment from Smartmatic, with the old ones

being reconditioned. This was the largest deployment of such machines anywhere in the world.

Each ballot is automatically counted as is fed into the machines. The results are then printed and forwarded electronically to the city or municipal Board of Canvassers as an election return.

UNITED STATES OF AMERICA (USA)



The USA has been using electronic voting machines, in some form, since the 1960s. Voting machines used can broadly be categorized into two groups: Precinct Count Optical Scan voting machines (PCOS) and Direct-Recording Electronic (DRE) voting machines. Optical scan voting devices are similar to standardized test scoring machines in that you fill in a bubble next to the candidate names on the ballot. Those are the most extensively utilized voting technologies in the United States at the moment. Direct-recording electronic voting machines are the alternative option, and have been used since the early 1990s. Some DRE machines produce paper trails, thus called DRE-VVPAT (Direct Recording Electronic- Voter Verified Paper Trail).

The Election Assistance Commission (EAC) issues voting guidelines. In some counties in Florida, Illinois, Indiana, Iowa, Michigan, Minnesota, Rhode Island, Tennessee and Wisconsin, election machines are online to communicate results between precinct scanners and central

tabulators as of 2018–19. "Remote Access Vote by Mail (RAVBM)" is another option. Voters with a computer and printer in several states can download a ballot, fill it out on the computer, print it, and mail it back. Individual voters can submit completed votes electronically in Hawaii, Idaho, Louisiana, and Utah.

The majority of voting and counting machines are sold by three companies. As of September 2016, American Election Systems & Software (ES&S) had serviced 80 million registered voters, Canadian Dominion Voting Systems had served 70 million, American Hart InterCivic had served 20 million, and smaller companies had served less than 4 million.

CANADA

Hand-counted paper ballots are used in federal elections. Paper ballots are also used in provincial elections; however, some provinces have implemented computer ballot counting (vote tabulators), and the Northwest Territories have tried out Internet voting for absentee voting. At the municipal level, paper ballots with computer vote tabulators have been used since the 1990s. Elections Canada made a statement in 2017 stating that "Elections Canada has no plans to introduce electronic casting or counting of votes. Polling places will continue using paper ballots, marked and counted by hand."

Similarly, with regards to internet voting, in 2020, Election Canada issued a statement saying *"At this point, Elections Canada is not considering introducing internet voting. Implementing such a change would require significant planning and testing to ensure that the agency preserves certain aspects of the vote, including confidentiality, secrecy, reliability, and integrity. Given the current operational and time constraints, this option cannot be explored properly at this time."*

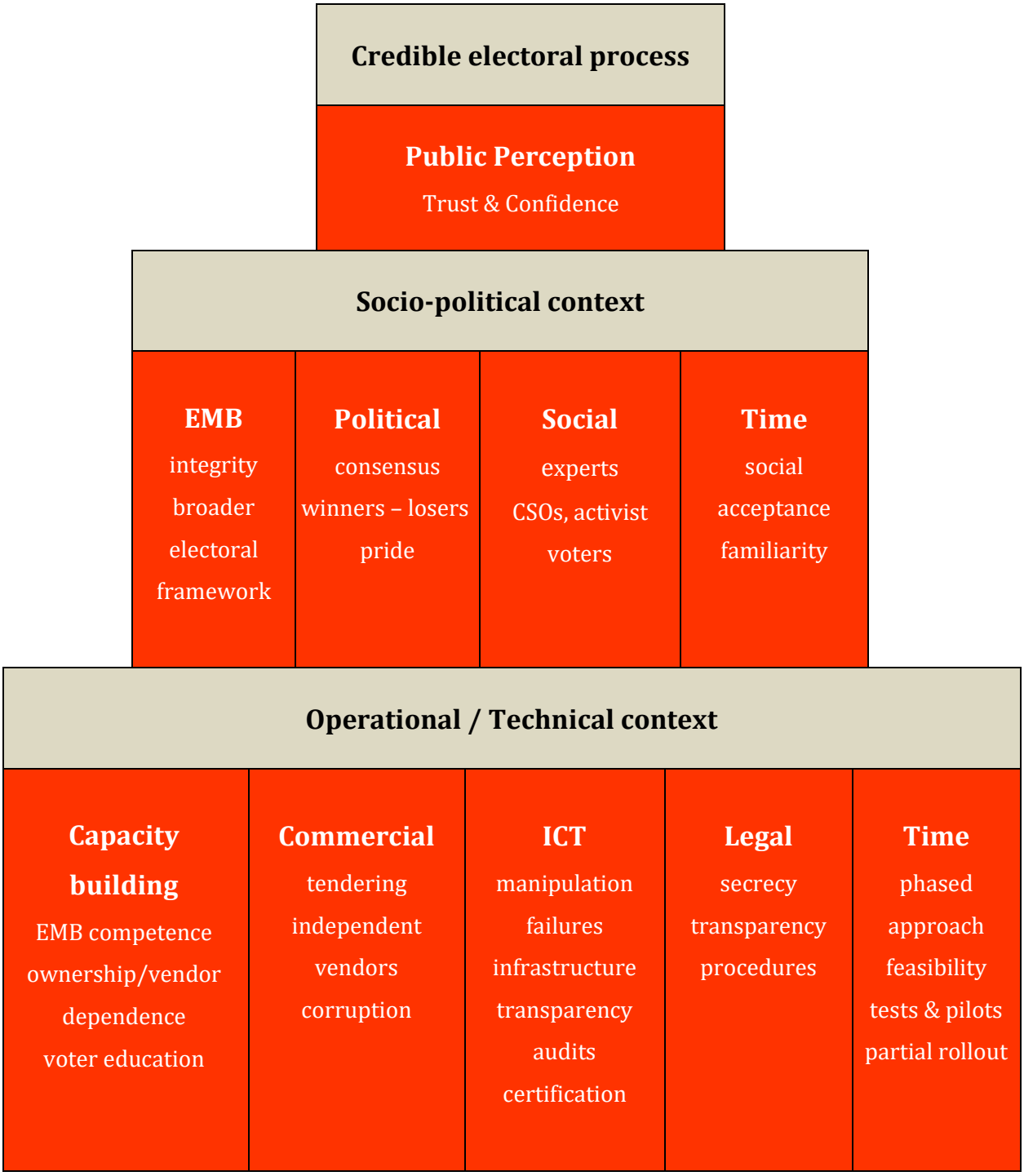
THE STRENGTHS AND WEAKNESSES OF EVMs MATRIX

Electoral issues, compared to paper voting	Internet voting	DRE without VVPAT	DRE with VVPAT	PCOS	Electronic ballot printers
Faster count and tabulation	Strength	Strength	Strength	Strength	Strength
More accurate results	Strength	Strength	Strength	Strength	Strength
Management of complicated electoral systems	Strength	Strength	Strength	Strength	Strength
Improved presentation of complicated ballot papers	Mixed	Mixed	Mixed	Weakness	Mixed
Increased convenience for voters	Strength	Mixed	Mixed	Weakness	Mixed
Increased participation and turnout	Strength	Neutral	Neutral	Neutral	Neutral
Addressing needs of a mobile society	Strength	Mixed	Mixed	Neutral	Mixed
Cost savings	Mixed	Weakness	Weakness	Weakness	Weakness
Prevention of fraud in polling station	Neutral	Strength	Strength	Strength	Strength
Greater accessibility	Mixed	Mixed	Mixed	Weakness	Mixed
Multi-language support	Strength	Strength	Strength	Weakness	Strength
Avoidance of spoilt ballot papers	Strength	Strength	Strength	Strength	Strength
Flexibility for changes, handling of deadlines	Strength	Strength	Strength	Weakness	Strength
Prevention of family voting	Strength	Neutral	Neutral	Neutral	Neutral
Lack of transparency	Weakness	Weakness	Mixed	Mixed	Mixed
Only experts can fully understand the voting technology	Weakness	Weakness	Mixed	Mixed	Mixed
Secrecy of the vote	Weakness	Mixed	Mixed	Mixed	Mixed
Risk of manipulation by outsiders	Weakness	Mixed	Mixed	Mixed	Mixed
Risk of manipulation by insiders	Weakness	Weakness	Weakness	Weakness	Weakness
Costs of introduction and maintenance	Strength	Weakness	Weakness	Weakness	Weakness
Infrastructure/environmental requirements	Mixed	Weakness	Weakness	Weakness	Weakness
Lack of e-voting standards	Weakness	Weakness	Weakness	Weakness	Weakness
Meaningful recount	Weakness	Weakness	Strength	Strength	Strength
Vendor-dependence	Weakness	Weakness	Weakness	Weakness	Weakness
Increased IT security requirements	Weakness	Weakness	Weakness	Weakness	Weakness

---

Introducing Electronic Voting: Essential Considerations (https://www.idea.int/sites/default/files/publications/introducing-electronic-voting.pdf)

THE PYRAMID OF TRUST



Introducing Electronic Voting: Essential Considerations (https://www.idea.int/sites/default/files/publications/introducing-electronic-voting.pdf)

HOW MANY COUNTRIES BANNED THE EVM?

There is worldwide acceptance of the need for a paper trail in conjunction with EVMs. Electronic voting was introduced in many countries, but serious doubts were soon raised about the security, accuracy, reliability and verifiability of electronic elections. In October 2006, the Netherlands banned the use of EVMs. In 2009, the Republic of Ireland declared a moratorium on their use. Italy has followed suit. **In March 2009, the Supreme Court of Germany ruled that voting through EVMs was unconstitutional, holding that transparency is a constitutional right but efficiency is not a constitutionally protected value.**

USA, the UK, Netherlands, France, Ireland and Germany have done away with Electronic Voting Machines (EVMs) due to their potential to compromise the election process.

Here is the list of those countries and reasons for their discontinuation –

(i) GERMANY - Constitutional Court banned the usage of EVM in elections. (Population - 82m)

The EVMs have been prone to hacking and have been declared as unfit for political use. In Germany, EVMs have been termed as unconstitutional and have been banned due to lack of transparency and public trust. Two voters brought a case before the German Constitutional Court after unsuccessfully raising a complaint with the Committee for the Scrutiny of Elections. Following this complaint, the German Constitutional Court banned the use of voting machines that voting machines were not transparent enough, the government stopped using them in 2009.

(ii) **THE NETHERLANDS - Dutch Council banned EVM in elections due to dependency on external actors, outdated testing and certification standards and tests/certification reports were not made to public and incomplete legal framework. (Population - 17.03m)**

The Netherlands is another country that has questioned the use of EVMS and banned the use of EVMs. This decision was taken by the Dutch council in 2008 after people questioned the authenticity of the voting machines. Dutch TV carried a story where with one change the EPROM (Erasable Programmable Read-Only Memory) of the Nedap (a Dutch Multinational Technology Company) voting machine changed the output, making people question its credibility.

After anti-e-voting campaigners demonstrated that it is not safe through attempting experimental hacking, the country resorted to paper ballots in 2007.

(iii) **IRELAND - Banned due to lack of security and transparency issues. (Population - 4.7m)**

Because of security concerns, the country cancelled plans to deploy the devices in 2006. Ireland spent millions of dollars on the installation of EVMs and to use them during the political elections. However, after spending more than 51 million pounds for three years,

Ireland went forward and scrapped the electronic voting system, citing it to lack of trust and transparency in the voting machine.

(iv) **PARAGUAY:** The government had experimented with voting devices that it had borrowed from Brazil in the early 2000s. It went back to paper ballots in 2008.

(v) **ENGLAND - No Ban,** however they chose conventional methods of elections over modern. (Population - 53m)

England has had various pilots for the electronic voting system to be used. However, these pilots have never led to the use of EVMs in the country. England is one of the few countries that has stayed away from the modern methods in political elections, and the government plans to continue on the same path. In January 2016, the UK Parliament revealed that it has no plans to introduce electronic voting for statutory elections, either using electronic voting in polling booths or remotely via the internet

(vi) **FRANCE - No Ban,** they chose internet voting method over EVMs for diplomats only - (Population - 66.9m)

Electronic voting was used in a national presidential primary in 2007. While the country has chosen to vote via the internet, EVMs have not been used in France. Elections in France utilized remote Internet voting for the first time in 2003, and this idea was made a custom in 2009 as people chose the internet voting system over paper.

On March 6, 2017 France announced that Internet voting (which had previously been offered to citizens abroad) would not be permitted in the 2017 legislative elections due to cybersecurity concerns.

As of 2020, citizens abroad voted by internet in legislative and consular elections, not for President or EU.

(vii) **ITALY - They had run a pilot project however upon completion they went back to ballot paper. (Population - 60.6m)**

In 2006, Italy used Nedap Voting machines in the national elections. The pilot project involved 3000 electors and four polling stations. However, after the pilot project was completed, the country chose to go back to paper as it is easy to manage and cheaper.

While these countries have banned or refrained from using EVMs, there are others who have taken a systematic approach and backed the use of EVMs with paper ballots. In various parts of the United States of America as well as in Venezuela EVMs are used on a large scale but are backed by paper trails of the votes. This simple step helps the government to regularize and check the authenticity of votes and avoid any discrepancies.

(viii) **USA - EVMs without paper trail were banned.**

(ix) **Venezuela - Same like USA**

HISTORY OF EVMs IN PAKISTAN

On 14th November, 2009, the then Hon'ble Chief Election Commissioner, Justice (R) Hamid Ali Mirza, established a Committee on the Use of Electronic Voting Machines in Pakistan (EVM Committee) under the chairmanship of Joint Secretary (Elections). The Hon'ble Chief Election Commissioner tasked the EVM Committee with conducting a detailed feasibility study into the potential use of EVMs in Pakistan with options and recommendations, considering all technical, operational, financial, and legal aspects.

The EVM Committee had drafted the EVM Feasibility Study Plan. The EVM Committee concluded that the overall objectives of the study were: (i) to conduct a feasibility study on the use of new technologies for voting and the counting of votes, (ii) to determine whether these technologies were suitable for introduction in Pakistan. The suitability of the technologies were needed to be assessed in terms of the advantages they might offer over the current system of paper balloting and counting, the technical and operational challenges associated with their use, a financial assessment of the comparative costs of paper versus electronic voting/counting, and the legal implications of using electronic voting/counting. The steps in the conduct of this feasibility study were:

1) Assessment of Strengths and Weaknesses of the Current Paper Balloting System
2) Assessment of the Benefits of New Technologies
3) Cost Analysis of Paper Balloting versus New Technologies
4) Assessment of Legal Implications of Using New Technologies
5) Vendor Demonstration of Technologies
6) Consultations with Stakeholders
7) Conclusion of Report and Recommendations

To address the first four steps, four working groups were constituted and were tasked to provide recommendations to the Election Commission.

In 2016-17, ECP conducted its first pilot project in a Bye-Election of NA-4 Peshawar-IV. To accomplish this, ECP had purchased customized 150 EVMs (DRE technology) from M/s Smartmatic through a tendering process and deployed these machines at 100 Polling Booths in parallel to the Paper based balloting system. Almost 12,419 voters of designated 35 polling stations used EVM devices at the end of the polling cycle as per approved SOPs. 78% of voters who casted their paper ballot, voluntarily participated in the mock pilot testing using the EVMs. **It was observed that voters enthusiastically participated in the pilot testing of Electronic Voting Machines.**

Figure 1. Comparison of voter turnout in constituency and turnout of voters to participate in the mock pilot

The key purpose of the pilot project was to test the EVM capabilities and the introduction of such technology in the electoral process to gauge participation of the voters by using the technology. The pilot for the EVM was held at 35 polling stations with 100 EVMs at designated polling booths earmarked by the Election Commission of Pakistan (ECP). These 100 EVM's were manned by 50 ECP personnel and 50 M/s Smartmatic personnel and tested on 26th October 2017. The ECP field operation staff was able to operate the EVM easily after the training. Following issues and observations were noted.

Issues Identified in EVM Pilot Project NA-4 Peshawar IV		
S #	**Nature of Errors being faced**	**Number of Issues Faced**
1.	Battery drainage issue (Control Unit + Ballot Unit)	29
2.	Paper stuck during printing of Ballot paper	28
3.	Voting Pad Sensor	20
4.	Software hanging issues	7
5.	Diagnostic Issues	6
6.	Damaged VGA Cable	2
7.	Error during consolidating votes by USB	1

ECP conducted a second Pilot project in a Bye-Election of PP-20 Chakwal-I on 9th January, 2018. The primary goal of the second Electronic Voting Machine (EVM) pilot was to implement all lessons learned during the first rollout in NA 4 Peshawar-IV Bye-Election. 2,870 males and 2,446 females cast their vote via the EVM. Results of all stations were consolidated via USB sticks by 6.30 pm at the RO office and published on the dedicated website.

The first pilot project Report of EVM was submitted to the Parliament on 08-01-2018 after which there was no response on the Report till date.

After submission of the first pilot project report of EVM and Internet Voting in Assemblies through Ministry of Parliamentary Affairs after the enactment of Section 94 and Section 103 of the Elections Act, 2017, the representatives of ECP had participated in meetings chaired

by the Hon'ble President of Islamic Republic of Pakistan to deliberate on the use of technology in electoral process in Pakistan. The Hon'ble President of Islamic Republic of Pakistan had constituted a Special Committee on "Emerging Technologies" in June, 2020 to cater for the technical aspects of the electoral technologies, including Internet Voting, EVM and BVM. The Special Committee comprised officials from various relevant Government departments including ECP.

The ECP had constituted a Technical Evaluation Committee (TEC) on 23rd November, 2021 to evaluate the machine designed and developed by the Ministry of Science and Technology and representatives of ECP attended several meetings in this regard. Further, ECP wrote a letter to the Ministry of Science and Technology for the provision of 3,900 EVMs along with support and services for the conduct of ICT Local Government Elections. The TEC held couple of meetings with officials of Ministry of Science & Technology after their live demonstration of prototype machine developed by a vendor M/s RapiDev (private firm) dated on 17th August, 2021. ECP Secretariat and MoST are still to settle on some operational plans. It appears till the submission of this report that the Ministry of Science and Technology is considering the funding and sustainability factors developing the machines.

BENEFITS OF ELECTRONIC VOTING MACHINES

EVMs can lead to considerable benefits which have been well documented in the international experience. These include the following:

Automation and Efficiency: EVMs automate the tabulation process which dramatically reduces the time and manual effort required to count votes. Using EVMs, the entire election process can be managed much more efficiently with less staff required, and EMBs can disseminate election results near-instantaneously after polls close. Automation and efficiency are primary motivation for the uptake of EVMs in some Western countries.

These factors are especially important today for developing countries, like India, Brazil, and Pakistan, which have very large populations, and vote counting can be a massive human endeavor. An illustrative example is Indonesia where the polls of April 2019 included over 190 million voters in a landmass of over 2 million square kilometers, with over 8 hundred thousand polling stations[5]. This was the world's largest single-day voting exercise to date and employed over 7 million poll workers and security staff. Vote counting was done entirely by hand, often running non-stop over a 24-hour period to meet official deadlines. More than five hundred and fifty polling staff died from exhaustion in the process and thousands more were hospitalized due to fatigue. In response to this tragedy, the Indonesian government has begun to re-consider using EVMs in polls.

Improved Security: Elections in large developing countries typically employ hundreds of thousands of staff, who can easily manipulate the results, giving rise to a culture of systemic rigging and distrust in elections and democracy. A key opportunity for vote rigging is during the vote counting process, which can extend over a few days and can be a period of great suspense and uncertainty nationwide.

Researchers have noted that EVM deployments have successfully countered polling-station fraud in countries like Brazil and India[6]. By automating the tabulation process and reducing involvement of polling workers, voting results can be recorded within minutes after polls close, thereby closing a critical window for rigging. For instance, in the recent 2019 elections in the Philippines, two thirds of the poll results were disseminated within two hours of polls closing[7].

Improved Accuracy: Most EVM types prevent spoilt votes, giving more accurate results, and thereby ensuring that 'every vote is counted'. Paper elections typically involve significant numbers of spoilt votes which raise questions about transparency and doubts

[5]The Jakarta Post: Voting-made-easy has a cost: Over 400 deaths (May 2021), https://www.thejakartapost.com/academia/2019/05/07/ voting-made-easy-has-a-cost-over-400-deaths.html

[6] Debnath, S., Kapoor, M., Ravi, S.: The impact of electronic voting machines on electoral frauds, democracy, and development. Democracy, and Development, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041197 (March 16, 2017)

[7] Philippine Votes Transmitted in Record Time in Largest Ever Electronic Vote Count (May 2016), https://www.smartmatic.com/media/article/ philippine-votes-transmitted-in-record-time-in-largest-ever-electronic-vote-count/

about election results. A study notes that headcounts of votes can have as much as 2% of error in the final tally. In the last two general elections in Pakistan, the number of discarded votes exceeded the margin of victory in over 30 constituencies, a significant number and cause for concern[8]. In the general elections of 2018, ECP undertook recounts in 70 constituencies, adding further to election costs, uncertainty and political delays[9].

Inclusivity: EVMs can be customized to be easy to use and can be equipped with accessibility options like audio aids and Braille support for differently-abled voters. Researchers have documented that EVMs have empowered women, scheduled castes and other marginalized groups in India[10]. In Canada, a Government Committee of MPs has made aids for differently-abled groups mandatory to continue use of EVMs.

Voter Confidence and Turnout: Studies have noted that EVMs tend to inspire greater trust and confidence in citizens. In some countries, voters have reported significantly greater user satisfaction when votes were cast using EVMs as compared to other voting methodologies [11,12,13]. Moreover, introduction of EVMs in some regions, such as the Philippines, correlates with greater voter turnout, although issues remains.

Cost Savings: By minimizing human involvement and automating vote casting and counting processes, EVMs can significantly reduce the operational costs of elections. Studies have documented significant cost savings when switching to EVMs. For instance, deployment of EVMs in Netherlands resulted in reduction in the number of polling stations, reduction in the number of staff required to man polling stations, and other improvements in electoral administration[14]. Another obvious saving is in the cost reductions in printing, distributing, and storing ballot papers.

Other Positive Trends: Interestingly, the introduction of EVMs in some regions correlates with improved governance and other positive trends. This pattern is highlighted in research which indicates competitive electoral races and improved electrification in parts of India[15] after introduction of EVMs, and better indicators of infant healthcare in Brazil[16].

---

[8]General Election Observation 2018: Key Findings and Analysis. http://fafen. org/fafen-general-election-observation-2018-result-assessment-and-analysis/ (2018)

[9] General Election Observation 2018: Key Findings and Analysis. http://fafen. org/fafen-general-election-observation-2018-result-assessment-and-analysis/ (2018)

[10] Debnath, S., Kapoor, M., Ravi, S.: The impact of electronic voting machines on electoral frauds, democracy, and development. Democracy, and Development (March 16, 2017)

[11] Everett, Sarah; Wallach, Dan S.; Greene, Kristen K.; Byrne, Michael: Electronic Voting Machines versus Traditional Methods: Improved Preference, Similar Performance (April 5-10, 2008)

[12]Herrnson, Paul S; Niemi, Richard G; Hanmer, Michael J; Francia, Peter L; Bederson, Benjamin B; Conrad, Frederick G.; Traugott, MichaelW : Voters' Evaluations of Electronic Voting Systems Results From a Usability Field Study (July 2008)

[13] Menno de Jong, Joris van Hoof, Jordy Gosselt: Voters' Perceptions of Voting Technology: Paper Ballots Versus Voting Machine with and Without Paper Audit Trail (Dec 18, 2007)

[14]Niemoller, Kees: Experience with Voting Machines in the Netherlands and Germany, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.138.3635&rep=rep1&type=pdf

[15] Debnath, S., Kapoor, M., Ravi, S.: The impact of electronic voting machines on electoral frauds, democracy, and development. Democracy, and Development (March 16, 2017) (2017)

[16] Fujiwara, T.: Voting technology, political responsiveness, and infant health: Evidence from Brazil. Econometrica 83(2), 423–464 (2015)

RISKS AND CHALLENGES

Despite demonstrated benefits, EVMs have several disadvantages, which have resulted in several technologically advanced countries, including Germany, Ireland, and the Netherlands discontinuing their EVM deployments.

Lack of Transparency: Arguably, the most problematic aspect of popular EVM types is that they are technically black boxes which do not give stakeholders transparency into their inner workings. This is unfortunately due to the inherent tension which exists between voter privacy and electoral integrity[17]: individual ballots have to be anonymized to safeguard voter privacy and this leaves them vulnerable to rigging and manipulation within the EVM.

This lack of transparency is also the key reason that as stated earlier, a German court ruled out the use of EVMs, terming them "unconstitutional" because voters could not confirm how the machines processed their votes without specialist knowledge of the subject[18]. A recent report by the Citizens' Commission on Elections, an Indian civil society organization, comprising contributions by international authorities in elections security, concluded that the Indian EVMs, due to lack of transparency in their present form, are "*near-fatal for electoral democracy*"[19].

Poor Security: Whereas EVMs have been documented to resolve pressing security issues in countries such as Brazil and India, it is now well acknowledged that they may create new opportunities for rigging and vote manipulation. A multitude of studies and reports over the last two decades have demonstrated that EVMs are notoriously prone to hacking. Almost every EVM that has been analyzed has been successfully compromised by researchers to leak sensitive vote information and alter vote counts, including various machines certified and used in the US, Brazil, Netherlands, and India. It is also possible to insert backdoors into EVM software and to manipulate votes on a large scale without detection[20].

To get a sense of the immense scope of this failure, we can turn to proceedings of the Voting Village, an annual hacking event organized by leading specialists which specifically focuses on security vulnerabilities of election technology. In the 2020 edition of this event, organizers gathered together over 100 voting machines, each of which was certified for use in at least one US voting jurisdiction, many of which were shortly deployed in the 2020 US presidential elections. **Over two and a half days, attendees successfully hacked each of**

[17] Orcutt, Mike: Internet Voting Leaves Out a Cornerstone of Democracy: The Secret Ballot, https://www.technologyreview.com/2016/08/18/107858/internet-voting-leaves-out-a-cornerstone-of-democracy-the-secret-ballot/ (August 18, 2016)

[18] Commonwealth Secretariat: Cybersecurity for Elections: A Commonwealth Guide on Best Practice, 1st May, 2020

[19] The Wire.in: ECI's Conduct of 2019 Elections Raises 'Grave Doubts' About Its Fairness: Citizens' Report, https://thewire.in/rights/election-commission-bjp-polls-fairness-citizens-commission-on-elections-report, March 15, 2021

[20] How to Hack and election in 7 minutes, https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144/

these machines, using "trivial attacks" that required "no sophistication or special knowledge on the part of the attacker".[21]

Prone to Malfunction: EVMs occasionally suffer serious technical difficulties due to extreme weather conditions and unexplained circumstances, which can frustrate voters and delay results. In the 2018 midterm elections in the US, ballot tabulators could not read ballots due to humidity in North Carolina and Alabama[22]. In New York City, election officials stated that rain had wet the ballots and caused scanning machines to jam. In India, 3-10% of voting machines are known to fail mock polls held prior to field deployment[23]. In polls in 2018, the Election Commission of India had to provision 15 percent extra EVMs during polls to compensate for faults because of extreme heat, light and dust[24].

Challenge of Usability: EVMs may be challenging to use in developing countries like Pakistan. Usability is also a complex topic and there are several facets to consider: for instance, usability generally correlates with computer literacy and technical skills within citizenry, the scope and effectiveness of voter education and outreach efforts and is typically assisted by gradual deployment strategies[25]. **The physical design and the voting protocol of EVMs must be adapted to cater to voters. A wide range of factors must be carefully considered, including legibility of text on the machines, the time it takes to cast a vote, how the machine deals with unintentional undervotes, etc. Adapting EVMs to the unique ground realities of a developing country like ours will likely require considerable research and pilot testing.**

Lack of Standards and Certifications: There are no clear and authoritative standards or certifications for EVMs as there are for various other technologies. The reason for this is that EVMs are a complex phenomenon which must be adapted to the unique ground realities of every society. A whole host of socio-political, cultural, logistical, and financial considerations come into play. **Attempts to transplant election technology on a large scale without rigorous homework are quite likely to fail and incur heavy political and financial costs, as observed in Ireland[26] and Kenya**[27].

---

[21]Vaas, Lisa: Hacking 2020 voting systems is a 'piece of cake', https://nakedsecurity.sophos.com/2019/10/01/hacking-2020-voting-systems-is-a-piece-of-cake/ (Oct 01, 2019)

[22] NBC News: Midterms 2018: Voters face malfunctioning machines and long lines at polls across country on Election Day (2018), https://www.nbcnews.com/politics/elections/midterms-2018-voters-face-malfunctioning-machines-long-lines-polls-across-n932156

[23] Agarwal, Poonam: Can We Trust EVMs? MP Election Vote Count Shows Huge Discrepancies, https://www.thequint.com/news/india/evm-hacking-tampering-malfunction-mp-election-2018-discrepancies-vote-count (Feb 02, 2019)

[24] India Times: Lo and Behold Heat Wave Saps EVMS, https://mumbaimirror.indiatimes.com/news/india/loo-and-behold-heat-wave-saps-evms-oppn-fumes/articleshow/64362680.cms

[25] OSCE Office for Democratic Institutions and Human Rights (ODIHR): Handbook for the Observation of New Voting Technologies

[26] Michela Wrong, New York Times: School Socket Syndrome,

[27] Paul Melia and Luke Byrne, The Independent: €54m voting machines scrapped for €9 each, https://www.independent.ie/irish-news/54m-voting-machines-scrapped-for-9-each-26870212.html (June 29, 2012

Cyberwarfare: In recent years, it has become clear that elections bodies and infrastructure are key targets for cyberwarfare. **In the US, the Department of Homeland Security, in response to Russian and Chinese cyberattacks on US election systems, has now designated election infrastructure as 'critical infrastructure', in the same class as dams and nuclear reactors**[28]. Foreign attacks on these systems may now result in retaliatory sanctions or even be considered acts of aggression or war. In recent US elections, several states called in the National Guard to assist with cybersecurity threats[29]. This represents a significant challenge for developing countries like Pakistan which is a frequent target for hacking attacks and there is a marked shortage of cybersecurity practices, expertise, and even awareness. **Ideally, election management bodies should implement best cybersecurity practices, hold frequent security drills and training sessions, and foster close working relationships with national cybersecurity agencies. Bringing our own systems and processes to the required level represents a significant challenge and could take years.**

Supporting Ecosystem: An often-overlooked factor is the immense ecosystem that is required to support successful EVM deployments. This ecosystem includes logistics concerns, such as training, manpower, and management of machines; infrastructure requirements, such as custom storage depots, maintenance facilities, and transport networks; various procedural arrangements including complex and detailed security and handling protocols and transparency mechanisms; legal concerns, which include supporting legislative frameworks, dispute resolution mechanisms, etc.; and political factors which include authority, capability, and independence of the governing election management body.

These ecosystem components can require significant intellectual effort and costs which may even exceed the actual cost of the EVMs themselves. [footnote: Commonwealth report] This is a key reason that successful EVM deployments in countries such as Brazil, India, and Australia, are backed by significant research and stakeholder consensus, and evolved and scaled organically in iterative cycles instead of moving directly to large-scale deployment.

High Costs and Sustainability Concerns: Many developing countries lack the resources for expensive EVM deployment and often rely heavily on international donors for funds and engage foreign consultants for technical expertise. This practice can be costly, its sustainability is questionable in the long run, thereby preventing countries from developing indigenous capacity. Moreover, EVMs manufactured in foreign countries or containing vital parts sourced from such countries raise important issues about security and trustworthiness of these machines and concerns about foreign interference. Such concerns have recently

[28] Department of Homeland Security: Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[29] NBC News: With election cybersecurity experts in short supply, some states call in the National Guard, https://www.nbcnews.com/tech/security/election-cybersecurity-experts-short-supply-some-states-call-national-guard-n1238893

been raised in the US by the three largest EVM vendors, Hart InterCivic, Dominion Voting Systems and Election Systems & Software, who have sought explicit guidance from the Department of Homeland Security and supporting legislation, regarding their dependency on components manufactured by companies based in or having links with China and Russia[30,31].

Technical Issues to consider in implementing EVMs

i) The state of Information Technology infrastructure in the country and within the EMB;

ii) Design and specifications of the e-voting system

iii) Cyber security

iv) Capacity/skill level for ECP staff and the citizens

Non- Technical Issues to consider in implementing EVMs

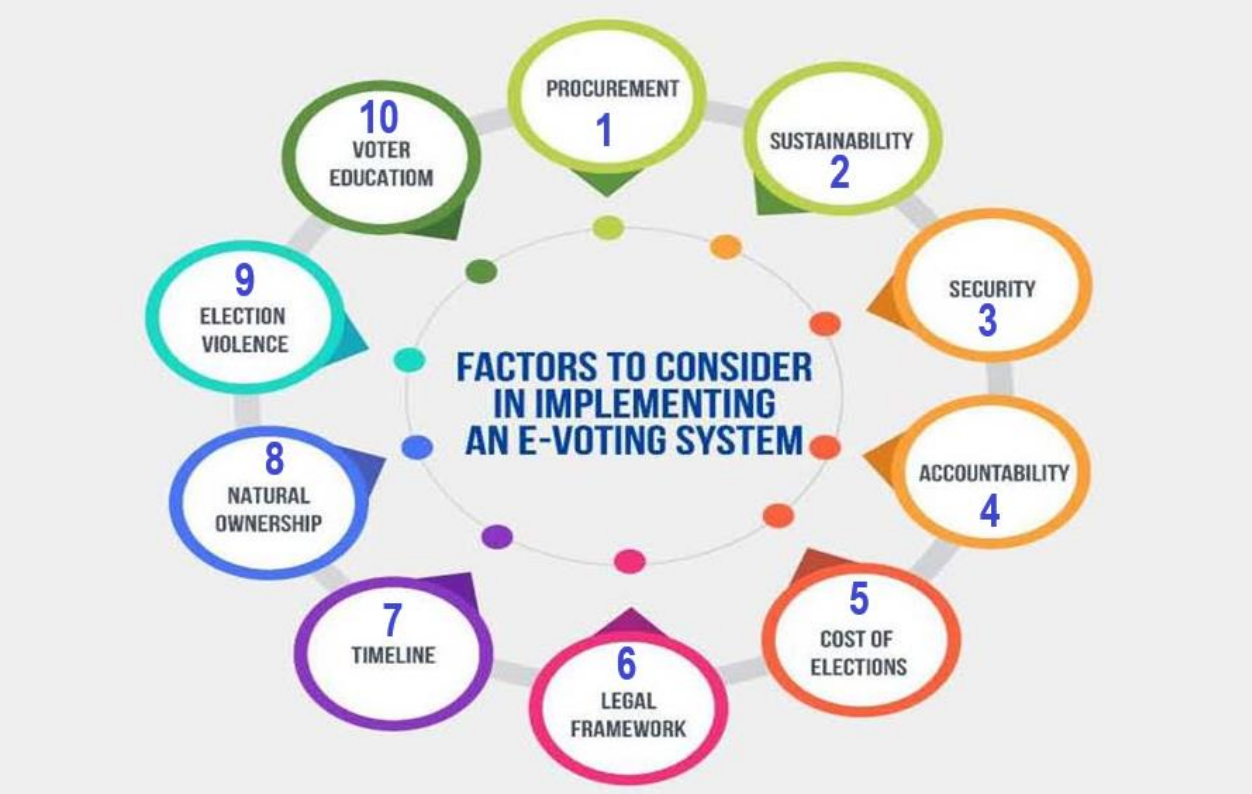
i) The level of consensus and acceptability among stakeholders, dynamic of intergroup relations and EMB trust level.

ii) The legal framework

iii) Budget impact and the cost of elections

[30] Michaela Ross, Bloomberg Law: Chinese Technology in Voting Machines Seen as Emerging Threat, https://news.bloomberglaw.com/privacy-and-data-security/chinese-technology-in-voting-machines-seen-as-emerging-threat, (Jan 10, 2020)

[31] The Wall Street Journal: Voting-Machine Parts Made by Foreign Suppliers Stir Security Concerns, https://www.wsj.com/articles/voting-machine-parts-made-by-foreign-suppliers-stir-security-concerns-11576494003 (Dec. 16, 2019)



Timeline for the implementation: Timing is a critical factor for the implementation of e-voting. There are two dimensions to the time-related issues on EVMs. The first aspect is that time must be sufficient enough to allow for adequate preparations, especially in terms of feasibility studies, procurement of hardware and software as well. Stakeholders' engagement and buy-in is mandatory. The second aspect relates to the spacing of the implementation, starting with pilot tests which will be progressively increased until the whole elections can be covered at once. Procurement processes of such magnitudes require considerable amount of time, especially if the equipment will be sourced from outside the country. Consistent with international best practices, a longer preparatory period for the full deployment of the EVMs should be respected. In most cases, the timeline for proper implementation of EVMs is measured in years rather than months, even for pilots.

TERMS OF REFERENCE OF EVM TECHNICAL COMMITTEE

i) To Determine Best Practices, Standards and Scope as per EVM Technical Committee ToRs:

In order to define the international best practices in implementation of EVM in Pakistan and to define the standards that are needed to support the EMB in implementation of such large scale projects with a critical infrastructure following standards and best practices are proposed;

a) Initiate the extensive consultation process with political parties, Election Management Bodies, CSO, technologist, bar council and academia etc.

    i) By organizing Meetings, Seminars, workshops and discussion forum in academia.

b) Witness the internationally implemented technologies by visiting the practicing countries for capacity building and to take foreign inputs to move forward.
c) Piloting of suitable popular EVM types (Optical Scan and DRE both touch screen and button) and conduct of comparative analysis to examine security, usability and other factors.
d) Supportive legislation which also includes piloting, Risk Limiting Audits (RLAs), End to End Verifiable Voting and Dispute Resolution.
e) Institute the Research & Development (R&D) facility to support technical inputs and long term strategy.
f) Define processes for certification and audit of EVM for satisfaction of voters and political parties to bring transparency and also organize multiple hackathons.

    i) This certification and auditing not only includes the machine but also the processes involved in the implementation of technology as defined in point iii of ToRs, feedback of voters, sampling of each process result, incorporation of SOPs etc.

g) Define the procedure and processes for adoption of technology for voter verification as defined in point vii (c) of ToRs.
h) Define the comprehensive plan for digital transformation strategy for enabling voters and other stakeholders to make them aware of the way the EVM is to be used for casting the vote.

    i) Determine goals. Understanding of how digital transformation has changed over time. Today, it goes beyond making an app or opening an IT window.
    ii) Analyze the market and competition.
    iii) Assess the current standing of HR and its capacity building.

iv) Initiate Research work for knowledge based input.
v) Prepare your infrastructure and talent strategy.

i) Define EVM as critical infrastructure and include in the National Security Policy.
j) Plan for cyber security infrastructure and threats on election systems.
k) Define mechanism for handling, maintenance, storage and warehousing of EVM devices as defined in point vii (b) of ToRs.
l) Study and define the best available technology in term of usability and cost effectiveness to include vulnerable groups.

ii) Define process and procedure, possibilities within stringent timeline as per ToR Elicitation and requirements finality:

The roadmap of the electronic elections through EVMs requires a clear distribution of the processes, procedures and the possibilities. The implementation plan divides the roadmap into 11 processes and 100 sub-processes to be executed in a specific order and timelines.

WBS #	TASK TITLE
1	**STEERING COMMITTEE FOR EVM PROJECT**
1.1	Strategize and oversee technical activities
1.2	Present detailed vision for EVMs in Pakistan
1.3	Draft detailed Roadmap for project
1.4	Constitute relevant teams to undertake key activities
1.5	Engage partners and stakeholders to assist with ECP tasks
1.6	Draft EOI/RFP/TOR for Hiring Third Party Audit Firm
1.7	Prepare Activities Plan for Third Party Audit/Certification of EVM
1.8	Issue periodic progress reports to stakeholders
1.9	Benchmark for Evaluation – What are we evaluating against?
1.10	High level analysis of various EVMs used in developing countries
1.11	Investigate application of new EVM security technologies to Pakistan
1.12	Compile list of best practices applicable to Pakistan
1.13	Evaluation of already procured Smartmatic Machines
1.14	Evaluation of MoST machines
1.15	Comparative Analysis of the EVMs

1.16	Map security properties of EVMs to threat model for Pakistan
1.17	Detailed analysis of components and supply chain
1.18	Present recommendations, feasibility report and way forward
1.19	Prepare EVM requirements and Technical Specifications
1.20	Share and get feedback from stakeholders on requirements/technical specifications
2	**HIRING OF THIRD-PARTY TECHNICAL AUDIT FIRM FOR EVM**
2.1	Appointment and designation of RFP/tender review staff
2.2	Estimation and availability of Budget
2.3	Preparing RFP/Tender document for Hiring Audit Firm Specialized in Electronic Voting Machine/Electronic Voting
2.4	Preparation of RFP/tender document
2.5	Preparation of evaluation procedure
2.6	Publication of RFP/tender
2.7	Pre-bid Meetings
2.8	Answer to bidders questions
2.9	Receiving and opening proposals
2.10	Review and technical evaluation of proposals
2.11	Financial evaluation of proposals
2.12	Selection of best bidder
2.13	Contract Signing
3	**EVM PROCUREMENT PHASE**
3.1	Legal framework review and adjustments
3.2	Generation and approval of final EVM Specifications
3.3	Appointment and designation of tender review staff
3.4	Estimation and availability of Budget
3.5	Preparation of tender document
3.6	Preparation of evaluation procedure
3.7	Vetting of Tender from Stakeholders
3.8	Publication of tender

3.9	Pre-bid Meetings
3.10	Answer to bidders questions
3.11	Receiving and opening proposals
3.12	Review and technical evaluation of proposals
3.13	Financial evaluation of proposals
3.14	Presentation and evaluation of prototypes from selected bidders
3.15	Selection of best bidder
3.16	Contract Signing
4	**PROJECT MANAGEMENT UNIT**
4.1	Constitution of Project Management Team
4.2	Project Management Plan/Timelines/Work Breakdown Structure
4.2.1	Create Work Breakdown Structure
4.2.2	Review Work Breakdown Structure with Project Team
4.2.3	Create project activities list and resources assignments
4.2.4	Review and adjust final activities for final schedule
4.2.5	Schedule approved and Baseline Set
4.2.6	Review and Adjust Project Management Plan
4.3	Resource Planning
4.3.1	Create organizational chart and RACI (Responsibility assignment matrix)
4.3.2	Create Communication Management plan
4.4	Risk Management Plan
4.4.1	Identify Risks and Mitigation plan
4.4.2	Review risks and mitigation plan with team
4.4.3	Create Risk log
4.5	Quality Control and Assurance Plan
4.5.1	Define Acceptance Criteria and Quality Metrics
4.5.2	Create Quality Metrics Scorecard
4.6	Monitoring and Controlling
4.6.1	Schedule Weekly Status Meeting

4.6.2	Schedule Executive Project Status Meeting

5	**DESIGN/DEVELOPMENT PHASE**
5.1	Requirements gathering and refinement
5.2	Industrialization of machine prototypes
5.2.1	Ideation and final concept development
5.2.2	Design and production of final hardware prototype
5.2.3	Presentation of prototype and final hardware acceptance
5.3	Firmware and Software development (development and quality assurance)
5.4	Massive tests
5.5	Presentation of prototype and final hardware and software acceptance
6	**HARDWARE PRODUCTION PHASE FOR PILOTING**
6.1	Procurement of components for hardware production
6.2	Small Scale Production of EVM devices for Piloting
6.3	Shipping and delivery
7	**TESTING PHASE**
7.1	Solution Acceptance Testing
7.1.1	Source Code Review and demonstrations of EVM to Stakeholders
7.1.2	Acceptance of EVM by Stakeholders (Trust Building Measures)
7.3	Constitution of EVM Inspection Team
7.3.1	Advisors from Industry/Academia
7.3.2	IT & Admin personnel from ECP
7.3.3	EVM Technical Experts from Vendor/3rd Party Audit Firm
7.4	Preliminary Inspection
7.4.1	Storage condition
7.4.2	Counting of Equipment
7.5	Detailed Inspection
7.5.1	Battery/Power
7.5.2	O/S Firmware
7.5.3	EVM Software/Firmware/Election Management Software Version Check

7.5.4	Security and Vulnerability Testing of EVM
7.6	Preparation of logistics and security plan and execution
7.7	Preparation of Technology Transfer/ Training Plan
7.8	Technology Transfer Training
7.9	Targeted Public Outreach Plan
7.9.1	Social Media
7.9.2	Print and Electronic Media
7.9.3	Awareness session for public, media and other stakeholders
7.9.4	Development of Leaflets
7.10	Execution of Public Outreach Plan
7.11	Preparation of required SOPs
7.12	Preparation of Electoral data
7.13	User Level Training
7.14	Appointment of Technical, Support and Operational Staff
7.14.1	Training of Polling staff
8	**ELECTION READINESS PHASE**
8.1	Warehousing Set up
8.1.1	Warehouse requirements and design
8.1.2	Warehouse Set up
8.1.3	Warehouse Manpower Recruiting and Training
8.1.4	Warehouse Consumables and Supplies Procurement
8.2	Hiring/Appointment and Training of Technical, Support and Operational Staff
8.3	Preparation of Training Plan
8.4	EVM Readiness and final QA
8.4.1	Preparation of Electoral data
8.4.2	Configuration of EVM
8.4.3	Audit/Certification of EVM
8.4.4	Source Code Review and demonstrations of EVM to Stakeholders
8.4.5	Security and Vulnerability Testing of EVM

8.4.6	Acceptance of EVM by Stakeholders (Trust Building Measures)
8.5	Logistics and Distribution
8.6.2	Training for Troubleshooting/Help desk staff
8.6.3	Training of Technical Administrators on Election Management Software/EVM
8.7	Pre Election Audit
9	**ELECTION DAY**
9.1	Election Day support
10	**POST ELECTION AND PROJECT CLOSE PHASE**
10.1	Reverse Logistics
10.2	Post Election Audit
10.3	Project Closure
11	**DIGITAL TRANSFORMATION EXECUTIVE PROGRAM: FROM MANUAL ELECTION TO VOTING WITH EVM (CHANGE MANAGEMENT)**
11.1	Capacity building on election deployments
11.2	Visiting election related customers
11.3	Touring developing installations
11.4	Touring manufacturing installations
11.5	Election project managements training
11.6	Analyze the organizational and team capabilities needed to support a digital-ready electoral body in a EVM environment
11.7	Develop personal, actionable plans to address the strategic, organizational and innovation-based opportunities faced during transformation from manual to electronic elections
11.8	Acquire a concrete view of key strategic drivers of digital transformation with EVMs
11.9	Learn about innovation capabilities of the EVM and to generate more insights on how to implement the technology

(iii) To define the exact scope of work related to EVM and Overseas Voting solution:

The scope of work consists of the following activities to provide the EVM and overseas voting solutions:

i. To identify fundamental security requirements for EVMs and overseas voting.

ii. To conduct detailed vulnerability and suitability analyses of available EVMs overseas voting.

iii. To undertake extensive comparative studies of different EVM types

iv. To undertake rigorous cost-benefit analyses for the EVMs and overseas voting exercise.

v. To formulate detailed technical specifications for EVMs to be deployed in Pakistan

vi. To conduct and oversee rigorous pilot deployments for EVMs and for overseas voting

vii. To conduct & oversee international hackathons for EVMs

viii. To devise appropriate standards and certification processes for EVMs and for overseas voting.

ix. To define procedural safeguards and checks and balances for EVMs and overseas voting.

x. To oversee the manufacturing processes and handling of EVMs and define appropriate checks

xi. To devise strategies to transmit, manage, and publish results from EVMs and from overseas voting.

xii. To devise effective incident response and cybersecurity strategies

xiii. To inform key policy decisions regarding EVMs and overseas voting and to guide the public discourse

xiv. To research and guide stakeholders regarding the ecosystem around EVMs

xv. To investigate the application of technology to improve key components and processes in the election's ecosystem in terms of transparency, trust, and efficiency

xvi. To establish research linkages with universities, research organizations and other election management bodies

(iv) To hire the services of third-party audit firm to prepare specification for proposed solution, develop mechanism and procedure for acquisition, implementation and testing of EVM and Overseas Voting solution in Pakistan as per best practice:

The Election Commission of Pakistan is executing the EVM and overseas voting project by establishing the project management unit and the R&D wing. The Research and Development (R&D) wing will be established to assist the project management unit in the areas where input is sought by conducting the exploratory and experimental studies. However, in order

to ensure that the specifications and recommendations of the PMU are consistent with the best practices in the world the specifications and developments will be audited by a third party. The third-party audit helps in ensuring the following:

i. To formulate and verify detailed technical specifications for EVMs and the overseas voting system to be deployed

ii. To devise appropriate standards and certification processes for EVMs and for overseas voting.

iii. To establish / guide that if the manufacturing and handling of the machine is according to internationally established best practices.

iv. To establish / guide that if the working of the EVMs and the overseas voting systems is secure, trustworthy, free from errors and malfunctions, and it's voter trails are verifiable.

(v) To determine objectively from time to time whether the implementation of use of EVM is possible within the stringent timelines before GE-2023 and also highlight to all stakeholders for its implementation:

The road map for electronic voting machines has been prepared and attached. The Election Commission of Pakistan through the Project Management Unit established for this purpose will keep an objective supervision of the timelines.

(vi) To prepare Expression of Interest (EOI)/ Request for Proposal (RFP) in the light of legal framework and as required by PPRA rules:

After the decision to conduct a pilot or to implement electronic voting, the critical first step is procuring the equipment needed to implement the technology. A comprehensive specification is essential for this procurement process. It is crucially important to ensure that a specification is developed that covers everything that is required from the technology provider.

Comprehensive specifications will form the basis for the procurement of electronic voting or counting equipment.

A comprehensive specification should include the following check list:

a) **Type of Technology** – The specification should indicate which type of electronic voting system (like DRE or OMR) required by election management body.
b) **Scale** – The quantity of required equipment and services may influence the ability of the supplier to deliver these items on time therefore should be clearly specified, especially if customized equipment and software need to be developed.

c) **Timeframe** – The timeframe for delivery will also have a significant influence on suppliers' ability to deliver and, potentially, on the cost of equipment and services as well.
d) **Voter Authentication** – Any requirements for voting machines to authenticate the identity of voters should be clearly identified, such as biometric fingerprint identification.
e) **Audit Mechanisms** – Any requirements for audit mechanisms should be clearly outlined.
f) **Results Transmission Mechanisms** – The means by which results are to be transmitted or transferred from individual voting or counting machines to the central vote tabulation system should be defined.
g) **Power and Environmental Conditions** – Any requirements for machines to operate for periods of time without mains power or to function in extreme temperatures, humidity or dusty conditions should be identified.
h) **Electoral Systems** – The electoral systems should be identified that electronic voting are to be used for
i) **Accessibility Requirements** – Any requirement for the equipment to deal with multiple languages and voters with disabilities should be detailed, including the need for visual and audible interfaces, as applicable.
j) **Security Requirements** – Security requirements for the electronic voting, as well as any security standards that they should comply with, should be detailed.
k) **Access to Source Code** – It is seen as increasingly important that electronic voting and counting solution source code be open to external inspection, if not fully open source, and any such requirements should be included in the specification.
l) **Additional Services** – Other required services, such as project management, configuration, training and support during implementation of the electronic voting or counting technology, should be identified.
m) **Consumables** – The specification should indicate whether it is acceptable for consumables, including paper, ink, cutters, batteries, memory storage units and devices, to be proprietary or whether they must be generic. If only supplier consumables can be used, will the supplier guarantee availability throughout the lifespan of the device, which might be as long as 15 years?
n) **Additional Software Systems** – There may also be a requirement to procure a results transmission, receipt and tabulation system or a more general election management system that would include the electronic voting or counting system.

The specifications for Request For Proposals (RFPs) may also contain following checklist;

a) Responsibility for the repair of faulty or damaged equipment (whether it lies with the EMB or the vendor) and whether the EMB is authorized to make any repairs.
b) Mechanisms for configuration of electronic voting or counting machines prior to each election.

c) The vendor's responsibilities regarding transferring skills and knowledge to the EMB for training its staff and staff operation of the technologies.
d) Consequences for the integrity of stored or in-process data transactions in the instance of a sudden loss of power to equipment.
e) Maximum capacity of electronic voting or counting machines in terms of the number of electoral races and candidates that can be accommodated.
f) Means of verifying that loaded software is the approved version.
g) Mechanisms to demonstrate that the electronic version of the ballot box is empty at the beginning of voting and/or counting.
h) Capacity of the electronic voting system to display photographs or symbols for ballot entities.
i) Mechanisms for review and confirmation of voter choices on the electronic voting solution.
j) Specifications and reliability of any printing device attached to the voting machine.
k) Mechanisms for ensuring the protection of data and secrecy of voters' choices.
l) Mechanism for generation of results at the end of voting or counting, and the ways in which these results are transferred or transmitted for tabulation.
m) Details of the election management system used with the electronic voting or counting technology, including whether the supplier is responsible for providing the tabulation system (software and hardware).
n) Responsibilities and capacities for troubleshooting and other servicing before and during Election Day processes.
o) Life expectancy of electronic voting or counting equipment.
p) Maintenance and storage requirements for equipment between elections.

(vii) To examine and analyze any future enabling requirements as and when needed:

a. Customized vs Readymade EVMs

After setting-up the PMU with the best possible expertise comprising of hardware, software, data and security experts, ECP will establish its own R&D wing to identify the customized requirement for the development of EVMs in Pakistan. The ECP may observe that the EVMs developed indigenously are up to the standards set by the ECP after confirmation by the third-party endorsement. The commercially available EVMs world-wide are designed to deal with the requirements of a specific type and may not fully comply with the electoral requirements of the country.

b. Storage (Provincial vs Divisional)

The storage of the EVMs in secure physical locations is an essential requirement. The establishment of the physical storages at either the provincial, divisional, or district headquarters is a strategic decision to be taken by ECP considering the level of security, temperature, transportation cost etc. While planning EVM warehouse storage, properly

defined policies and procedures should be documented for its implementation by considering the following aspects.

i. Inventory Management
ii. Security
iii. Storage Environment
iv. Durable Equipment
v. Location of Packing
vi. Packing Control
vii. Health and Safety Standards
viii. Asset Management
ix. Disposal Schedule and Procedure
x. Transportation
xi. Delivery sites
xii. Transportation security

c. Integration of Biometric verification system with pros & cons and challenges

Voter identification is required during two phases of the electoral process: first for voter registration in order to establish the right to vote and afterwards, at voting time, to allow a citizen to exercise their right to vote by verifying if the person meets all the requirements needed to vote (authentication).

Fingerprint recognition is the electronic method of recording and recognizing an individual. Identification can be achieved in a few seconds with reasonable accuracy. As a result, the use of automated fingerprint identification systems (AFIS) that records, stores, searches, matches and identifies fingerprints is obtaining rapid acceptance. AFIS can be integrated with a microcontroller and other peripherals to form an embedded system which is a comprehensive electronic voting machine with fingerprint print identification system[32].

The picture and fingerprint biometric of voters will be captured in biometric device to assist those voters who have problems in fingerprint identification. The legitimate voter would be identified through scan or data entry of CNIC number and details can be verified manually though machine. The machine will record all the data and mark biometrically unidentified legitimate voters as supervised by the Presiding Officer.

ADVANTAGES

i. Providing the preventive measures against the run-time errors in the voting system.

[32] Electronic Voting Machine Authentication using Biometric Information. International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Published by, www.ijert.org
NCETET - 2017 Conference Proceedings, Special Issue - 2017

ii. It completely rules out the chances of spurious votes which results in problems in electoral process, and in law and order.
iii. It brings transparency and auditability in the system.
iv. The system can also restrain polling staff to imitate the process.
v. Lower risk of human and mechanical errors.

DISADVANTAGES

i. Each fingerprint voting system depends on an important external factor which is the fingerprint's image. The resolution and the quality of the image have huge impact on the system. This system works well with high quality image, but its working is compromised when the available image is of low quality. Very low-quality image leads to rejecting the image or to false rejection.
ii. Database Images have a large size with resolution of eight bits per pixel. Uploading a large number of fingerprints image to the database demands a large memory space and internet availability at a higher bandwidth. Large number of voters mean more fingerprint images to be stored into the database which makes the database slower and leads to slower voting process.

CHALLENGES

i. Training needs to be conducted for biometric authentication of the voters
ii. Availability of Electoral Rolls (ER) Data along with facial images of the voters and fingerprint biometric
iii. Configuration and data loading of ER data in a stipulated time period on biometric devices
iv. Inherent weakness in this system of false acceptance or false rejection.
v. People with damaged fingerprints and ladies with mehndi or dye on their hands cannot be authenticated from the BVM system properly.

(viii) To assess any activity / process with the assistance of 3rd party audit expert entity, if and when required:

The inclusion of third-party audits will increase the quality of this project of implementing the electronic voting in local and overseas environment. There are some vulnerabilities where the national or international third-party audit will be needed to improve the quality of the process and the overall project:

a. To establish the specifications of the EVMs to be developed
b. To establish the confidence in the EVMs manufactured by the vender for the purpose of trust to use them as an instrument to conduct elections.

REPORT OF THE FINANCIAL COMMITTEE

(A) FINANCIAL ASPECTS OF ELECTRONIC VOTING MACHINE

The activity wise breakup of EVM project along with its estimated costs are hereby given below;

Activities	Amount in PKR
A) Electronic Voting Machines (EVM) 400,000 EVMs @ PKR **380,000** per unit including taxes plus Services, Support and Maintenance (SLA) with array power bank	152 Billion (Machine Cost) **+** 23 Billion (Support, Services and Maintenance Cost) 15% of Total Cost
B) Project Management i. Staffing ii. Procure / Specify Solution iii. Develop / Adopt Solution iv. Trainings v. Testing / Acceptance vii. Execute Full Scale Rollout vi. Real-time tracking on GIS viii. EMS Dashboard	1 Billion
C) Warehousing, Storage and Maintenance 30 Sites at regional level (25,000 Sq. Ft per Location) Air Conditioning, Anti Dust, CCTV & Access Control Security, Fire Detectors & Extinguishers, HR, Power Backup, Security Staff/Guards	35 Billion
D) Hiring and Training of Staff *(including backup pool)* i. Lead and Master Trainers: **10,000 approx.** ii. EVM operators / APOs : **400,000 approx.** iii. Technical Staff for 5 Assembly Lines and Support in Polling Stations: **150,000 approx.**	10 Billion
E) Third party Audit of EVM	800 Million
F) Logistics, Transportation, Data Integration and EVM Configuration, Check Testings and Factory Assembly Lines Rental of around 2,000 Specialized Trucks (200 EVMs per truck), Administration & Operational Cost, GPS trackers, Drivers/Helpers	20 Billion
G) EVM R & D, Certification and Security Labs (Technical & Support Staff) (Laptops, Computers, Printers, Scanners, Copiers, GPS Devices, Mobiles, Storage Devices, Software Licenses & Other IT Gadgets)	800 Million
H) Mass Media Campaign / Voters Awareness and Large scale Publicity over a period of 3 years with consultative forums with all major stakeholders	15 Billion
TOTAL	**258 Billion** **(Approx.)**
Grand Total (A+B)	**260.5 Billion** (approx.)

The assessments in this section are approximately and based on current general standards, estimates, prevailing Forex rates and economic circumstances relating taxes, etc .

(B) FINANCIAL DETAILS OF ELECTRONIC VOTING MACHINES (EVM)

(i) Purchase of Machines & Services:

ECP intends to procure approximately 400,000 machines for the conduct of elections through Electronic Voting Machines (EVMs) for approximately 100,000 countrywide polling stations. An average of 3 machines per polling station are required alongwith 1 machine per polling station as backup purpose. The purchase of 400,000 EVMs (hardware and software) will incur the approximate cost of 152 Billion PKR approximately. Furthermore, alongwith these machines, various services pertaining to support and their maintenance are also required to be obtained from the vendor/firm. In this regard, Service Level Agreements are also needed with the firm. As per estimate, 23 Billion PKR will be required for support, services and maintenance cost including GST.

(ii) Project Management:

To conduct the countrywide elections through EVM is a gigantic task for such a country having approximately 122 million voters. Therefore, to manage the whole project, many requirements need to be fulfilled like human resource, developing & adopting solution, impart trainings, testing & acceptance, real-time tracking on GIS and EMS dashboard etc. All such activities shall be planned, executed and monitored by the Project Management team on real time basis. For the said purpose, specialized and customized MIS/GIS solutions with dashboards are required. To perform/accomplish these tasks, services of professional team are required which will approximately cost 1 billion rupees. Ideally the work of the PMU will be supervised by a high-level Steering Committee reporting directly to the Commission.

(iii) Warehousing, Storage & Maintenance:

Storing/housing of 400,000 machines at a standard / safe place before & after the elections is also a hard task. For this purpose, a plan has also been proposed according to which 30 sites (warehouses) at divisional levels having minimum area of 25000 Sqf are recommended. These warehouses should have proper air conditioning system, anti-dust environment, rodent repellent, heat and humidity control, CCTV & access control security system, fire detectors and extinguishers, human resource, power backup, security staff / guards. All such warehouses need to be placed fully under the control of ECP. For this purpose, acquiring of land for warehouses and their construction, maintenance, logistics, transportation may incur approximately 35 billion rupees. If over a period of time these storage sites are not de-

regulated to the divisional level, the storage costs plus transportation from federal or a provincial site may be very high.

(iv) Hiring & Training of Staff:

Machines without skilled user are useless. The skilled professionals are always behind any successful technical project. As per plan, ECP will require approximately 10,000 Lead & Master Trainers and 400,000 EVM operators / APOs (1 per machine) including skilled backup staff pool. Moreover 150,000 technical / support staff for 5 Assembly Lines & Support are also required. To fulfill such requirements and resources, approximately 10 billion rupees are required.

(v) Third Party Audit of EVMs:

Performing a third party audit on any project before & after its commencement is very essential for transparency as well as to assess any bugs or loop-holes in the system. To do this, ECP has planned to conduct a third party security audit of EVM machines. Such resource is not available within the country. For this ECP may have to involve international vendors which will incur approximately 800 million rupees.

(vi) Logistics, Transportation and Configuration of EVMs:

To conduct any election through EVMs, configuration of EVMs with data population and integration is required before its transportation to the polling stations. Furthermore, all machines shall be securely transported back to the warehouse after its usage in election. For a general election, this will be a huge task which will require extensive resources and efforts. Main challenge would be to carry out these activities on 400,000 plus machines in the stipulated time period which may incur involvement of human resource, vehicles, fuel etc. As per estimate, this will incur approximately, 20 billion rupees.

(vii) EVM R & D, Certification & Security Labs:

Before EVM usage in any election, it is mandatory for the EVM to be fully compliant to the regulations set by the regulatory authorities/international standards. For this purpose, international companies shall be required to perform the certification process. In addition to this, Research and Development teams shall be constituted along with EVM Certification and Auditing Laboratory where various tests of EVM could be performed. Various IT Gadgets

like Laptops, Computers, Printers, Scanners, Copiers, GPS Devices, Mobiles, Storage Devices, Software Licenses & Other IT Gadgets are required. This may cost around 800 million rupees.

(viii) <u>Voter Awareness / Media Campaign:</u>

Introducing new idea / technology requires change management process for its adoption and success. In order to make aware the masses and stakeholders about the new way of voting through EVM, proper media campaigns and engagement of various stakeholders is required at different stages of EVM implementation. Large scale media campaign for the voters is essential to make the process clear, transparent and adoptable. These media include electronic, radio, print, social media, SMS, TV advertisements, documentaries, seminars, posters, banners etc., for a sustained period of time.

REPORT OF THE LEGAL COMMITTEE

The Legal Committee has drafted the following vital legal amendments that need to be addressed during legislation;

Existing Laws	Proposed Amendments	Rationale of Legislation before Incorporation of Electronic Voting Machine
Nil	**Section 2** **(xx-A) "voting machine"** means any machine or apparatus whether operated electronically or otherwise used for giving or recording and counting of votes and any reference to a ballot box or ballot paper in this Act or the rules made there under shall, save as otherwise provided, be construed as including a reference to such voting machine wherever such voting machine is used at any election.	EVM is a combination of electromechanical or electronic equipment that is used to cast, store, tabulate and count votes; to display and declare the election results. The different types of voting machines allow for various kinds of operations ranging from touch screen to button based technologies, such as LCD monitor, pressing a button and optical scanner. Usually, the technology is finalized on the basis of legal provisions in the law with its features. Since, no features or operations are mentioned in the law. Therefore, technology is handicapped for its opting. It is recommended that features of machine or e-voting system should be defined in the law prior its introduction.
Chapter V "CONDUCT OF ELECTIONS TO THE ASSEMBLIES"		
Section 103. Electronic voting.— Notwithstanding anything contained in this Act or rules made thereunder, the Commission shall, with the technical assistance of any authority, or agency, procure and use in prescribed manner, subject to secrecy and security, stand-alone electronic voting machines in general elections in Pakistan."		Article 218(3) of the Constitution of the Islamic Republic of Pakistan obliges the Election Commission ***"to organize and conduct the election and to make such arrangements as are necessary to ensure that the election is conducted honestly, justly, fairly and in accordance with law, and that corrupt practices are guarded against."*** Article 218(3) of the Constitution must necessarily be read and interpreted in harmony with the Article 222 of the Constitution and not in isolation. The substitution of Section 103 of Elections Act, 2017 does not provide voting and counting procedure through electronic voting machine. The existing law deals with the detailed procedure of manual voting and counting through ballot papers therefore, the express provision
Nil	**103 A. Voting machines at an election.—**Notwithstanding	

	anything contained in this Act or the rules made there under, the giving and recording of votes by voting machines in such manner as may be prescribed, may be adopted in such constituency or constituencies as the Election Commission may, having regard to the circumstances of each case, specify.	is required to give legal cover to the electronic voting and counting process. As observed by the Indian Supreme Court in **A. C. Jose vs Sivan Pillai & Ors (1984 AIR 21)** wherein, Court declared the election from the constituency void and directed a re-poll to be held in the 50 polling stations where EVMs were being used. On 19th May, 1982, the Election Commission of India issued directives under Article 324 of the Constitution of India for the use of EVMs and conducted elections at fifty polling stations using the machines in an election in 70-Parur Assembly Constituency (AC) of Kerala on an experimental basis. The EVMs were further used in 10 Bye-elections across the country in 1982-83. However, due to absence of any specific law prescribing the use of EVMs, the election was challenged in a petition and on 5th March, 1984, the Supreme Court of India held that EVM cannot be used in an election unless a specific provision is made in law for its use. Election Commission has to conduct elections according to law enacted by Parliament and it could in exercise of its powers under Article 234 of the Constitution, supplement the law but not supplant it. The amendment through Section 103 does not provide any provision for resolution of election dispute and mechanism to guard against corrupt practices. It is proposed that appropriate amendment may also be made in chapter-IX and X of Elections Act, 2017 dealing with election dispute. It is further proposed that the amendments and new legislation may be incorporated in the Elections Act, 2017 to conduct the elections through EVMs.
Nil	**103 B. Supply of Electronic Voting Machines.—** (1) Every electronic voting machine shall be of such design as may be prescribed and approved by the Commission. (2) The Returning Officer shall provide each Presiding Officer with such number of electronic voting machines as may be necessary. (3) Not more than one electronic voting machine shall be used at a time for the purpose of the poll at any polling station, or where there are more than one polling booths at a polling station, at any polling booth. (4) The electronic voting machine used at polling station shall bear a label marked with— (a) the serial number of machine, if any, (b) number and name of the constituency(ies); (c) number and name of the polling station; and (d) the date of poll. (5) Immediately before the commencement of the poll, the presiding officer shall demonstrate to the polling agents and other persons	

	present that no vote(s) has been already recorded in the voting machine. (6) To ensure secrecy and security of electronic voting machine, the Commission shall prescribe a mechanism. (7) Before the time fixed for the commencement of the poll, the Presiding Officer shall ensure that every electronic voting machine to be used is properly configured and zero reported	
Nil	**(103-C)** Where the Presiding Officer is of opinion that booth capturing, machine snatching or tampering is taking place at the Polling Station or at a place fixed for the poll, he shall immediately stop the poll and inform the Returning Officer for seeking appropriate orders that he has done so.	
Nil	**103 D. Proceedings at the close of poll where electronic voting machine is used.—** (1) After the close of poll, the Presiding officer shall close the EVM as per prescribed manner to ensure that no further votes can be recorded. (2) After the close of poll, the Presiding Officer in the presence of such of the contesting candidates, election agents, polling agents and authorized observers as may be present, declare the result of poll in the prescribed manner. (3) The Presiding Officer shall give such of the contesting candidates, election agents, polling agents and authorized observers as may be present reasonable facility of observing the EVM during result tabulation process and give them such information with respect to the count as can be	

	given consistent with the orderly conduct of the count and the discharge of his duties in connection with the count. (4) The Presiding Officer shall provide to the contesting candidates, election agents and polling agents for generating copies of the results as a token of proof. (5) The Presiding Officer shall, immediately after the count, prepare a Result of the Count in such form as may be prescribed. (6) The Presiding Officer shall seal the EVM as may be prescribed and take the same to the Returning officer for safe storage as may be directed by the Commission.	

Chapter-IX "ELECTION DISPUTES"		
At present, no provision exists in the Elections Act, 2017 for resolution of election disputes arising out of voting through EVM.	It is proposed to make amendments in Chapter IX relating to Election Disputes.	
Chapter-X "OFFENCES, PENALTIES AND PROCEDURES"		
167. Corrupt practice.— A person is guilty of the offence of corrupt practice if he— (a) is guilty of bribery, personation, exercising undue influence, capturing of polling station or polling booth, tampering with papers, and making or publishing a false statement or declaration; (b) calls upon or persuades any person to vote, or to refrain from voting, for any candidate on the ground that he belongs to a particular religion,	**167. Corrupt practice.—** A person is guilty of the offence of corrupt practice if he— (a) is guilty of bribery, personation, exercising undue influence, capturing of polling station or polling booth, tampering with papers, **snatching the EVMs**, and making or publishing a false statement or declaration; (b).....	Article 218(3) of the Constitution of Islamic Republic of Pakistan obliges the Election Commission ***"to organize and conduct the election and to make such arrangements as are necessary to ensure that the election is conducted honestly, justly, fairly and in accordance with law, and that corrupt practices are guarded against."*** Article 218(3) of the Constitution must necessarily be read and interpreted in harmony with the Article 222 of the Constitution and not in isolation. The substitution of Section 103 of Elections Act, 2017 does not provide voting

province, community, race, caste, bradari, sect or tribe; (c) causes or attempts to cause any person present and waiting to vote at the polling station to depart without voting; or (d) contravenes the provisions of section 132	(c)..... (d).....	and counting procedure through electronic voting machine. The existing law deals with the detailed procedure of manual voting and counting through ballot papers therefore, the express provision is required to give legal cover to the electronic voting and counting process. As observed by the Indian Supreme Court in **A. C. Jose vs Sivan Pillai & Ors (1984 AIR 21)** wherein, Court declared the election from the constituency void and directed a re-poll to be held in the 50 polling stations where EVMs were being used. On 19th May, 1982, the Election Commission of India issued directives under Article 324 of the Constitution of India for the use of EVMs and conducted elections at fifty polling stations using the machines in an election in 70-Parur Assembly Constituency (AC) of Kerala on an experimental basis. The EVMs were further used in 10 Bye-elections across the country in 1982-83. However, due to absence of any specific law prescribing the use of EVMs, the election was challenged in a petition and on 5th March, 1984, the Supreme Court of India held that EVM cannot be used in an election unless a specific provision is made in law for its use. Election Commission has to conduct elections according to law enacted by Parliament and it could in exercise of its powers under Article 234 of the Constitution, supplement the law but not supplant it. The amendment through Section 103 does not provide

		any provision for resolution of election dispute and mechanism to guard against corrupt practices. It is proposed that appropriate amendment may also be made in chapter-IX and X of Elections Act, 2017 dealing with election dispute. It is further proposed that the amendments and new legislation may be incorporated in the Elections Act, 2017 to conduct the elections through EVMs.
169. Personation.— A person is guilty of personation, if he votes or applies for a ballot paper for voting, as some other person whether that other person is living or dead or fictitious	**169. Personation.—** A person is guilty of personation, if he votes or applies for a ballot paper for voting or to **vote through EVM**, as some other person whether that other person is living or dead or fictitious.	
171. Capturing a polling station or polling booth.— A person is guilty of capturing a polling station or polling booth if he— (a) seizes a polling station or a polling booth or a place fixed for the poll or makes polling authorities surrender the ballot papers or ballot box or both and does any other act which affects the orderly conduct of elections; (b) takes possession of a polling station or a polling booth or a place fixed for the poll and allows his supporters to exercise their right to vote while preventing others from free exercise of their right to vote; (c) coerces, intimidates or threatens, directly or indirectly, any voter and	**171. Capturing a polling station or polling booth.—** A person is guilty of capturing a polling station or polling booth if he— a) seizes a polling station or a polling booth or a place fixed for the poll or makes polling authorities surrender the ballot papers or **EVMs** or ballot box or all and does any other act which affects the orderly conduct of elections; (b)..... (c).....	

prevents him from going to the polling station or a place fixed for the poll to cast his vote; or (d) being in the service of any Government or corporation or institution controlled by the Government, commits all or any of the aforesaid activities or aids or connives in, any such activity in furtherance of the prospects of the election of a candidate.	(d).....	
175. Illegal practice.— A person is guilty of the offence of illegal practice if he— (a) is guilty of disorderly conduct near a polling station, canvassing in or near a polling station, interferes with the secrecy of voting, or adversely affects the interests of a candidate; (b) obtains or procures, or attempts to obtain or procure, the assistance of any person in the service of Pakistan to further or hinder the election of a candidate; (c) votes or applies for a ballot paper for voting at an election knowing that he is not qualified for, or is disqualified from, voting; (d) votes or applies for a ballot paper for voting more than once in the same polling station; (e) votes or applies for a ballot paper for voting in more than one polling station for the same election; (f) removes a ballot paper from a polling station during the poll;	**175. Illegal practice.—** A person is guilty of the offence of illegal practice if he— (a)..... (b)..... (c) votes or applies for a ballot paper or **for a vote through EVM** for voting at an election knowing that he is not qualified for, or is disqualified from, voting; (d) votes or applies for a ballot paper or a **vote through EVM** for voting more than once in the same polling station; (e) votes or applies for a ballot paper or for a **vote through EVMs** for voting in more than one polling station for the same election; (f) removes a ballot paper or **any paper of the EVM** from a polling station during the poll;	

(g) violates restrictions on publicity laid down in section 180 or restrictions on announcement of development schemes under section 181;	(g)	
(h) violates prohibition on public meetings during a certain period as provided in section 182;	(h)	
(i) fails to comply with section 134 relating to election expenses;	(i)	
(j) carries or displays any kind of weapon or fire arm in a public meeting or procession during campaign period, on the poll day and till twenty four hours after the announcement of the official results by the Returning Officer;	(j).....	
(k) resorts to aerial firing or uses firecrackers and other explosives at public meetings or in or near a polling station; or	(k).....	
(l) resorts to violence in any form or manner against an election official or any other person officially deputed to work at a polling station. Explanation.—The word —weapon‖ used in clause (j) includes a danda, lathi, knife, axe or any other thing which can be used as a weapon to inflict injury to a person.	(l).....	

We believe the challenges listed above are significant and we must be very careful not to underestimate them. However, we also believe that these challenges can be satisfactorily addressed, as evident from the example of countries like Brazil, India, Estonia and others, which have successfully deployed election technology. To avoid the pitfalls suffered by these countries, it is essential to learn from them.

5.1 Guiding Principles

Key Considerations in EVM Implementation

The adoption of election technologies, like in most democracies, is a very complex subject matter as there are many variables, technical and non-technical, that need to be taken into consideration by the Electoral Management Bodies (EMBs) for successful implementation of e-voting. The capacity and manner in which these challenges are resolved will determine whether e-voting will constitute an asset or liability to the electoral process. Basic considerations on e-voting center around four key principles namely SUSTAINABILITY, COST EFFECTIVENESS, APPROPRIATENESS, and TRANSPARENCY, with security considerations serving as a cross cutting factor across all these principles. These principles are defined as follows:

➢ **Sustainability** – This refers to electoral policies and practices in relation to e-voting which are in line with the needs and expectations of stakeholders both now and in the future, aiming to minimize reliance on external inputs and resources.

➢ **Cost Effectiveness** – This principle stresses the re-usability of the e-voting technology to be adopted. The cost must relatively be cheaper than a manual voting system. However, this can be difficult due to the huge capital investment at the initial stage and rapid changes in the ICT sector which make ICT hardware and software procured few years ago to become obsolete over time.

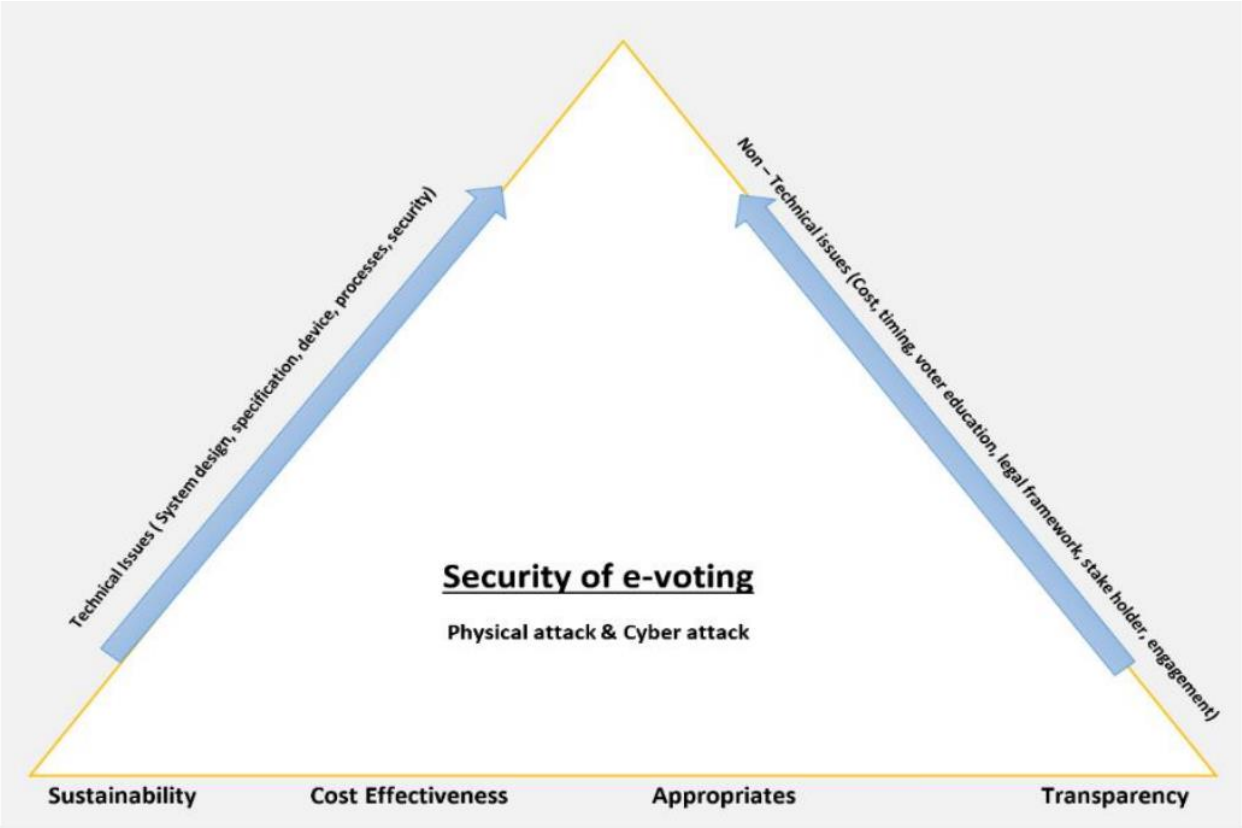
➢ **Appropriateness** – This is usually used to describe suitable simpler technologies especially within the context of developing countries with weak infrastructural base and less literate population.

➢ **Transparency** - Every stage of a transparent election must be open to auditing and examination by stakeholders (political parties, election observers and the general public), who are able to verify that the process is conducted in line with procedures and irregularities have not been perpetrated and are open.

➢ **Security** - Underlining all these basic principles is the need for security of the e-voting system, not only in terms of physical safety of the ICT equipment and facilities but also protection from cyber-attacks and manipulation especially by third parties. Applying the

principles of sustainability, cost effectiveness, appropriateness and transparency must therefore be considered within the overarching context securing an e-voting system.

The need to comply with these basic principles raises technical as well as non-technical issues to be addressed in the implementation of e-voting. These principles are universal; however, they can be uniquely applied in accordance to different electoral contexts and define the kind of questions to be raised and addressed.



Fabio Bargiacchi: *"Counting the Ballots and Accounting for the Votes. The use of Technology for Enhancing the Transparency of the Electoral Process" presented at The Association of World Electoral Bodies (A-WEB) International Conference on Bucharest, 1-2 September 2017.*

We first define key principles which are fundamental to successful deployment of election technology in Pakistan, and which should guide our strategy on the way forward. Key security concerns include the following:

Ballot secrecy is recognized as a fundamental human right and is enshrined in Article 21 of the Universal Declaration of Human Rights[33]. Ballot secrecy is a primary requirement in Article 226 of the Constitution of the Islamic Republic of Pakistan, 1973 and in Section 94 of the Elections Act, 2017. A voter's choice must be kept strictly private to prevent outside

[33] United Nations: Universal Declaration of Human Rights, https://www.un.org/en/about-us/universal-declaration-of-human-rights

influence, bribery, or coercion, which corrupts the electoral process, and ultimately undermines democracy itself.

Electoral integrity refers to the accuracy and correctness of the results of the electoral exercise. Citizens should derive confidence that the elections have been conducted fairly and that the results correctly reflect the will of the public. Considering election technology like EVMs or Internet voting, this element of trust can be engendered in various complementary ways:

i. By **democratizing** the debate on election technology, engaging stakeholders, and striving for consensus on key decisions regarding technology

ii. By adding **redundancy** mechanisms to support the technology, such as paper trails for EVMs, receipts for Internet voting, etc.

iii. By making the inner workings of these systems more **transparent** using mechanisms such as cryptographic checks, public tallying, post poll statistical audits, machine logs, random EVM checks, etc.

iv. By giving voters **guarantees** on how their vote has been processed, using phone checks, Internet tracking mechanisms, etc.

Next, we will describe essential non-security principles for deploying election technology:

Usability refers to the ease with which voters can cast their votes effectively. Usability of technology depends on a variety of social and cultural factors and can vary significantly from region to region. A series of rigorous pilots and mock polls must be undertaken prior to any large-scale deployment to ensure that EVMs do not exclude certain eligible citizens or impair their ability to cast their votes.

Accessibility extends the concept of usability to differently-abled citizens. Ideally, EVMs should provide equal opportunities for access and participation. If this is not possible, initially, alternate voting arrangements must be made for excluded voters, which ensures ballot secrecy and electoral integrity.

Sustainability refers to practical concerns and costs of deploying EVMs. Pakistan is a developing country and efforts should be made to emulate the model of India and Bangladesh, which chose to invest in indigenous expertise and developed low-cost machines suited to their environments. Moreover, EVMs should be usable for at least three to four electoral cycles, which necessitates that the technology be broadly aligned with future trends and innovations.

It is very important that these properties be clearly identified by stakeholders. The research literature acknowledges that several of these properties inherently conflict with each other and a workable acceptable balance must be sought. For instance, ballot secrecy and electoral integrity are directly at odds with each other, as the act of anonymizing votes in an electronic

system tends to make it very difficult to track and protect them from being manipulated. Likewise, researchers note that stakeholders may unwittingly tend to conflate electoral efficiency with electoral transparency. Michael Yard of IFES notes: "*This is not to say the efficiency in elections is, in itself, a bad thing; on the contrary, it is only when efficiency comes into conflict with transparency that it becomes undemocratic.*"[34] A narrow focus on efficiency can result in deployment of "*black box*" components that "*lead to more efficient development and employment*", but this risks transferring power "*away from the many*" into the "*hands of the few*"[35]. As a baseline, to justify the use of EVMs for elections in Pakistan, we should identify a system that, at the very minimum, provides significant advantages over paper-based elections. These advantages could be in terms of superior security, greater transparency, reduced election costs, simplified logistics, etc. These benefits need to be documented and spelled out explicitly in rigorous cost-benefit analyses.

5.2 Open Questions and Knowledge Gaps

Considering the key guiding principles listed above, there are several critical questions and knowledge gaps that require urgent resolution. For example:

a) It is not yet clear exactly which problems EVM will solve on the ground. There is a common conception of EVMs being more 'secure' than paper based elections, but security is an umbrella term for an entire spectrum of issues, some of which EVMs will solve but also others which they likely will not. It is also not clear how effective EVMs will be at solving these problems and whether these benefits justify the cost of this entire exercise.

b) It is widely recognized that deploying technology to solve security risks likely creates new security problems, which we are not yet able to predict. These risks must also be clearly defined and addressed with a proportionate response if trust in elections is to be maintained. A thorough risk-assessment exercise is needed before embarking on large-scale EVM deployment.

c) Current legislation mandates the ECP to procure and deploy EVMs "*in prescribed manner, subject to secrecy and security*". It is an open question if generic EVM types provide adequate secrecy and security, as evidenced in recent and ongoing election controversies in countries like India and the United States. The ECP's highest priority therefore is to identify, confirm and, moreover, to demonstrate effectively to stakeholders that EVMs that we deploy ensure ballot secrecy and electoral integrity.

[34]Direct Democracy, Progress and Pitfalls, https://www.ifes.org/sites/default/files/20111026_direct_democracy_progress_and_pitfalls_election_technology_yard_0.pdf]

[35] Nic Cheeseman, Gabrielle Lynch & Justin Willis: Digital dilemmas: the unintended consequences of election technology, https://www.tandfonline.com/doi/pdf/10.1080/13510347.2018.1470165?needAccess=true&__cf_chl_managed_tk__=uV7i.fCW5R2rX73iNOYwmo86brs42RyoADHCwdGQFSI-1641149087-0-gaNycGzNCJE

These fundamental knowledge gaps in our understanding give rise to a whole chain of other uncertainties. For instance:

a) We cannot at this point ascertain whether EVM types on the market are suitable for deployment in Pakistan or do we have to customize them. Or do we design our own machines from scratch? Different countries have opted for different strategies, and each has its pros and cons which we must consider

b) We are unable at this point to ascertain the logistics of the entire EVM exercise. For instance, we do not know how many machines will be required. Simple button-press EVMs (used in India) can only accommodate a small number of candidates and multiple machines may be required in each polling booth for different races. On the other hand, EVMs with keypads or touchscreens or scanners can accommodate much larger numbers of election types and candidates on the same machine.

c) Likewise, some EVM types require specialized storage with temperature control facilities, which adds significantly to costs. The storage strategy will also have to decide if the EVMs are stored at central, provincial or divisional level. Maintenance and handling costs and processes will also differ considerably for machine types.

d) Introduction of EVMs will also likely necessitate a rethink of fundamental election practices in Pakistan and necessitate specific legislation. For instance, since most EVMs tally results within minutes of polls closing, should vote counting and results announcement happen in a distributed fashion or in a centralized manner as is the case with paper-ballots?

e) Logistics and costing concerns could potentially affect the modality of the entire EVM exercise. If the costs and manpower requirements prove excessive, we may even have to consider staggering general elections over days or weeks as in the case of India.

It is for these reasons that we still have no reliable estimates for logistics and costing of EVMs or of their timelines for deployment. Various EVM vendors have briefed the ECP on their products, but as yet there remain considerable questions about their quality, security guarantees and transparency, their usability and accessibility, and what sort of ecosystem is needed to support them.

As an example of these knowledge gaps, we note that there are huge question marks on the suitability of biometric verification of voters at polling stations: a small but significant number of citizens do not have their fingerprints on the official record. Also, fingerprint verification bears a small percentage of false positives. **Most importantly, however, fingerprints tend to become less recognizable after a certain age or in people who do a large amount of manual labour with their hands, and verification in these cases can fail**. Do the benefits of biometric verification outweigh the costs? Considerably more research and dialogue is needed to answer this. However till we research this aspect, more, the answer to using this technology right away is clearly a “No”.

Such questions arise for every country that considers deploying election technology and they are ideally addressed by undertaking extensive technical analyses, testing EVMs in mock polls and pilot projects, and involving stakeholders in wide-ranging discussion and policy decisions. We expect that once we start to examine the applicability of EVMs in Pakistan in earnest, we will discover that there are tradeoffs that must be carefully analyzed and debated. Unfortunately, these crucial exercises have yet to be undertaken in earnest in Pakistan. Better now than never!

Next, we present future roadmap to address the challenges.

5.3 Future Roadmap

Drawing on the history and experience of election technology deployments in various countries, we recommend a multi-pronged strategy as follows:

1. **the ECP should set up a dedicated Research and Development (R&D) Wing** to address critical knowledge gaps and to adapt best practices and international guidelines to the election ecosystem in Pakistan;

2. **the ECP should investigate, adapt, and deploy next-generation election technologies** which give stakeholders rigorous guarantees of election security and transparency;

3. **the ECP should undertake extensive and systematic consultation efforts** with stakeholders to identify and resolve problems with new technologies, to address outstanding concerns, solicit feedback and draw on specialized resources, and to collectively achieve consensus and trust in the electoral process;

4. **the ECP should institute a dedicated Project Management Unit (PMU) and devise a comprehensive roadmap for implementation of E-Voting** to track and coordinate all of the above activities effectively and efficiently in the limited time available. The detailed roadmap with timelines is attached at **Annex-D**.

These recommendations are in strong agreement with best practices and guidelines issued by various international expert organizations and elections support networks. Moreover, various studies and expert reports over the last few years have recommended identical or very similar strategies directly to the ECP, but they have not yet been fully actioned upon.

Each of these recommendations requires considerable effort, initiative, planning, and resources, and we strongly urge all stakeholders to cooperate to the fullest in executing them. We believe these four steps are vital to the success of election technologies in Pakistan and, given our time constraints, must be actioned immediately. We would emphasize that **there are no shortcuts with election technology**. Countries that neglect due diligence tend to pay a heavy price in terms of failed elections, public embarrassment, wasted funds, political deadlock, protests, violence, and eroding confidence in democracy among citizens. In fact we at the ECP believe that if any quick solutions are adopted at this stage to

circumvent or bypass the roadmap it may trigger or offset problems in the future deployment of e-voting in Pakistan, the credibility of which will be difficult to re-establish later.

In the following sections, we discuss each step in more detail.

5.3.1 R&D Wing to address critical knowledge gaps

There are critical knowledge gaps in our discourse regarding EVMs and election technology in general. These include:

a) a lack of awareness regarding best practices and international guidelines in election technology;

b) a lack of exposure to new election technologies which radically improve security and transparency;

c) a lack of international standards in software and hardware development and project management;

d) a lack of specialized cybersecurity expertise;

- These shortcomings are evident in our discourse regarding EVMs, our previous experiences with election technology in 2018 (Internet voting[36] and the Result Transmissions System[37], and in the recent hacking attack on the systems of the Federal Bureau of Revenue[38]. These concerns have also been documented in various ECP reports and studies over the last several years, including the report of the ECP's EVM Committee in 2010[39] and the report of the Internet Voting Task Force (IVTF) in 2018[40].

- These reports also explicitly urge the ECP to invest in research and development to adapt election technology for Pakistan, following the successful examples of countries such as India, Brazil, Estonia, and the US. The report of the EVM Committee recommends formation of a dedicated Working Group for this purpose and states: "*Local high-tech universities and research institutions should be encouraged to conduct*

[36]Hina Binte Haq, Ronan McDermott, and SyedTahaAli: Pakistan's Internet Voting Experiment, https://www.e-vote-id.org/wp-content/uploads/2019/10/Pakistans-Internet-Voting-Experiment-Ronan-McDermott-d2.pdf

[37]Dawn: RTS controversy likely to haunt ECP, Nadra for a long time, https://www.dawn.com/news/1424394

[38] The Express tribune: Neglect caused FBR cyber-attack, https://tribune.com.pk/story/2316604/neglect-caused-fbr-cyber-attack?__cf_chl_managed_tk__=hPNLRdcX8lxEU65ExFf7mqzJC6qHI8q2Rez.LhJ9zFs-1641149370-0-gaNycGzNCtE

[39]Election Commission of Pakistan: Committee on the Use of Electronic Voting Machines in Pakistan Final Report and Recommendations, https://aceproject.org/ero-en/regions/asia/PK/pakistan-final-report-of-the-committee-on-the-use

[40]Election Commission of Pakistan: Findings and Assessment Report of Internet Voting Task Force ((IVTF) On Voting Rights 0f Overseas Pakistanis Executive Report 2018, https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf

R&D with a view to design domestically produced EVMs, meeting ECP's stringent requirements as per international standards in terms of technical and environmental specifications."

- The IVTF report also notes "*a critical shortage of cybersecurity skills and expertise in Pakistan, particularly within the field of election security"* and strongly recommends ECP launch a dedicated R&D cell to study election technology. The authors emphasize the need for this step: "*Due to this lack of dedicated technical expertise, we witness past mistakes being repeated and no tangible progress on the development of election systems in Pakistan."*

- The ECP has considered this step various times in the past, including setting up a dedicated Electoral Innovation Lab in partnership with UNDP and instituting research collaborations with universities. ECP has also emphasized a commitment to institutional development and strengthening research capacity in the last two Strategic Plans. However, these efforts have not been fully realized to date.

We urgently recommend the ECP follow through and institute a dedicated R&D Wing to study best practices and new technologies and to make informed policy decisions on EVMs. Developing indigenous expertise in election technologies at this point is vital. We can successfully adapt and customize technology as per our own unique ground realities, with significant cost savings, and reduce our overwhelming reliance on foreign expertise and resources.

This process will also enable transparency and improve credibility of elections. An IFES report notes: "*When technology is not well understood by both those who must administer the systems and the voters who will use the systems on election day then it is likely that real or perceived insecurities about the implementation and use of the systems will be apparent and may unnecessarily discredit the integrity of the elections.*"[41]

Moreover, indigenous design and development is a very feasible proposition: such innovation has been undertaken relatively successfully by neighboring countries, India and Bangladesh (still in experimental phase).

This R&D Wing should consist of a multi-disciplinary team comprising personnel with strong backgrounds in applied research, information security, election technology, applied statistics, computer networks, electronics, software and hardware development, etc.

The R&D Wing should have a twofold mission to assist the ECP and PMU in use of EVM:

1. Immediate Goals consisting of key open questions which need urgent resolution to deploy EVMs in Pakistan. For instance:

[41] Schmidt, Adam: Application of Election Technology: Considerations for Election Administrators, Practitioners and Policy Makers, https://www.ifes.org/sites/default/files/application_of_election_technology.pdf

i. define baseline security requirements for EVMs for Pakistan

ii. ascertain the viability of biometric verification units

iii. undertake extensive vulnerability and suitability analyses of available EVMs

iv. undertake extensive comparative studies of different EVM types

v. undertake rigorous cost-benefit analyses for the EVMs exercise

vi. address usability and accessibility concerns for differently-abled citizens

vii. formulate detailed technical specifications for EVMs to be deployed in Pakistan

viii. conduct and oversee rigorous pilot deployments

ix. conduct and oversee hackathons for EVMs

x. devise appropriate standards and certification processes

xi. define procedural safeguards and checks and balances for EVMs

xii. oversee the manufacturing processes and handling of EVMs and define appropriate checks

xiii. devise strategies to transmit, manage, and publish results from EVMs

xiv. devise effective incident response and cybersecurity strategies

We have scheduled many of these tasks in the Roadmap document accompanying this report.

2. Long-term Goals, consisting of essential high-level research. For instance:

i. inform key policy decisions regarding EVMs and guide the public discourse

ii. research and guide stakeholders regarding the ecosystem around EVMs

iii. investigate the application of technology to improve key components and processes in the elections ecosystem in terms of transparency, trust, and efficiency

iv. establish research linkages with universities, research organizations and other election management bodies

The R&D Wing could also commission specific research in partnership with universities and other technical organizations, such as Ministry of Science & Technology, NTC, NIE, NADRA, provincial IT boards, the HEC National Center of Cyber Security, etc. Donor bodies can be requested to support the operations of the R&D Wing with resources and technical expertise.

We believe this R&D Wing can have a transformative effect on the national discourse and policy regarding EVMs. With adequate staff and resources, we believe it can start producing actionable findings within 2-3 months with justification and research back up.

5.3.2 New Technologies and Processes for Transparency and Security

Risk Limiting Audits:

Post-election audits are statistical tests to root out anomalies before election results are made official. These anomalies could be undetected human error, intentional malfeasance, and/or voting system malfunctions that would undermine the integrity of the voting process. The aim is to build trust in EVM's that are otherwise thought to be black boxes. Thus, post-election audits are public ceremonies that the public, civil society, and media can attend and/or can be live streamed. This open inspection helps raise the voter perception of electoral integrity and increase stakeholder confidence on the outcome of elections.

There are primarily two types of post-election audits:

Hand-count audits: In conventional hand-count audits, election officials sample a percentage of the ballots, at random. They tally the ballots manually and compare the results to the reported results. Generally, they stop there.

Risk Limiting Audits: The current methods for risk-limiting audits, examine an increasing number of randomly selected ballots until the evidence is convincing that an uncensored manual tally would confirm the reported outcome.[42]

Risk-limiting audits are more time- and cost-efficient than hand-count audits. By the end of the audit, we have either a quantifiable level of confidence in election outcomes or detected discrepancies that can be corrected by way of a full hand count. Other possible benefits have also been claimed for risk limiting audits, including potential to reduce audit costs, increase voter confidence, deter fraud attempts and unnecessary recounts, and simplify other election processes. Election officials might be able to scale back some preventative voting system testing and certification processes, for example, if they have a way to identify and correct for vote counting issues after the fact.

Risk-limiting audits have been recommended as an election security measure by the Senate Select Committee on Intelligence[43] and the National Academies of Sciences[44], American

[42] IFES, Risk Limiting Audits, A Guide for Global Use

[43] *Brennan Center Quick Take: Senate Intelligence Committee's Election Security Recommendations*. Brennan Center for Justice. (2018). https://www.brennancenter.org/our-work/analysis-opinion/brennan-center-quick-take-senate-intelligence-committees-election.

[44] Nationalacademies.org. (2018). https://www.nationalacademies.org/news/2018/09/securing-the-vote-new-report.

Statistical Association[45], Brennan Center for Justice[46], among others. Electoral integrity and security experts are increasingly pushing to make risk-limiting audits (RLAs) a legal requirement for elections in all 50 states. In just the last few years, 11 US states have passed laws requiring, allowing, or piloting risk-limiting audits. Colorado was the first state to pass legislation about risk-limiting audits, in 2009; its first statewide RLA took place in 2017. It is estimated that by the next US election as many as half the US states will adopt risk limiting audits.[47]

On road to EVMs Risk Limiting Audits (RLAs) are to assume a significant role, if we are to move on the right path.

End-to-end Verifiability:

Strong evidence about the correctness of the outcome is fundamental to developing public trust in the integrity of a voting system. Conventional electronic voting machines are black boxes and lack the transparency that should be central to any voting system. E2EV voting systems are a promising new class of voting systems which offer voters the benefits of automation, including ease of vote-casting and quick reporting of results, along with stringent cryptographic guarantees of voter privacy and correct computation of the tally. Numerous such systems have been proposed over the years for precinct-based and Internet voting. Over the years these systems have been backed by National Academy of Sciences[48], international researchers, experts, and technologists[49]. It has been referred to as the holy grail of electronic voting[50].

These systems have been piloted in numerous small-scale mock elections and pilots. On a larger scale, they have been deployed in politically binding elections in the state of Victoria, Australia in 2016[51]. Estonia also deploys a E2E Verifiable Voting system for its nationwide parliamentary elections, the first deployment being held in 2019[52]. Recently, E2E Verifiable Voting has garnered immense interest by technology giants and various large scale commercialization efforts are underway. Among these is Microsoft's partnership with

[45] American Statistical Association Recommends Risk-Limiting Audits of Federal and Statewide Elections. (2010) https://www.amstat.org/asa/files/pdfs/POL-ASARecommendsRisk-LimitingAudits.pdf
[46] Brennan Centre, Risk Limiting Audits for Arizona (2021). https://www.brennancenter.org/our-work/research-reports/risk-limiting-audits-arizona
[47] National Conference on State Legislatures, Risk Limiting Audits (2021) https://www.ncsl.org/research/elections-and-campaigns/risk-limiting-audits.aspx
[48] Securing the Vote, National Academy of Sciences (2018) https://www.nap.edu/resource/25120/Securing%20the%20Vote%20ReportHighlights.pdf
[49] Evaluation of Department of Defense Voting Assistance Programs for Calendar Year 2020, https://media.defense.gov/2021/Mar/31/2002611446/-1/-1/1/DODIG-2021-066_REDACTED.PDF
[50] World's Most Hi-Tech Voting System Raises Cyber Defences https://e-estonia.com/worlds-most-hi-tech-voting-system-raises-cyber-defences/
[51] Inquiry into Electronic Voting, https://www.parliament.vic.gov.au/file_uploads/EMC_Inquiry_into_electronic_voting_HDMYyfRd.pdf
[52] Estonia's -Voting, more popular, more secure https://e-estonia.com/estonias-i-voting-more-popular-more-secure/

Smartmatic, a leading vendor for election technology. Hart InterCivic, Dominion, and others are also set to trial E2EV voting systems.

End-to-end verifiable election techniques enable individual voters to check crucial ingredients of election results – without requiring voters to trust election software, hardware, election officials, procedures, or even observers. Voters may check these processes themselves, place their trust in others of their choice (e.g., their preferred candidates, news media, and/or interest groups), or accept the outcome produced with the usual administrative safeguards.

Blockchain Technology

One of the biggest technology breakthroughs of the last decade is the blockchain. At its core is a distributed tamper-resistant ledger, that aggregates timestamped transactions and preserves them through cryptographic primitives. Blockchain offers characteristics such as decentralization, immutability, persistence, anonymity and auditability, consensus, traceability. It has found applications in remittances, micropayments, crowdfunding, proof of ownership for degrees, certificates, real estate and other assets, digital identity, copyright protection etc. When combined with election technology, blockchain can prove to be very powerful as a tamper- resistant and tamper -evident single source of ground truth, imparting radical transparency and legitimacy to the election activity and results.

Blockchain could be crucial in maintaining an accurate and tamper-proof voter rolls registry. Blockchain, as part of the voting system, will have EVMs record votes onto the blockchain as well as a VVPAT. This enables independent observers, political parties, media, and tech savvy citizens to track the cast votes in real-time as well as perform an audit and tabulate the results to ensure they match official results. Similarly, citizens can track their vote and be sure that it was not altered, discarded, or replaced after being cast and before being tabulated. Historically, threats to electoral integrity appear most often in the aggregation of vote totals at the regional level, not the individual polling stations. Blockchain may thwart this vulnerability, making it difficult for corrupt actors to modify the election results. Blockchain will also revolutionize the speed of result accumulation.

In 2018, Sierra Leone became the first country in the world to conduct blockchain based elections, offering instant access to the election results[53]. Moscow has had successful pilots of remote electronic voting assisted by blockchain in 2020[54]. On 20th October 2021, the

[53]Sierra Leone just ran the first blockchain based elections, Tech Crunch, (2018) https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/

[54]How Moscow organized voting on blockchain in 2020, ICT Moscow (2020) https://ict.moscow/en/news/how-moscow-organized-voting-on-blockchain-in-2020/

District of Khammam in Telangana, had a mock poll of the country's first ever remote and blockchain based e-voting exercise, with over 100,000 voters[55].

In 2020, Utah county held a blockchain based remote voting pilot, the first of its kind in the whole of the United States. With this development, some researchers also voiced their concerns about the possible vulnerabilities in a blockchain based system. Renowned MIT professor Ron Rivest, one of the names behind the public-key encryption scheme RSA, and his team also expressed their concerns over the use of blockchain technology in Elections: A key concern highlighted was that although the blockchain structure is inherently secure, but it will still be hosted on "*potentially vulnerable devices and network infrastructure*." Blockchain based systems also lack software independence[56], and thus an error and/or hack may go undetected. By design, blockchain systems are decentralized which can considerably increase the difficulty of effective management, governance, and coordination. Disseminating security fixes, updates may take longer, exposing the system to vulnerabilities for longer. This is potentially brand new technology and needs to be investigated at length for its perfection and imperfection.

5.3.3: Extensive Stakeholders Consultation and Consensus

There is considerable research from developing countries to suggest that active participation and consensus of stakeholders in formulating election technology policy is not only a highly effective strategy to prevent political deadlock, escalation, and electoral violence but it also results in more productive experiences with technology. Public, inclusive, and systematic consultation efforts which lead to the free exchange of ideas over a period of time can result in an open atmosphere of cooperation and foster greater trust in technology.

Currently, in Pakistan, there are considerable differences of opinion regarding EVMs and Internet voting across the political spectrum, election watchdog bodies and civil society. These differences are further amplified due to a pronounced lack of information regarding the complexities of election technology, particularly security concerns and requirements of the ecosystem. Moreover, we lack mechanisms, forums, and processes for stakeholders to engage on this topic in a systematic and constructive manner.

We believe that ECP, as the primary custodian of elections in Pakistan, should take the lead in democratizing this process by engaging stakeholders in extensive consultation efforts, to help streamline the national discourse and harmonize conflicting points of view. This should be part of strategy going forward as ECP's responsibility.

These efforts would have the following aims:

i. to introduce stakeholders to the advantages and challenges of election technology

[55]Dry run of blockchain based smartphone app in Telangana's Khammam https://qz.com/india/2070519/dry-run-of-blockchain-based-smartphone-voting-app-in-telanganas-khammam/

[56]Software independence is the assurance that an undetected change or error in a system's software cannot cause an undetectable change in the election outcome

ii. to inform stakeholders on ECP's stance and plans

iii. to promote dialogue, solicit critical feedback, and address reservations

iv. to invite stakeholder participation via position papers, working groups, etc.

v. engage in public outreach efforts

vi. arrange seminars, expert talks, and public demos on election technology

vii. strengthen linkages with stakeholders

These sessions should include political representatives, members from election watchdog bodies, activist groups, and civil society, and technologists, academics, and elections experts. Sessions should be conducted frequently, as per an official schedule, and structured to cater to different aspects of EVMs and Internet Voting. The ECP should maintain the minutes of these meetings and make them publicly available.

a. https://reliefweb.int/report/world/shared-security-shared-elections-best-practices-prevention-electoral-violence

b. https://www.tandfonline.com/doi/full/10.1080/13510347.2018.1470165

5.4 Execution and Timelines

The work to be done is considerable in the limited time available, but it is imperative that we do not cut corners or opt for shortcuts at this critical stage. ECP's foremost priority is to deliver trustworthy and credible elections.

Political mandates often result in rushed deployments of technology which quickly become problematic, result in wastage of funds, and may have considerable negative impact on citizens' trust in technology and government in the long run. This is evidenced in examples around the world: Kenya has suffered multiple and spectacular failures of technology with some of the most expensive and cutting edge deployments in the world. In the US, IFES notes that "[t]he rapid or premature introduction of technologies driven by HAVA mandates, in particular voting systems technology, has resulted in considerable levels of controversy" [https://www.ifes.org/sites/default/files/application_of_election_technology.pdf].

The Association of Computing Machinery (ACM) explains the reasons for this: *"many electronic voting systems have been evaluated by independent, generally-recognized experts and have been found to be poorly designed; developed using inferior software engineering processes; designed without (or with very limited) external audit capabilities; intended for operation without obvious protective measures; and deployed without rigorous, scientifically-designed testing."* We have witnessed this firsthand in our own prior experience with Internet voting and the Results Transmission System in the General Elections of 2018.

It is a tempting end piece to think of EVMs as simple machines which can be purchased, stored and deployed once every five years, but the reality is that technology is a long-term and constant engagement, which requires fundamental adjustments, or 'growing pains' on the part of stakeholders and citizens. The literature on best practices strongly cautions against rushed deployment and makes compelling arguments for a piecemeal process which scales up organically from multiple small pilots to larger scale elections. This process identifies problematic issues with machines at an early stage, it addresses technical and legal challenges at early stages and allows for mitigation measures and changes to EVM design and processes, it gives stakeholders space to adjust to technology, and most importantly, it engenders trust and confidence in the system.

However, we are mindful of the urgent timelines at hand. To resolve this Gordian knot, we recommend that ECP institute and support a dedicated Project Management Unit (PMU) to oversee this entire enterprise and make best possible use of the limited time available. This PMU should streamline and coordinate the multiple disparate tasks required, parallelize operations where needed, and ensure course correction in case of unforeseen circumstances and delays. The PMU should also oversee the transformation of the ECP and modernization of critical processes. As a way forward, ECP hired the services of I.T professionals in Project Management Unit. In this regard, the Hon'ble Chief Election Commissioner of Pakistan has written a letter to the Hon'ble Prime Minister of Islamic Republic of Pakistan for provision of space to establish PMU and other information technology / technical facilities which will hopefully be honoured.

RECOMMENDATIONS

We believe it is possible to attain the benefits of EVMs and to minimize the disadvantages by adhering to international guidelines and best practices and navigating this domain carefully. Our research indicates that EVMs are a viable and cost-effective option in the long run to improve Pakistan's polling processes and improve trust and credibility in our elections. Popular EVM types can be customized to cater to our own ground realities and augmented with new technologies which alleviate stakeholder concerns about security and render the elections process more transparent to the public.

We estimate it will take 8-10 months to define detailed technical specifications for EVMs, 14-16 months to start large-scale pilot testing, and aim to initiate large-scale procurement after 20-24 months. However, this is a very optimistic estimate: we should expect considerable delays due to administrative processes, setbacks from the current pandemic situation, and severe ongoing disruptions in global supply chains. Moreover, this timeframe does not account for the challenges of building the ecosystem, an extensive exercise. It is simply not possible to conclude these activities by 2023 without exposing our elections to grave and reckless risks.

The twenty-nine recommendations that follow identifying critical knowledge gaps and problems in our discourse on EVMs. In each case, we specify remedial steps with concrete and tangible outputs, in the form of studies, specifications, pilots, demos, and consultations. Our goal is not just to detail the way forward to the best of our ability, but also to give stakeholders a sense of the immense scope, depth, and complexity of this project.

Key tasks to be undertaken are listed in the attached Roadmap document. Several of these listed tasks are independent of each other and may be undertaken in parallel[57]. A Gantt chart is also enclosed [**Annex-C**] which guides through various steps.

The Road to EVMs

1. **We recommend ECP develop and implement a comprehensive plan to prepare for cybersecurity threats on election systems and to develop Critical Digital Infrastructure (Assets) for the establishment of standardized ecosystem framework to support E-Voting (EVM and Online Voting) operations.** There is growing recognition that election infrastructure, including election systems, databases and organizations are key targets for attacks by malicious actors[58,59]. Recently, the United States designated their election databases and systems as critical infrastructure, in the same category as dams and nuclear reactors. Our own election

[57] This depends on the availability of personnel and expertise as well as the resources including finances and facilities available.
[58] Cybersecurity for Elections, A Commonwealth guide for best practices, https://thecommonwealth.org/sites/default/files/inline/Cybersecurity_for_Elections_PDF_0.pdf
[59] International Publics brace for cyberattacks on elections infrastructure, national security https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/

systems have suffered cyberattacks in the past[60]. Development of ecosystem framework to attain the capabilities and sustainability for the successful implementation of EVM and voting for Overseas Pakistanis and also for the independence of the governing election management body.

In March 2013, former CIA contractor Edward Snowden revealed that Pakistan was among the countries most targeted for surveillance by the U.S. National Security Agency (NSA). In June 2017, Pakistan's Senate Committee on Foreign Affairs also warned the government that Pakistan was a principal target of cyberespionage. With the recent devastating cyber-attack on the systems of the Federal Bureau of Revenue and National Bank of Pakistan, there are now increased calls within the country to devote more resources for securing computer systems, investing in the security of the country's digital infrastructure, and strengthening cybersecurity research and development. This necessitates that in Pakistan all such organizations including ECP fully devote energies to this critical aspect.

In order to safeguard the election infrastructure (Data Center, Servers, Certification Labs, Telecom) from non-state actors, hackers and cyber-attacks, this digital asset should be declared as critical and the government should include election digital infrastructure in its recently promulgated National Security Policy.

The Commonwealth Cyber Security Guidelines of Best Practices be strictly followed for strengthening the use of Information Communication Technology (ICT) for elections.

2. **We recommend ECP undertake extensive cross-sectional consultation measures with stakeholders** including political representatives, civil society, activists, and technologists, and seek their inputs at every stage of the deployment process. There is considerable polarization in the current discourse around EVMs and we lack mechanisms and forums for stakeholders to engage constructively on this topic. ECP, as the only custodian of elections in Pakistan, should guide, inform, and democratize the debate on EVMs. This can be achieved by setting up active working groups and organizing outreach efforts, such as public calls for comments and organizing seminars, invited talks, demos, and hackathons. The facilitation of Civil Society and development partners, which has established platforms can be used for this.

   ECP should also actively engage with stakeholder concerns, particularly on the issue of security. The ECP's mandate, as per the law, is to procure and deploy EVMs "*in prescribed manner, subject to secrecy and security*"[61]. As a corollary to this, it is vital that ECP convincingly demonstrate the security properties of EVMs to stakeholders and allay their concerns. Reducing concerns on security will give tremendous boost to the whole process and give it a head start for public and political parties buy-in.

[60] Report on I-Voting Pilot, https://ecp.gov.pk/documents/ivotingreport.pdf

[61] Elections Amendment Act 2021, https://senate.gov.pk/uploads/documents/1623649621_687.pdf

This is particularly important considering the trust-deficit, which is common in developing countries like Pakistan, and is fundamental to ensuring credible elections. Research studies and expert reports indicate that dialogue and consensus-building measures during the election technology research and deployment phase considerably benefit the electoral process. Such measures harmonize conduct of the elections, reduce post-poll tensions and violence, and contribute to the overall credibility of the polls[62,63]. We repeat here the words of US civil rights icon, Bayard Rustin (quoted by an elections observer body), "*If we desire a society that is democratic, then democracy must become a means as well as an end.*"[64]

To make the EVM acceptable to the stakeholders, it must satisfy the following technological parameters:

a. The machine is dependable, and the results of dependability testing are available for the public.
b. In case of damage or physical theft of the EVM, alternate measures have been suggested /provided.
c. The working of the EVM is simple and understandable to common people.
d. Enough training on the system has been (will be) provided to the polling staff and the voters.
e. The software has not been programmed to malfunction and is free from intentional errors.
f. The stakeholders have trust in the software.
g. The paper trail is verifiable through the electronic record.
h. The EVM has been tested at college union, local government elections, and bye-elections, successfully.
i. The problems faced in gradual deployment have been resolved
j. Resources to manufacture EVMs are available as done in countries which are serious in their development.
k. Training to some 30,000 technicians has been provided.
l. The polling staff is trained to run the system without any considerable problem.
m. The EVM can be used for the e-voting at a larger scale when the questions raised above have been addressed and the challenges identified, have been answered. However, pilots of the EVM at small (gradual) scale are always possible which will help in forming the gradual trust of the stakeholders.

[62] Cheeseman, N., Lynch, G., & Willis, J. (2018). Digital dilemmas: The unintended consequences of election technology. Democratization, 25(8), 1397-1418.
[63] Shared Security, Shared Elections, https://www.afsc.org/story/quaker-group-releases-study-election-violence
[64] Making real the promises of democracy, https://www.afsc.org/newsroom/making-real-promises-democracy

3. **We recommend ECP adopt best practices and international guidelines and strive towards a culture of excellence.** It is a well-documented fact that most failures of election technology can be traced back to a lack of best practices and a markedly poor understanding of security principles. A well-known report from the Association of Computing Machinery (ACM) elaborates: "*many electronic voting systems have been evaluated by independent, generally-recognized experts and have been found to be poorly designed; developed using inferior software engineering processes; designed without (or with very limited) external audit capabilities; intended for operation without obvious protective measures; and deployed without rigorous, scientifically-designed testing.*"[65]

   We have witnessed this firsthand in Pakistan: these findings echo our own prior experience with the failure of the iVOTE[66,67] and the Results Transmission System[68] in 2018. We are now aiming for one of the largest EVM deployments in the world and for a project of this magnitude, it is critical that ECP commit to international best practices in deploying election technology and spare no effort or expense to develop a culture of excellence, that is sustainable through continued R&D.

4. **We recommend that ECP urgently institute a Research and Development (R&D) Wing.** The immediate goals of this body are to identify security requirements for EVMs, oversee pilots, define EVM specifications, undertake mission-critical research and organize Market Need Analysis through reputed firm. Long-term goals include adapting best practices and international guidelines to ground realities in Pakistan, to have informed policy and discourse on election technology and define appropriate standards, research the ecosystem that is needed to support EVMs, and liaise with other research-intensive organizations and stakeholders. This body should be staffed with researchers and technologists and, if possible, supported by an advisory board of experts. This critical institutional support is being practiced by the leading practitioners, Brazil and India.

   Multiple reports over the past decade have strongly recommended that ECP develop this in-house expertise and capacity to guide them on the way forward[69,70,71,72] but this vision has yet to be realized. The Internet Voting Task Force from 2018 report

[65] US Public Policy Committee Association for Computing Machinery; Recommendations on Electronic Voting Systems, 2004, https://cacm.acm.org/magazines/2004/10/6402-acm-statement-on-voting-systems/fulltext
[66] Consultancy for the analysis, design, and implementation of Internet voting for overseas Pakistanis, https://www.ecp.gov.pk/documents/reports/Final%20report%20by%20Minsait%20Final.pdf
[67] IVTF Report 2018, https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf
[68] Result Transmission System, https://www.ecp.gov.pk/frmGenericPage.aspx?PageID=3083
[69] IVTF Report 2018, https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf
[70] Committee on the Use of Electronic Voting Machines in Pakistan, Final Report and Recommendations, 2010, https://aceproject.org/ero-en/regions/asia/PK/pakistan-final-report-of-the-committee-on-the-use
[71] ECP Second Five Year Strategic Plan, 2014-2018, https://www.ecp.gov.pk/Documents/sp%20revised/Strategic%20Plan%20Revised%20final.pdf
[72] ECP Third Strategic Plan, 2019-2023, https://www.ecp.gov.pk/ECP%203rd%20Strategic%20Plan%20copy%20for%20Website.pdf

notes "*a critical shortage of cybersecurity skills and expertise in Pakistan, particularly within the field of election security*" and that "*due to this lack of dedicated technical expertise, we witness past mistakes being repeated and no tangible progress on the development of election systems in Pakistan.*"[73] This shortcoming restricts the range of choices available to the ECP, and fundamentally impairs its ability to deploy technology effectively.

We believe this R&D Wing is central to this entire technology exercise and will have a transformative effect on the national discourse and policy. If this body is allotted the necessary staff and resources, we believe it can start producing actionable findings within 2 months.

5. **We recommend ECP define baseline security requirements for EVMs**. This study, also referred to as a threat model, should precisely define the security issues and vulnerabilities on the ground that we expect to address using EVMs. This exercise is to be undertaken in active consultation with stakeholders, researchers, and election observer bodies. Key security agencies can be kept in picture in this exercise.

6. **We recommend ECP undertake a detailed comparative analysis of the suitability of popular EVM types for use in Pakistan**. This includes push-button EVMs (used in India and Bangladesh), EVMs with keypad inputs (used in Brazil), optical scanning machines (used in Iraq), etc. These machines offer significantly different features: for instance, push-button EVMs are very low-cost, keypad-input machines can accommodate very large numbers of candidates on single machines, and optical scanning machines maintain the privacy of the voting paper trail. Different models also have vastly different storage and handling requirements. These features need to be examined in light of ground realities in Pakistan by the PMU.

7. **We recommend that ECP procure multiple units of each EVM type and pilot them** (in small scale polls or non-political elections, such as bar councils, trade bodies, etc.). This will be an extensive exercise examining a range of factors, including security, usability, costs, logistics, storage and handling requirements. Use both DRE and Optical scanner in small pilots and give report to the Parliament before selecting final technology.

   To the best of our knowledge this exercise has not yet been undertaken. ECP's previous EVM pilots only examined one particular EVM type (push-button EVMs). It is important that we investigate the complete range of options available to us, including new innovations. Our electorate is not uniform, our society is also stratified along various socio-cultural and economic divides and technical literacy is abysmal. It is important that we attempt to determine, to the best of our ability, the 'people's

[73] IVTF Report 2018, https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf

choice', i.e. which EVM type and interface our citizens find easiest to use and is most conducive to enabling them to exercise their voting rights.

8. **We recommend ECP urgently investigate and integrate new security features into EVMs**. EVMs equipped with VVPATs (as used in India, Bangladesh, and parts of the United States) are no longer considered the gold standard for election security. Many recent expert reports propose use of new techniques, such as risk-limiting audits (RLAs) and end-to-end verifiable voting solutions. These solutions give citizens unprecedented transparency into election processes and have the potential to be a game changer in improving confidence in election results.[74,75,76,77]

9. **We recommend ECP prototype these technologies**, introduce them to stakeholders, and pilot them to assess their use in Pakistan. Its better and ideal to pilot both technologies together in different bye elections at small scale using DRE and optical scanner both.

10. **We recommend ECP research and devise voter verification strategies**. Our investigation indicates that biometric verification machines (BVMs) may not be a feasible option for Pakistan. For one, the NADRA record currently lacks biometrics for approximately 4.3 million citizens which effectively disenfranchises them. ECP's earlier pilot of BVMs (in NA-19, Haripur, in2015) also noted a significant failure rate of 54%[78]. This was due to scanning issues, environmental or lighting conditions, and poor quality of fingerprints due to injuries, or calluses due to intensive manual labor. These are widely recognized to be inherent limitations of biometric technology[79] and have been observed in other countries too[80].

11. **We recommend ECP investigate and trial alternate biometric authentication mechanisms,** including multi-finger authentication, facial recognition, and smart cards in consultations with NADRA and stakeholders. It totally depends on the capacity and capability of NADRA's digital biometrics data quality and its efficacy because use of technology on large magnitude will always be challenging for any EMB as quality of biometrics data varies which resultantly gives more risks in the system.

---

[74] Securing the Vote – Protecting American Democracy, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

[75] Citizens' Commission on Elections' Report on EVMs and VVPAT, https://www.cse.iitd.ac.in/~suban/reports/CCEpaper.pdf

[76] IVTF Report 2018, https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf

[77] World's Most Hi-Tech Voting System Raises Cyber Defences https://e-estonia.com/worlds-most-hi-tech-voting-system-raises-cyber-defences/

[78] Biometric gizmos fail to verify 54% of voters https://tribune.com.pk/story/944232/test-run-biometric-gizmos-fail-to-verify-54-per-cent-of-voters

[79] IDEA - Introducing Biometric Technology in Elections, https://www.idea.int/publications/catalogue/introducing-biometric-technology-elections

[80] Introducing Biometric Technology in Elections, https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf

12. **We recommend ECP incorporate accessibility options in the EVM design** like Braille or audio aids for differently-abled voters. If this is not possible, ECP should devise appropriate alternate voting protocols to compensate, whilst ensuring voters' ballot secrecy and security. Once these studies conclude, ECP will be in a position to identify the precise EVM type and features, which should then be prototyped and deployed in large-scale pilot testing.

13. **We recommend ECP develop a comprehensive plan for large-scale pilot testing**. ECP will need to undertake multiple large-scale pilots in a mix of urban and rural areas to ensure a representative cross-section of the electorate is covered. During these pilots, the machine can be further assessed with feedback and modified accordingly. For this purpose, ECP can seek assistance from universities and research organizations. ECP may commence large scale procurement and nation-wide deployment after a sufficient number of successful pilots.

14. **We recommend ECP strive towards developing indigenous expertise and local manufacturing of EVMs.** This has several advantages: first and foremost, it has become clear in recent years that the election technology supply chain is also a key security concern[81]. Critical EVM hardware and software components should ideally be prepared within Pakistan. Local production will give ECP and stakeholders greater oversight and control over the process over time.

    Second, from a sustainability perspective, local production will result in dramatically lower costs for EVMs, which is a key determining factor in the economic viability of this entire enterprise. This project will likely cost hundreds of billions of rupees over the years, and investing such a large amount in local industry, capacity building, and talent is to be considered a welcome step which would stimulate the national economy. In the first go, systems set up in Brazil can be studied.

    Third, in the long run, building local capacity would significantly reduce our reliance on foreign inputs, funding and expertise. Indeed, if our EVM experience is successful, we anticipate this will create new export opportunities for us, like how US and Indian EVMs have carved out a market in other countries.

    Moreover, a large-scale EVM deployment is not a one-off transaction but represents a very close and long-term engagement with the vendor which can last decades, and it would be advisable to prioritize local vendors, subject to local laws and regulations. There have been instances in the international experience where election

[81] Election Technology Cyber Security Supply Chain Guide, https://www.cisecurity.org/press-release/center-for-internet-security-cis-releases-new-elections-technology-cybersecurity-supply-chain-guide/

management bodies (EMBs) have clashed with foreign vendors[82,83] resulting in undesirable complications and litigations.

We should not be intimidated by the scale and complexity of this task. Countries much like our own, including Brazil, India, and Bangladesh, have successfully innovated EVMs as per their own needs within their own limited resources.

Ecosystem, Logistics, and Infrastructure

Deploying EVMs necessitates building a comprehensive supporting infrastructure from scratch. No aspect can be seen in isolation rather linked in an integrated way.

15. **We recommend that ECP institute a dedicated Project Management Unit (PMU) to oversee this entire enterprise.** This PMU should streamline and coordinate the multiple disparate tasks required, parallelize operations where needed, and ensure course correction in case of unforeseen circumstances and delays. Apart from the process of procuring and deploying EVMs, the PMU should also oversee the transformation of the ECP and modernization of critical processes. The PMU should also issue quarterly reports to apprise stakeholders of ECP's progress on this project. It should contain basic expertise of the required elements.

16. **We recommend ECP develop comprehensive storage and transport facilities and protocols for EVMs.** This is a massive exercise. It is likely that EVMs will require multiple large storage sites or warehouses subject to various criteria on a provincial or regional basis. These sites will also require special facilities, e.g., environmental controls, and state-of-the-art security and remote monitoring solutions. Moreover, EVMs will also likely require fleets of customized trucks or large vehicles to transport EVMs between storage sites and polling booths on election day.

    For this purpose, ECP should develop detailed standards and SOPs to store and transport EVMs, as devised in countries like India and Brazil. About 30 warehouses for storage of all EMVs will be required at divisional level at least and guarded security, anti-dust, anti-insect, water and heat proof environment is required with CCTV and biometrics access control systems. In some countries like Brazil where centralized storage is undertaken, huge costs are incurred in sophisticated delivery of EVMs.

17. **We recommend ECP develop comprehensive handling and maintenance standards and protocols for EVMs.** Instances of manhandling or mishaps regarding

[82] Duterte to Comelec: Smartmatic no longer acceptable, https://www.philstar.com/headlines/2019/05/30/1922385/duterte-comelec-smartmatic-no-longer-acceptable

[83] Loeber, L. (2020). Use of Technology in the Election Process: Who Governs?.*Election Law Journal: Rules, Politics, and Policy*, *19*(2), 149-161.

EVMs tend to adopt scandalous proportions and can raise question marks about election credibility. In Congo, a suspicious fire broke out in an EVM's storage facility and destroyed thousands of machines[84]. A recent news report from India indicates that almost 2 million EVMs may be unaccounted for in inventory[85], a staggering amount, almost 3-4 times the number of EVMs Pakistan would need in its own general elections. This is yet another lesson learnt from international best practices which ignored, can have highly negative repercussions. It is vital that ECP devise stringent protocols for accessing, handling, and maintenance of EVMs that can be rigorously monitored and policed.

Supporting Technologies and Related Concerns

18. **We recommend ECP develop a comprehensive strategy for supporting technologies, particularly for result transmission.** Procedures must be devised to transfer the results from the EVMs in a safe, secure and timely manner. As per expert guidelines, the result transmission technology should be rigorously stress tested and be piloted alongside EVMs multiple times to identify potential integration issues[86].

19. **We recommend ECP develop sustainability strategies for EVMs and supporting technologies.** As a developing country, it is vital that we seek out cost-effective options and utilize our resources effectively. For example, we should consider emphasizing the use of open-source software tools in our systems as much as possible. We should also try to 'future-proof' our EVMs, such that they have a lifetime of at least 2 to 3 electoral cycles. This can be done by identifying and using EVM components that are easy and cost-effective to maintain and to replace. We should attempt, to the best of our ability, that our EVMs are built to accommodate anticipated future technologies, such as smart-cards, iris verification and facial recognition technology.

ECP Preparedness for EVMs

20. **We recommend ECP devise a comprehensive digital transformation strategy.** For successful deployment it is not enough to merely acquire technology, it is important to build synergy between people, processes and technology as well as refactor the election paradigm. It is necessary for the EMB to articulate a vision and lay down a roadmap for the bottom-up digital transformation. According to Deloitte, a lack of strategy is the biggest impediment to early-stage organizations taking full advantage of digital trends. *"Only 46% of public-sector agencies have a clear and coherent digital strategy."*[87] In a similar vein, the 2020 UN E-Government Survey

[84] DR Congo, why do voters mistrust electronic voting? https://www.bbc.com/news/world-africa-46555444
[85] Whereabouts of 19 Lakh EVMs Not Known, Reveals RTI-Based Court Case, https://thewire.in/government/evm-missing-rti-court-case-frontline
[86] Challenges and Opportunities for the implementation of e-voting in Nigeria https://www.eces.eu/template/default/documents/E-Voting%20in%20Nigeria%20-%20ECES.pdf
[87] Digital transformation and the future of voting, https://elections.smartmatic.com/digital-transformation-and-the-future-of-voting/

revealed that *"the most advanced levels of e-government development have assigned priority to developing capacities and mindsets that fully support an integrated, whole-of-government approach to digital government transformation."*[88]

One such success story in Estonia: in early 1990s there were practically no computers in this former impoverished Soviet Union member state. However, today it is one of the top 5 in the UN E-Government Survey rankings. Apart from its much-touted Internet Voting system, in Estonia, 99 percent of public services are available online 24 hours a day. As a country, Estonia saves over 1400 years' worth of effort annually. Estonia's Internet Voting system is also fully integrated into a larger overall framework of digital governance.

21. **ECP should modernize its systems and urgently work towards implementing international security information standards** like ISO/IEC 27000 to secure critical digital assets and infrastructure. ECP should also undertake periodic and comprehensive risk assessment audits as recommended in expert reports[89]. This exercise can take up to a year or more for large organizations. For this purpose, ECP may seek active assistance from national cybersecurity agencies and specialist bodies, as has been done in other countries.[90,91]

22. **We recommend ECP conduct research and identify key factors against which to assess their preparedness to introduce and operate EVMs.** Such standards have been proposed for advanced countries (such as the E-Voting Readiness Index[92] which considers various aspects, including social, legal, and political dimensions) and these contain several valuable insights. However, yet no such rigorous study has been undertaken for developing countries with vastly different ground realities. This exercise may be done in partnership with stakeholders and universities.

23. **We recommend ECP develop comprehensive standards and testing and certification protocols for EVMs**. These processes must be designed with a view to giving stakeholders greater transparency into the state of the machines. Many regions define their own technical standards in consultation with experts and stakeholders,

[88] UN E-government survey, 2020, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

[89] Cybersecurity for Elections, A Commonwealth guide for best practices, https://thecommonwealth.org/sites/default/files/inline/Cybersecurity_for_Elections_PDF_0.pdf

[90] US National Guard, https://https://www.nationalguard.com/

[91] Computer emergency Response Team, Ghana, https://www.csa.gov.gh/cert-gh.php

[92] Krimmer, R., & Schuster, R. (2008). The e-voting readiness index. In *Electronic Voting 2008 (EVOTE08). 3rd International Conference on Electronic Voting 2008, Co-organized by Council of Europe, GesellschaftfürInformatik and EVoting. CC*. GesellschaftfürInformatik e. V.

against which EVMs are then assessed. Countries such as India and Brazil arrange public ceremonies where citizens can watch EVMs be tested prior to election day.[93,94]

24. **We recommend ECP organize hackathons for EVMs and solicit feedback from the international election technology community.** This step will help identify any further vulnerabilities and issues in EVMs and supporting practices and will give stakeholders greater confidence in the machines. This may be accomplished in partnership with universities. The EVM may even be showcased in international forums, such as the DEFCON Voting Village, the world's premier election technology security event[95].

25. **We recommend ECP engage third party technical experts and consultants at periodic intervals to analyze the EVMs and the supporting technologies and infrastructure.** The threat landscape is constantly evolving, and election systems should be subject to periodic auditing and improvement. These external experts with credibility should verify the security properties of the systems, study the adequacy of supporting processes, analyze for new threats, if any, and give critical feedback which can be incorporated by ECP.

26. **We recommend ECP build active linkages with other Election Management Bodies (EMBs) and research-intensive organizations**. This step will assist with addressing knowledge gaps and with technology transfer. The ECP should also engage with universities and issue grants and commission research studies to address local issues related to elections and technology. Such linkages have proved highly fruitful in countries like the United States, Brazil, India, Bangladesh, Estonia, and Australia and can be modelled after those examples.

Supporting Legislation and Processes

27. Issues with existing legislation

The law should also provide for conducting pilots for Risk Limiting Audits and End-to-end Verifiable Voting in politically binding elections.

The Federal Government on 2nd December, 2021 introduced a basic amendment (**Annex-B**). Usually, the technology is finalized on the basis of generic legal provisions in the law with its features. Since, existing law is vague and does not define the detailed procedures and processes. Therefore, the adoption of technology is not focused to any particular type or kind of machine. It is recommended that features of the machine or e-voting system should be defined in the law prior to introduction and selection of any particular type of technology or EVM.

[93] Brazil voting Machines are tested for safety ahead of 2022 elections, https://agenciabrasil.ebc.com.br/en/justica/noticia/2021-11/brazil-voting-machines-are-tested-safety-ahead-2022-elections

[94] How electronic voting machines have improved India's democracy https://www.brookings.edu/blog/techtank/2019/12/06/how-electronic-voting-machines-have-improved-indias-democracy/

[95] Defcon, Hacking Conference, https://defcon.org/

EVM also requires multiple pilots, R&D in terms of verifiable voting system in it and real-time tests to qualify legal obligations of maintaining standards of Secrecy and Security which takes lucrative time as per world best practices and International standards.

28. **Legislation to support EVMs - modality of elections, staggered or same-day,** voting laws should not be so specific that they hinder innovation, nor should they be so generic that they leave room for lingering litigation. There should be a law related to the protection of electoral data, and its derivatives. Legislation should also stipulate severe penalties for cybercrimes related to elections.

    The National Assembly has already expedited the passage of laws to allow e-voting. There should be laws that mandate the pre-audit and post-audit of EVMs and supporting equipment.

29. **We recommend ECP urgently conduct research and develop appropriate dispute-resolution mechanisms and strategies to cater to EVMs.** A new large-scale technology intervention like EVMs carries multiple uncertainties, which can cause tensions in case of mishaps or failure and adequate dispute resolution mechanisms can help prevent such escalation. Dispute resolution was a critical failure in the 2013 polls, which resulted in large-scale protests and extended political deadlock. ECP can gain valuable insights for this purpose from experiences of countries like India and Brazil.

30. **We recommend following EVM plan for year 2023:**

i) ECP will try its level best to meet the target of General Elections-2023 subject to overcoming following challenges:

   a. **Establishing critical infrastructure for the eco-system of EVM (manual to digital transformation processes, trained technical and operational human resource, certified data centre, testing & certification labs, secure communication, implementing and assuring infrastructure security i.e. ISO Certifications etc.)**
   b. **Establishment of warehouses/storage sites at provincial/division/ district level.**
   c. **Reliable mass production & supply-chain in Covid-19 situation.**

   In the best-case scenario, if ECP overcome those challenges and work on EVM progresses well, then it may be possible to pilot EVM in selected regions in elections in 2023.

ii) Based on our current findings, it is reasonable to assume that we can conduct the next general elections of 2028 with a standalone EVM deployment.

iii) **However, even with a deadline of 2028, it is imperative that ECP commence work on this project immediately in all earnestness and try to beat all odds, to the extent possible.**

iv) **If ECP is unable to conduct General Elections-2023 through EVM, we recommend that keeping in view the requirements, forthcoming General Elections of 2023 be conducted with age-old paper ballot and in parallel EVM based pilots in key districts both urban and rural covering 5% of constituencies.**

v) **Mobilization of EVM resources shall require substantial budget, and to begin with, initially Rs. 70 to 80 Billion will be required to start different processes relating to EVM.**

CONCLUSION

We are confident that if this project is undertaken in a structured and systematic manner, with necessary due diligence, it will result in a landmark achievement towards ensuring credible and trustworthy elections in Pakistan.

The international experience demonstrates that success stories in EVM deployment, such as India and Brazil, adhere to a common formula. These nations have developed and introduced EVMs in a careful systematic manner, taking careful heed of ground realities and international best practices, democratizing the process and engaging stakeholders in active consultation, and encouraging evolution in the system design and features. Moreover, EVM deployment is an immense investment and indigenous development and production of machines tend to be far more cost effective and beneficial than importing expensive technology from abroad. This entire process can span years but provides a robust foundation for responsible use of technology and credible elections.

This report is also accompanied by an activity plan detailing essential activities, key milestones and deliverables for procuring EVMs over an 18-months period.

OVERSEAS VOTING

Countries that allow external voting need to ensure that it is conducted in such a way as to meet the requirements of security, transparency and secrecy. It is also desirable that as far as possible all electors have the same opportunity to vote. However, countries and territories also need to make adjustments and innovations to cope with the challenges that are particular to external voting, such as the geographical location of voters, security in transporting ballot papers, the high costs of external voting and other administrative issues. Every voting procedure when applied abroad has implications in terms of the coverage of potential voters and their opportunity to cast a vote.

There are four major voting methods for external/ out-of-country/ overseas voting in the world as following:

1) Postal voting;
2) In-Person voting (Paper ballot or EVM in embassy or other designated places);
3) Voting by proxy; and
4) E-voting (Internet Voting or Online).

1. Postal voting

In postal voting, ballots are mailed out to out-of-country registered voters in time for them to be completed and returned by mail for counting. Through this facility, a voter can cast his/her vote remotely by recording his/her preference on the ballot paper and sending it back to the Returning Officer before counting.

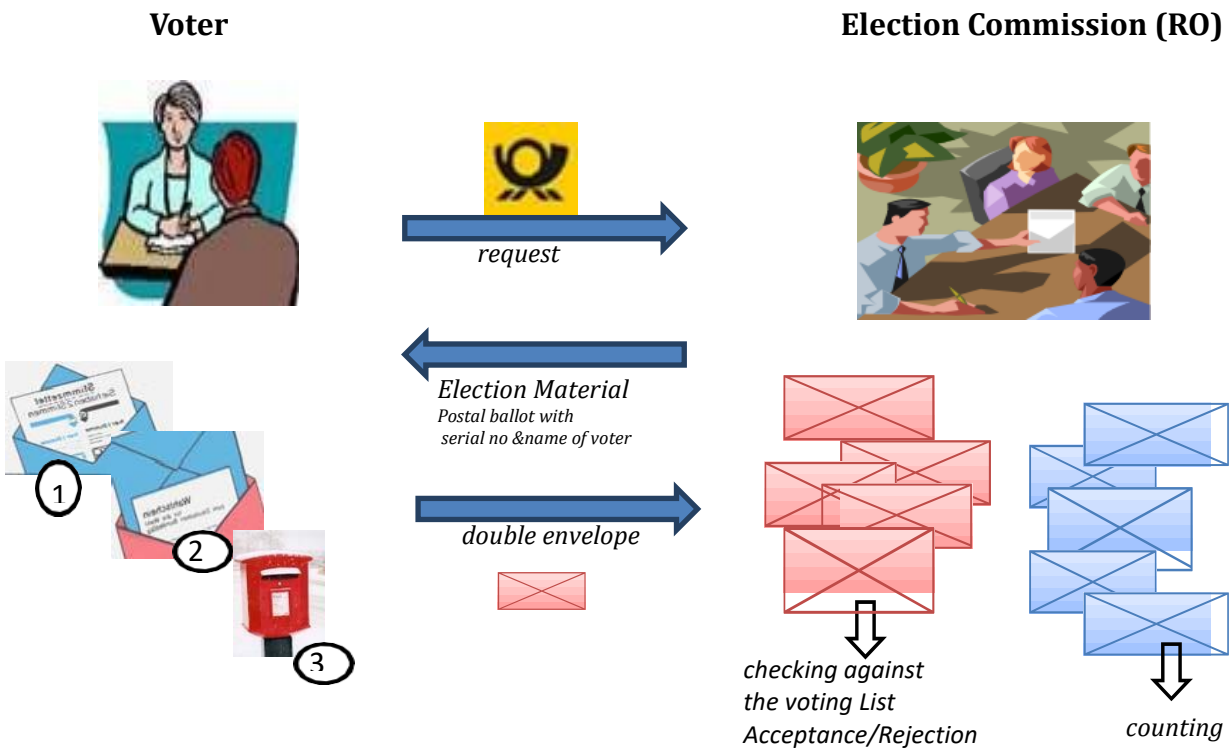


Figure: The overseas postal voting process

Advantages of Postal Voting:

i. It is a convenient option to use. You can avoid going to an in-person location to cast a ballot. You don't need to worry about standing in a long line of people during a working day so that you can vote. You can open the ballot at home, write/mark it on your own time, and then return it by mail (sometimes with postage paid) before the election deadline.

ii. It increases participation rates.

iii. Vote by mail reduces the political influences that can impact votes.

Disadvantages of Postal Voting:

i. Voters have different deadlines that they must meet with this option.
ii. Some ballots run the risk of getting lost.
iii. Security is a significant concern for postal voting.
iv. Postal voting encounters more accuracy errors.
v. Voters have less confidence in the accuracy of vote by mail (postal) systems.
vi. More chances for manipulation and other people may influence.
vii. Voting is done from remote areas, therefore, unsupervised and uncontrolled environment.

Issues and Challenges of Postal Voting:

i. An opening for Fraud of wholesale proportions
ii. Intimidation, coercion, family /group voting and impersonation may become easily.
iii. Voters might be excluded from their right to vote in case their votes arrive too late
iv. Election results may be delayed for several days that is not welcomed by the parties or candidates
v. Countries like UAE where there is no postal system.

2. <u>In-person Voting:</u>

In-person Voting requires a personal appearance by the voter at a designated polling place, established by the country of which the overseas voter is a citizen. The polling place is often in an embassy or consulate or any other government facility, more rarely in borrowed or rented halls.

Advantages of In-Person Voting:

i. The true identity of the voter can be established or verified by providing proof of identity (and of being registered to vote) and there is an assurance that the ballot was actually cast by the voter him/herself.

ii. With in-person voting, officials ensure that the voter can cast his/her vote without being affected, coerced, or observed; thus, a free, transparent and secret election is ensured.

iii. Voting being carried out under supervised, controlled and managed environment.

Disadvantages of In-Person Voting:

i. The overseas polling stations may not be accessible to many voters during the day or days allowed for overseas voting due to economic constraints, physical disability or other reasons.

ii. Voting in-person from abroad may be difficult to observe at all stages.

iii. The in-person voting is done in a controlled environment (such as embassies or consular offices), observation may be possible but will be expensive.

iv. Difficult to manage voting in large countries like USA, Canada, Saudi Arabia, Australia, etc. where distances are too long for Pakistanis living in far flung areas of that country to travel to Embassy or consulate.

Issues and Challenges of In-Person Voting:

i. In –Person Voting depends entirely on host country approvals

ii. Host Governments can be reluctant in allowing large scale elections of another country in its territory

iii. Limitations of Diplomatic Missions – may not have the capacity to deal with large numbers of Diaspora arriving to vote within a limited time

iv. Most expensive voting method

v. Hiring of Polling Staff

vi. Absence of Polling Agents / Election Observes can potentially compromise transparency and credibility of voting process

vii. The overseas polling stations may not be accessible to many voters on Poll Day involving time and cost consumed during travel or other reasons

viii. Feasible only if voting rights are limited to diplomats, military officials deployed abroad and their families residing abroad

In person abroad

Voting takes place in embassies, consulates or other locations in foreign countries. In some cases this option is also open to those who are temporarily abroad.

✔ Serves overseas voters and takes place in a controlled environment

✖ Voters may have to travel far to reach the voting location.

Voting In-Person from Abroad: Possible Opportunities and Threats

OPPORTUNITIES	THREATS
- It can be used by people who live **abroad.** - Voting takes place in a **controlled environment**, following the standard process. Secrecy is ensured because voters themselves place the vote in the ballot box. - There are often **polling booths** or specific spaces to vote in private. - The identity of the voter can be verified in person. - It may be **observed** (although it could be more complicated and resource-intensive than standard voting). - There is no dependency on the **postal services.** - It implies low costs for voters if they live close to the consulate.	- Not all countries have **consulates**. - It may entail a lot of **travelling and cost** for those who live abroad but **without having a nearby consulate**. - It may be difficult to use by **differently-abled persons.** - If votes are counted at the polling station abroad and there are very few voters, secrecy can be at risk. - There may be problems of **dual inscription**, with voters being registered in the electoral lists abroad and within the country. - If votes are sent to the country for counting, there is some risk that they get **damaged or lost** during transportation. - An **advance application** is often needed to use this option. - It implies some **costs** for the public administration, as well as organizational efforts. - If there are very few polling stations, there would be long **queues** for voters. - Voters may not be able to use **constituency-specific ballots** (or require additional organization to deliver such ballots to the voters' location abroad).

3. Proxy voting

A citizen living or staying abroad may be authorized or enabled to vote by choosing a person (proxy) who casts the vote on behalf of the voter in the home country, or abroad.

Advantages of Proxy Voting:

i. It is technically simple and does not involve the huge financial and administrative costs that are customary in elections held outside the state territory.

Disadvantages of Proxy Voting:

i. The proxy could use this procedure to obtain an additional vote and thus infringe on the principle of equal suffrage, with the electoral authorities being unable to intervene.

4. E-Voting

The voter may use the Internet, personal digital assistants (PDAs), introduction telephones or a mobile phone to cast his or her vote. This type of electronic voting is most often referred to as remote electronic voting or e-voting and may become more common in future.

a. Polling place E-Voting (EVM):

Polling place e-voting refers to systems where a voter casts his or her vote inside a polling station or similar premises controlled by electoral staff. Carried out in diplomat or consulate etc.

b. Remote E-Voting (Internet Voting):

Remote e-voting is used to describe those systems where a voter casts his or her vote at any place outside the polling station i.e to allow voters who are abroad to transmit a vote using electronic means, for example, casting a vote at a PC and transmitting it to the electronic ballot box over the Internet.

Advantages of E-Voting:

i. In some cases, citizens living or staying abroad are considered to be an ideal test group for remote e-voting, while the real intention is to introduce this new method for electors inside the country as well.

ii. In some cases, citizens abroad are well organized—even better organized than interest groups inside a country—and capable of assessing their needs and putting them onto the agenda.

iii. Depending on the circumstances and the other voting channels available for external electors, remote e-voting might save costs.

Disadvantages of E-Voting:

i. **Data Security concerns**. The security concerns include doubts about the Internet as a means of transmission of confidential information, fear of hacker attacks—both by insiders (e.g. software programmers) and by outsiders (e.g. political parties, terrorists or other states)—

ii. **Influence**. Anxiety about the possibility of undue influence being exerted on the voter during the voting process (e.g. 'family voting').

iii. **Financial aspects**. It may be costly to build the infrastructure for providing remote e-voting only to a limited number of electors. The expensive items can be the building of a digitized, harmonized register of external electors or the maintenance of security of the system.

iv. **Equal treatment of all electors**. External electors from one canton should not be able to vote electronically if those from another canton do not have this opportunity.

Challenges of E-Voting:

i. **Unambiguous identification**: The participant election / voter must be clearly identified and authorized.

ii. **Authenticity of the e-voting servers**: Citizens must have the guarantee that their votes are sent to the official servers.

iii. **Unique and universal voting**: Citizens are allowed to cast one vote. The casting of two or more votes must be prevented.

iv. **Protection of voting secrecy/protection of privacy**: The intention of citizens must remain secret and must not be seen by a third party

v. **Cyber-attacks to**:

   a. Voting devices (private computers, etc.): possible interception and modification of votes, e.g. by Trojan horses (the weakest point of any e-voting system).

   b. Vote transaction from client to server: possible interception and modification of votes (e.g. man-in-the-middle attack, domain name server (DNS)- hacking).

   c. Central server platform (heart of the e-voting system), e.g. denial-of-service attack.

vi. **Force majeure**: Thunderstorms, earthquakes, terrorist attacks etc.

vii. **Traceability, recounting**: Electronic votes must be recounted if appealed.

viii. **Confidence**: The system and its components must be trustworthy. External experts must be able to review source codes.

OVERSEAS PAKISTANI NICOP CARD HOLDERS

As per NADRA's estimates of year 2021, NICOP Overseas Pakistanis card holders are as following:-

S #	Country of Stay (As per NICOP)	Total
1.	Saudi Arabia	3,219,988
2.	United Arab Emirates	2,688,306
3.	United Kingdom	634,716
4.	Oman	442,761
5.	United States	290,837
6.	Canada	180,512
7.	Qatar	153,215
8.	Malaysia	148,415
9.	Bahrain	140,436
10.	Italy	121,167

11.	Kuwait	107,839
12.	Spain	66,065
13.	Greece	66,708
14.	Australia	46,165
15.	France	44,039
16.	Germany	30,264
17.	South Africa	26,349
18.	Libyan Arab Jamahiriya	14,349
19.	Hong Kong	12,487
20.	Ireland, Republic of	11,391
21.	Korea, Republic of	10,216
22.	Belgium	10,198
23.	Others	158,238
	Total	**8,624,661**

NICOP Voters	
Balochistan	142,325
K.P	2,208,466
Punjab	5,166,630
Sindh	1,009,496
Islamabad	97,744
Total	**8,624,661**

HIGHLIGHTS OF ADVANTAGES AND DISADVANTAGES OF EXTERNAL VOTING

	Tentative advantages	**Tentative disadvantages**
Postal voting	Lower financial and organizational costs Able to reach most eligible electors	Problematic transparency of voting procedure Dependent on a speedy and reliable postal service
Voting in diplomatic missions	High transparency of voting procedure	Higher financial and organizational costs Many eligible electors do not live near the location of the mission
Proxy voting	Almost no additional expenses	Principle of electoral equality not sufficiently guaranteed
Electronic voting	No delays Available worldwide Facilitates counting	Security concerns Financial costs of implementation

THE ROAD TO I-VOTING

Pakistan has the 6th largest diaspora in the world, numbered at almost 9 million[96]. Overseas Pakistanis have made a major economic contribution and sent home remittances of $ 29.4 billion in the Fiscal Year 2021[97]. Overseas Pakistanis raised calls for the right to enfranchisement under Article 17 of the Constitution, as early as the first General Elections in 1970. Multiple constitutional petitions were filed in this regard (in the year 1993, 2011, 2014 and 2015). The judiciary has been consistently upholding their basic right to vote and has called on the ECP to make provisions.

To overcome the budget and logistic constraints that pose huge hurdles in enfranchising the diaspora, the ECP established a Directorate for Overseas Voting, which experimented with various voting modalities. Mock voting exercises for postal ballots and telephone failed, as the ECP reported they *"lack the necessary electoral integrity checks to preserve the credibility of an election result."* Commenting on the feasibility of other modalities, ECP stated: ``*...given the size and dispersal of the Pakistani diaspora, coupled with the limited official resources available in-country and abroad, any significant in-person voting operation would be expensive and logistically challenging."*[98] In 2017, the ECP was sanctioned by the Elections Act, 2017 *''to conduct pilot projects for voting by Overseas Pakistanis in bye-elections.''*[99]

In 2018, the Supreme Court of Pakistan consolidated 16 constitutional petitions demanding overseas right to vote[100]. In what ensued, the Supreme Court asked NADRA to build a system in 10 weeks. This system was presented in a public session of the Supreme Court in April 2018. The technical experts in attendance voiced serious reservations, following which the Supreme Court formed the Internet Voting Task Force (IVTF) to audit the system.

Internet Voting Task Force (IVTF) was composed of information security experts and researchers, who in the short time of 3 weeks, conducted a high-level security analysis of the system and submitted their report. The IVTF report raised some serious security concerns: lack of ballot secrecy, vulnerabilities allowing multiple votes per voter to name a few. Their report stated that deployment of iVoting in General Election 2018 would be "*a hasty step with grave consequences"*. The report also emphasized that *"many of these security vulnerabilities are not specific to iVOTE [sic] but are inherent to this model of Internet voting systems''*[101].

Cognizant of this, Supreme Court directed ECP to pilot iVoting only in bye-elections. The bye-elections were held in 35 constituencies on 14th October 2018. Out of the 631,909 eligible overseas voters, a mere 7,419 citizens (1.17%) registered to vote using the new system. On

[96] Overseas Pakistanis Foundation, https://www.opf.org.pk/
[97] Pakistan gets record remittances, https://www.dawn.com/news/1650949
[98] Voting from abroad, https://www.dawn.com/news/1335670
[99] The Election Act 2017, https://www.ecp.gov.pk/frmGenericPage.aspx?PageID=3111
[100] IVTF Report 2018, https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf
[101] IVTF Report 2018, https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf

the day of the elections, a total of 6,233 voters out of these citizens cast their votes. ECP later reported that on the day of the polls the system withstood 7,476 DDoS attempts. The trial was smooth and uneventful. In its own report, the ECP cited key issues in the system that violated ballot secrecy, enables voter coercion, lacks auditability, and may be vulnerable to state-level cyberattacks[102].

I-Voting pilot project report was presented in the National Assembly (NA) and Senate in January 2019. Their discussion in parliament however remained pending for 3 years. In 2021, the Ministry of IT (MoIT) hired Minsait as consultant to audit the Internet voting system. The Spanish firm reiterated IVTFs concerns and reported that the internet voting system does not meet "constitutional requirement of vote secrecy, *and neither the voters, nor the ECP would have any guarantee that the results obtained from the system represent the choices made by the voter ... Therefore, the audit team strongly recommends the existing system shall be upgraded prior to being used on any Election[103]."*

The i-voting developed by NADRA during year 2018 was deployed on shared resources rather than dedicated servers. Similarly, some guess questions were asked from the remote voters to identify and authenticate them rather than using proper state-of-the-art Biometric technologies. Moreover, the whole voting system revolves around email, if email is compromised resultantly it compromises the integrity of the whole electoral system.

The IVTF Report that resulted from this study (Commonwealth Report on Cybersecurity in Elections-2020), which is publicly available, highlighted a range of concerns, including the following:

i. iVOTE did not provide the ballot secrecy required in the Constitution of Pakistan and in the Elections Act, 2017. This was inherent to the computational approach taken in iVOTE, rather than a failing of the software implementation.

ii. Voter coercion and vote buying were very possible in this system.

iii. A particular vulnerability was allowing users to choose other constituency within the voting system, outside of which they are registered.

iv. The website and interface were vulnerable to being impersonated in phishing attacks.

v. The DDoS-protection utilised by NADRA could compromise ballot secrecy, exacerbated by the foreign nature of the external provider.

---

[102] Report on i-Voting Pilot, https://ecp.gov.pk/documents/ivotingreport.pdf

[103] Minsait Consultancy for Analysis, Design and Implementation of Internet Voting for Overseas Pakistanis, https://www.ecp.gov.pk/documents/reports/Final%20report%20by%20Minsait%20Final.pdf

vi. iVOTE employed deprecated and compromised third-party components.

vii. No usability studies had been carried out, particularly in relation to low-literacy individuals, which in turn might raise new security concerns.

viii. iVOTE emails could be blocked by spam filters.

ix. iVOTE did not offer the verification or redundancy features in other jurisdictions with experience in internet voting.

x. There was no threat model analysis or code documentation.

xi. There was no known resource planning for monitoring iVOTE on polling day.

xii. There was no known planning for preventing insider attacks.

xiii. Newer technologies and architectures should be considered.

The NADRA's Chairman in August 2021 proposed a Verifiable Voting system, saying "Elections are not free and fair unless they are verifiable." He also said the work on developing the system was underway and expected to be completed in a year[104].

THE IMPACT OF OVERSEAS VOTERS

The bloc of overseas voters poses a unique situation with serious implications. Research has identified that the inclusion of overseas citizens votes can have three kinds of impact, *"'swings' in which overseas votes change election-night results; 'interregnums' in which the wait for overseas votes distorts coalition negotiations; and 'feedback effects' where the perceived importance of the extra-territorial votes drives political parties to engage increasing numbers of overseas voters[105]*".

In 2019, the first empirical analysis to understand if and by how much overseas voters can impact the results of elections was undertaken. It compared the margin of victory with the number of eligible overseas voters for the constituencies in bye-elections 2018. In a conservative estimate, the authors reported that at least one in five races in the General Election may be decided by votes cast by overseas Pakistanis[106]. A 2020 report on cybersecurity for elections, by the Commonwealth Secretariat also points how internet

[104] Nadra proposes major change in i-voting system, https://www.dawn.com/news/1638691
[105] Gamlen, A. (2015). The impacts of extra-territorial voting: Swings, interregnums, and feedback effects in New Zealand elections from 1914 to 2011. *Political Geography*, *44*, 1-8.
[106] Binte Haq, H., McDermott, R., & Taha Ali, S. (2019). Pakistan's Internet Voting Experiment. arXiv-1907.

based online voting could impact 50% seats in election outcomes, in a simplistic analysis[107]. In 2021, similar analysis has been conducted, the most prominent being by media groups namely Samma[108] and Geo[109].

There are two aspects to this phenomenon. It is heartening and positive for overseas Pakistanis as they can be sure that their votes will impact the politics back home. However, it necessitates that the voting system has stringent electoral integrity checks. Previously, the ECP itself as well as major political parties have expressed their reservation over how an overseas voting system could be used as a tool to rig elections. If elections are swung by overseas votes, such allegations will gain traction.

OUTSTANDING CHALLENGES FOR INTERNET VOTING

There are numerous outstanding challenges that need to be addressed without further delay. Without resolution, these issues could raise serious questions regarding the integrity of elections conducted through internet voting for overseas Pakistanis.

Ballot Secrecy: Since the development of i-Voting various actors including the IVTF, ECP, Minsait Report have reiterated that the incumbent system does not provide secrecy of ballot, in clear violation of the Constitution and Elections Act, 2017. It should be ensured that providing overseas Pakistanis the right to vote, should not sabotage the right to a secret ballot.

Voter Coercion: In remote voting modalities, there is virtually no way to ensure that an individual is not revealing its vote or being coerced to vote a certain way. Specifically, the demographics of the Pakistani diaspora, a majority of which resides in the middle east as laborers, aggravates the possibility of coercion, an eventuality that the ECP itself recognizes when it addresses the issue of the" kafeel" abusing custody of passports.[110.]

Cybersecurity Challenges: Internet voting is susceptible to a whole range of cybersecurity issues. The IVTF report documented multiple such problems in 2018 which are representative of this class of systems. Phishing attacks can easily be mounted; there have

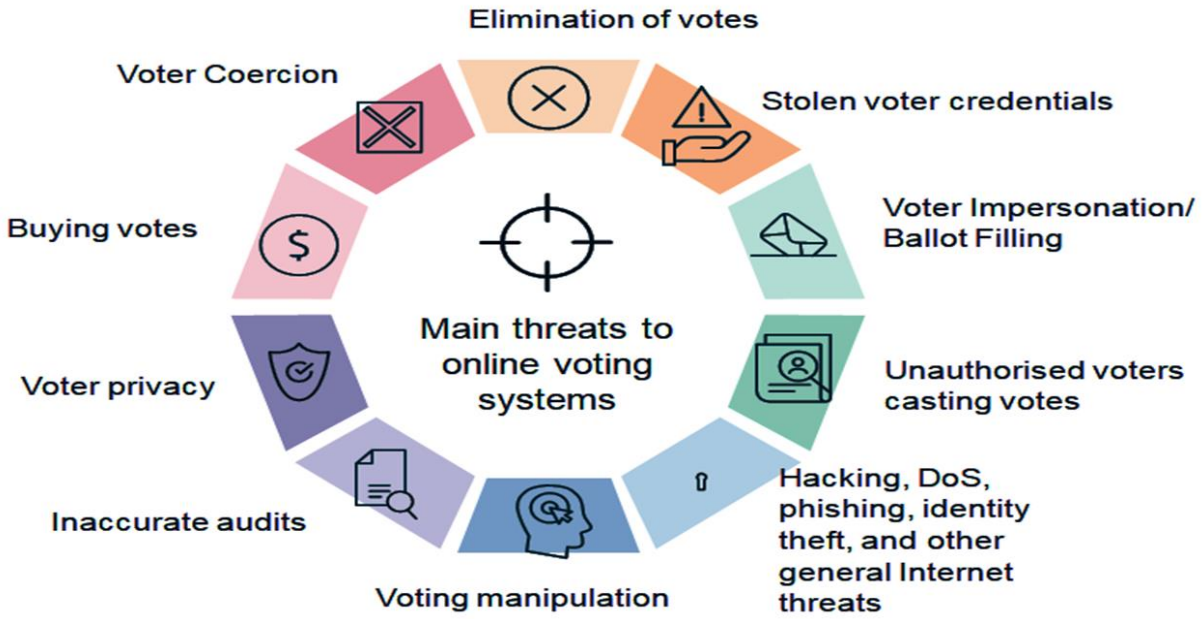
[107] Cybersecurity for Elections, A Commonwealth guide for best practices, https://thecommonwealth.org/sites/default/files/inline/Cybersecurity_for_Elections_PDF_0.pdf
[108] How 8 million overseas Pakistanis will affect general elections, https://www.samaa.tv/news/2021/11/how-8-million-overseas-pakistan-will-affect-general-elections
[109] Almost 7m overseas Pakistanis registered to vote in 20 hotly contested NA constituencies https://www.geo.tv/latest/371503-almost-07m-overseas-pakistanis-registered-to-vote-in-20-hotly-contested-na-constituencies
[110] Election Commission of Pakistan, Report on I/-Voting Pilot Test. https://ecp.gov.pk/documents/ivotingreport.pdf, October 2018.

been instances where malicious parties have built websites which have successfully masqueraded as websites of official government entities, including NADRA[111].

Denial-of-service attacks are common and they necessitate reliance on traffic filtering services which can be hard to police. In the domain of cyberwarfare, international agencies with unlimited resources can launch zero-day attacks to cripple elections systems or manipulate voting results. Moreover, with Internet voting, hackers no longer have to focus exclusively on hacking elections infrastructure but can attack user PCs and smartphones which now represent the weakest link in the system. Malware can be constructed to infect voter PCs and change their votes without detection.

Voter Usability: Prior to the deployment of any internet voting solution, extensive usability tests need to be conducted with real time input from actual users. Given the low literacy rate of almost half of the diaspora, difficulty in registering and voting could cause exclusion of a fraction of the voters. Similarly, accessibility features need to be incorporated for differently-abled persons.

Voter Authentication: As the process of voter registration and authentication is done remotely and adjudicated by a computer program, there is currently no foolproof detection mechanism that can differentiate between a genuine voter and a malicious actor.



Possible Disenfranchisement: The spirit behind introducing voting for overseas Pakistanis is to give equal opportunity to all voters, regardless of their geographic location. However, the single day time limit for vote casting, in effect disenfranchises and excludes voters that live in time zones incompatible with the allocated voting period. This could be easily rectified

[111] Overseas Pakistanis Scammed by Fake NAdra Website, https://www.samaa.tv/money/2020/07/overseas-pakistanis-scammed-by-fake-nadra-website

by extending the voting period to two weeks. Most countries allow voters voting from abroad a period between 5 and 14 days to cast their votes.

Electoral Dispute Resolution: The current i-voting system lacks auditability features, which means that there is no convincing evidence generated by the system that would be admissible in a court of law. This along with the capacity of the judiciary to understand the nuances of internet voting technology and consequently resolve issues related to it, needs to be considered.

Electoral Offences: After the Bye-Elections of 2018, some voters posted screenshots of their votes on the social networking site Twitter, rather unintentionally, but without a doubt in clear violation of the electoral code of conduct. Electoral offenders being outside the jurisdiction of Pakistan, it is unclear how law will take its course.

MISPERCEPTION ABOUT ONLINE BANKING AND ONLINE VOTING:

A very common question, which arises in conversations regarding Internet voting, is that if applications such as shopping, banking or commerce can be conducted online, then why not voting? This is a fair question as banking and e-commerce are critical applications and considerable effort is made to secure them. Are the same techniques applicable to Internet voting?

There are two important differences to be considered here: first, online banking and e-commerce systems are vulnerable to cybercrime with attacks costing the economy up to hundreds of billions of dollars every year. A recent study estimates cybercrime revenue at $1.5 trillion per year and indicates that not only is cybercrime a fast-growing phenomenon but also that cybercriminal outfits may actually be making more money than small and mid-size companies. Banking and e-commerce websites get hacked routinely and the costs of these attacks are typically counted as 'the cost of doing business'.

Second, and most important, the key tools that banks use to fight cybercrime are not applicable to Internet voting. For instance, financial institutions maintain detailed records and audit trails of every transaction. In the case of voting, maintaining audit logs or trails that identify the voter is a direct violation of the secret ballot property. Moreover, Internet voting cannot recover from attacks in the same way that banks can: miscast votes cannot be easily detected or reversed the way banking transactions can. Furthermore, elections are a far more sensitive matter than banking and news of a hacking incident may have a serious negative impact on citizen confidence in elections and long-lasting political repercussions.

In case of an incident, banks and merchants have recovery protocols in place, which include blocking stolen credit cards, reversing irregular transactions, compensating clients for lost funds, etc. Again, these mechanisms do not apply to Internet voting. In the words of election security expert, David Jefferson:

> "Vote fraud is much less manageable than ecommerce fraud. There is no election analog to the natural business practice of "spreading the cost" or "spreading the risk". There is no way to pass on to other voters the "losses" due to illegal ballots cast by ineligible voters or attackers, or to recover votes changed by malicious software. There is no "insurance" that one can buy to cover those losses. There is just no way to compensate for damage done to an election."

For these reasons, in the election security community, paper is still considered the gold standard when it comes to elections. To quote renowned cybersecurity expert, Bruce Schneider:

> "Today, we conduct our elections on computers. Our registration lists are in computer databases. We vote on computerized voting machines. And our tabulation and reporting is done on computers. We do this for a lot of good reasons, but a side effect is that elections now have all the insecurities inherent in computers. The only way to reliably protect elections from both malice and accident is to use something that is not hackable or unreliable at scale; the best way to do that is to back up as much of the system as possible with paper."

The detailed research paper to clarify this misperception written by **David Jefferson**, *[Computer Scientist, Lawrence Livermore National Laboratory, Board of Directors, Verified Voting Foundation, Board of Directors, California Voter Foundation]* *https://verifiedvoting.org/publication/if-i-can-shop-and-bank-online-why-cant-i-vote-online* (**Annex-E**)

RECENT GLOBAL VIEW ON INTERNET VOTING

Several developed countries have piloted remote internet voting solutions only to suspend them later, citing security issues. Here we summarize recent international developments and trends in Internet voting since the IVTF report was issued in 2018.

United States:

In its 2015 report, the U.S. Vote Foundation asserted that any possible future Internet voting system should utilize E2E-verification, but the report stated that this should not even be attempted before greater experience has been garnered with E2E-V systems deployed and used within in-person voting scenarios.

Later in 2018, the National Academy of Sciences report also reiterated: *"At the present time, the Internet **should not be used** for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as **no known technology** guarantees the secrecy,*

security, and verifiability of a marked ballot transmitted over the Internet. Conducting secure and credible Internet elections will require ***substantial scientific advances***[112]*."*

The report urged *"U.S. Election Assistance Commission standards and state laws should be revised to support pilot programs to explore and validate new election technologies and practices. It also recommended "Election officials are encouraged to seek expert and public comment on proposed new election technology before it is piloted."*

In May, 2020 Department of Homeland Security issued a confidential report to voting vendors and election officials in all 50 USA states cautioning against use of Internet voting in forthcoming polls, warning that ballots "*could be manipulated* ***at scale***," meaning hackers could change large volumes of votes undetected.

India: The Indian Chief Election Commissioner has ruled out the possibility of internet voting being deployed in India due to ballot secrecy concerns, saying that "*People can be put at gunpoint or even bribed to vote for anyone.*" Since then the Indian government has approved a proposal to allow citizens above 65 years of age to use postal ballots for voting. There have also been talks to use hybrid voting, where ballots are sent by email and returned by post.

Estonia: Estonia is the only country where remote internet voting is available for national level binding elections to the whole electorate. However, internet voting is not a stand-alone voting modality in Estonia. Voters can cast vote multiple times in precincts and/or online and only the final vote will be recorded.

France: In France, in early 2020, the Ministry for Europe and Foreign Affairs approved a new Internet-voting platform for the consular elections of May 2020, after rigorous audits, risk analysis and vetting by independent experts. This development means that French citizens abroad will have the choice of voting to choose their representatives in person, by proxy, or via the Internet. It is not yet clear which technology this system will be using.

Panama: Panama has since 2014, allowed its citizens living abroad to cast their votes through online voting.

Armenia: In Armenia only diplomatic staff and military personnel posted abroad can use online voting.

Switzerland: Switzerland has deployed internet voting for voters living abroad from a few cantons.

[112] Securing the Vote – Protecting American Democracy, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

Canada: Internet Voting has been deployed in a few municipalities for local elections and a provincial level election in N.W.T In 2020, Election Canada issued a statement saying "*At this point, Elections Canada is not considering introducing internet voting. Implementing such a change would require significant planning and testing in order to ensure that the agency preserves certain aspects of the vote, including confidentiality, secrecy, reliability, and integrity. Given the current operational and time constraints, this option cannot be explored properly at this time.*"

Russia: Russia has rapidly expanded its Internet voting initiative. In the fall 2021 Duma elections, over 1.5 million voters have registered to vote using the internet voting system, amid allegations of using the internet voting system as a tool for voter intimidation and election rigging.

Australia: In Australia, Internet voting has been used in New South Wales local elections since 2013. Considerable security issues have surfaced over the years and the system has been rebuilt a couple of times. In the most recent deployment, in December 2021, the iVote system crashed midway through the local council elections following which the NSW Electoral Commission issued an apology. Online votes were delayed for three days as a result.

Country	Voters	Country	Voters
 **Estonia**	**National**	 **Armenia**	**Military personnel, Diplomatic staff**
 **Canada**	**Municipal, Provincial**	 **France**	**Diplomats Citizens**
 **Switzerland**	**Overseas citizens**	 **Panama**	**Overseas Citizens**
 **Russia**	**Local Elections**	 **Australia**	**Provincial**

RECOMMENDATIONS

The recommendations of IVTF, Minsait report, The Commonwealth Report on "Cybersecurity for Elections" and ECP's own report on the October 2018 pilot exercise are comprehensive. Before Pakistan can progress along the internet voting route, it is necessary to build stakeholder acceptance and consensus, build indigenous election management and technical expertise, for effective policymaking and to ensure ECP can take ownership of the resulting solution. It should be noted that failure and/or rigging in the overseas voting process will impact every constituency, playing a crucial role in the outcome of elections.

Our recommendations draw primarily from the IVTF, NAS, and Minsait report and emphasize certain key considerations to enable overseas voting. We recommend that ECP address critical research gaps and that two solutions be considered in parallel to enfranchise overseas citizens in the forthcoming general elections.

Foundational Concerns

1. We recommend that ECP urgently undertake a comprehensive study of the myriad legislative and constitutional challenges posed by overseas voting and propose definitive solutions that are acceptable to stakeholders. There are considerable gray areas in the overseas voting discourse which need to be addressed before the question of an overseas voting exercise can even be considered. We discuss some of the problems:

Ballot secrecy is the primary concern in remote voting modalities. It is a well-established fact that once polling is taken out of the precinct, ballot secrecy can no longer be guaranteed[113]. Researchers have devised foolproof Internet voting systems on paper, but they are still far from actual realization[114,115]. Currently, to the best of our knowledge, there is no viable technological solution for this scenario. This view is in accord with recommendations from some of the world's leading international technology experts[116] .

The Estonian system resolves the secrecy issue by deploying Internet voting in parallel with precinct-based voting, and citizens are free to choose between the two modalities. Moreover, if they cast a vote using the Internet, they can nullify by casting the vote again at the precinct. In the 2019 elections, 247,232 citizens, or 43.8% of all eligible voters, voted over the

[113] Embassy voting is an exception to this rule and may be considered a variation of precinct voting, in that voters get privacy in a polling booth setting to cast their vote

[114] Panchal, A., Indrale, S., Jadhav, N., & Karlekar, N. I-voting System using JCJ Protocol.

[115] Clarkson, M. R., Chong, S., & Myers, A. C. (2008, May). Civitas: Toward a secure voting system. In *2008 IEEE Symposium on Security and Privacy (sp 2008)* (pp. 354-368). IEEE.

[116] Securing the Vote – Protecting American Democracy, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

Internet, of which a small number re-cast their votes later at polling stations[117]. This is clearly not possible in our current scenario.

Another option is to pass legislation whereby overseas citizens waive their right to a secret ballot. This is a highly controversial practice and was observed until recently in some US states which allowed overseas citizens to vote in elections. Some states, like Alaska, even explicitly informed voters that they were foregoing ballot secrecy when casting votes on the Internet[118] .

If ballot secrecy is not assured, several more problematic scenarios emerge. For instance, publicizing one's ballot is a clear violation of the Article 226 of the Constitution of Islamic Republic of Pakistan. When Prime Minister Imran Khan committed this violation in 2018, ECP sought a written apology from him[119]. However, in the bye-elections of 2018, multiple overseas voters posted snapshots of their casted votes on Twitter. How does ECP investigate and address electoral offences in foreign jurisdictions?

Votes can easily be bought in a remote setting. An overseas citizen can be coerced to vote a certain way by a family member or an employee. Specifically, the demographics of the Pakistani diaspora, a majority of which resides in the middle east as labor class, aggravates the possibility of coercion, an eventuality that the ECP itself recognizes when it discusses the

[117]Estonia Voting, General Statistics, thttps://rk2019.valimised.ee/en/voting-result/voting-result-main.html
[118] Internet Voting Leaves out a cornerstone of democracy: The Secret Ballot, https://www.technologyreview.com/2016/08/18/107858/internet-voting-leaves-out-a-cornerstone-of-democracy-the-secret-ballot/
[119] ECP demands signed apology from Imran, https://www.thenews.com.pk/print/353258-ecp-demands-signed-apology-from-imran

issue of the" kafeel" abusing custody of passports[120]. In a hypothetical scenario, what would ECP do if a video surfaces online of voters selling their votes to a third party or being coerced to vote for a certain candidate? How would ECP investigate this issue? How would those votes be identified and treated? Certain parties could even manufacture or circulate such videos simply to cast suspicion on election results or make whole election controversial.

These issues were identified by the Internet Voting Task Force in 2018, but there is still little recognition of them in the mainstream discourse. If these fundamental gray areas are not debated and resolved prior to deploying overseas voting, we can expect considerable controversy in the next polls. The viability of our entire overseas voting exercise depends upon this.

2. We recommend the ECP's R&D Wing should undertake an extensive study of next-generation Internet voting solutions developed in the last 3-4 years. Some very sophisticated and novel systems have been built recently by Estonia, Russia, Mexico, Switzerland, United States, and Australia. The purpose of this exercise is to study the different architectures and security properties of these systems and gain fundamental insights into designing such systems for Pakistan. The majority of these systems have failed, and we would benefit considerably from examining their mistakes.

This study describes the different dimensions of Internet voting in these countries, including the social, legal, technical, and political aspects, and develop guidelines and standards. This work can be undertaken by the ECP's R&D Wing in partnership with universities and research organizations. The ECP should also contact EMBs in these countries to build linkages and arrange on-site visits.

3. We recommend that ECP develop specifications for remote voting modalities in accord with best practices, international guidelines, and pilot studies. This is a key lesson from our prior experience with iVOTE in 2018 [121,122]. The iVOTE system repeated many of the fundamental design and technology mistakes encountered in similar systems developed in other countries and overlooked fundamental software development processes.

ECP should identify system specifications as per its requirements, in partnership with the vendor (or any third party, if need be), and ensure quality control and standards are maintained. The different levels of specifications need to be integrated seamlessly along with a rigorous evaluation framework. This means a detailed technical plan of what features are needed in the remote voting solution and also accompanying criteria upon which the assessment of the resulting solution will take place. Many of these criteria should be based

[120] Report on I/-Voting Pilot Test, 2018. https://ecp.gov.pk/documents/ivotingreport.pdf
[121] Election Commission of Pakistan: Findings and Assessment Report of Internet Voting Task Force ((IVTF) On Voting Rights 0f Overseas Pakistanis Executive Report 2018, https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf
[122] *Consultancy for the Analysis, Design, and Implementation of Internet Voting for Overseas Pakistanis*. Minsait Report for Ministry of Information, Technology & Telecommunications, https://www.ecp.gov.pk/documents/reports/Final%20report%20by%20Minsait%20Final.pdf.

on the core values of elections. This prevents ad hoc system design and ensures a baseline along which the resulting system is evaluated. Evaluation becomes an uphill task if expected outcomes are clearly defined at the start.

This exercise requires careful deliberation and a fine appraisal of the challenges that remote voting offer, and should be undertaken in close consultation with experts, technologists, vendors and legal experts. This process will require multiple rounds of feedback, ideally through independent audits and scrutiny, combined with pilot deployments.

Overseas Voting

4. As a first option for General Elections of 2023, we recommend that ECP coordinate with NADRA (or any other vendor) to develop or procure a state-of-the-art verifiable Online voting solution to be used in an embassy-voting scenario. This effort should be undertaken in very close collaboration with the vendor and great care must be taken not to repeat the mistakes of 2018.

This system must be rigorously piloted at every possible opportunity, preferably in non-political elections. However, even if the pilots are successful, it is premature at this stage to consider a full-fledged Internet voting deployment. The verifiability paradigm offers strong guarantees for electoral integrity, but it is widely acknowledged that it cannot as yet safeguard ballot secrecy outside of a precinct setting.

In this case, we concur with the NAS Report which states, "*the Internet should not be used for the return of marked ballots.*" [123] We therefore advise that this system be considered for use primarily within an embassy-voting scenario. Voting terminals deploying this solution can be set up in various embassies, interconnected over VPN or Intranet and protected by firewalls and access control lists. Votes can be collected electronically, while still maintaining ballot secrecy in a highly supervised and controlled environment. We advise piloting as a solution to get greater insight into its use.

We would also recommend that ECP reassess the overseas voter registration mechanisms. The iVOTE system and the more recent proposal from NADRA suggest that voters should prove their identity for registration by answering a series of personal questions. The ECP should rigorously assess the security of this methodology as this may also open avenues for vote selling and coercion. Voter registration and vote casting in an embassy setting as well may present a more secure option because this will be called Online Voting behind firewalls. All the Embassies will be directly connected though secure VPN with ECP/NADRA Data Center to route all voting traffic bypassing Internet main Information Highway. This mode of voting has low risk factors than Internet Voting off course. Similarly,

[123] Securing the Vote – Protecting American Democracy, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

ECP may opt for using biometric authentication from embassy rather than asking guess questions for registering as voter.

Building an Internet voting system with satisfactory security guarantees will be challenging in the limited time we have available for the next polls. This is a formidable endeavor. The Minsait report of 2020 predicted such an exercise could take 1-3 years, depending on the resources and expertise available. We expect it could take longer, considering delays due to administrative overheads and paperwork, hiring overheads, the pandemic situation, etc.

5. As a second option for General Elections of 2023, we recommend ECP urgently reinvestigate postal voting to enfranchise overseas voters. We are aware of the challenges of this modality: an earlier pilot of postal voting by the ECP was not very successful, there are serious logistics issues with postal voting in some Middle East regions (postal mail is only delivered to a PO box in some countries), and postal voting is considered a dated methodology in some circles.

However, postal voting has considerable advantages: many countries have deployed it at small scale and continue to use it successfully, giving us a wealth of guidelines to refer to. The issues of secrecy and coercion still exist in postal voting, but these risks are well-studied, and are much smaller as compared to Internet voting because it is difficult to manipulate large numbers of physical ballots. Postal voting will also likely incur significantly less costs than Internet or embassy voting and be more convenient to use.

More interestingly, there have been very promising new developments in postal voting. First, a hybrid form has emerged that has been deployed relatively successfully in the US presidential elections of 2020. In this case, ballots are sent electronically to the voter by email or downloaded from the elections website. The voter prints and fills out the ballot and then returns it via postal mail to be counted. This easily solves the problem of voters being unable to receive the physical ballot in the post. Second, researchers have proposed mechanisms to extend end-to-end verifiable voting guarantees to postal voting as well[124], thereby ensuring electoral integrity equivalent to that achieved by verifiable Internet voting or EVMs.

We recommend that ECP explore the viability of postal voting and, if necessary, undertake pilots to determine its effectiveness.

The final decision of which of these two proposed modalities to deploy in General Elections of 2023 should only be made after both solutions have been thoroughly studied, rigorously piloted and compared.

6. We recommend that ECP develop a digitization strategy for the General Elections of 2023. This entails a rigorous study and cost-benefit analysis of using digital technology

[124] Crimmins, B. L., Rhea, M., & Halderman, J. A. (2021). RemoteVote and SAFE Vote: Towards Usable End-to-End Verification for Vote-by-Mail. *arXiv preprint arXiv:2111.08662*.

resources to support remote voting. It will likely not be possible to set up an extensive digital infrastructure and equip with skilled staff in the limited time available to us. The ECP should consider stop-gap arrangements with other suitable national bodies including NADRA data center because of some inherent databases like NICOP, biometrics of every citizens, Machine Readable Passports, Mobile SIM verifications, etc for this purpose until it develops its own resources and expertise to the required capacity. Similar arrangements have already been made in the past with stakeholders like NADRA, which already host critical national databases which will need to be integrated with our systems.

7. **For strengthening the use of Information Communication Technology (ICT) for elections while enhancing their security, we follow the following recommendations of Commonwealth Report named as "Cyber Security for Elections – A Commonwealth Guide on Best Practice":**

i. EMBs should give careful consideration to use of technology in the elections process if and where it demonstrably addresses a clear need, while carefully managing the resulting cybersecurity risks with measures that are proportionate.
ii. Cross-government (including EMBs, national cybersecurity centers, state and local government agencies, data protection and media/telecoms regulators) co-ordination, and co-operation with political parties, traditional and new media, and civil society are key to effective action and societal trust in elections. A standing multi-stakeholder election security group should manage preparation and directly oversee the election process, trigger continuity plans, and communicate with the media and parliamentary oversight bodies.
iii. EMBs and national cybersecurity agencies should consider whether designation of key election systems as part of critical national infrastructure will improve their security.
iv. EMBs must model and mitigate the potential of insider attacks, both within their own activities and those of other electorally relevant organizations, such as political parties. Existing anti-corruption efforts, non-disclosure agreements and strong access controls are useful tools in this context.
v. Individuals with reading – and especially writing and administrative – access to significant systems should be security vetted to an appropriate level. While government security agencies may carry out vetting, for independence reasons, EMBs should retain the ultimate decision as to staff appointments.
vi. EMBs should regularly audit automated systems used for electoral planning for integrity, and put in place processes to ensure documentation and assurance of the provenance of data sources being used.
vii. EMBs should be aware of and seek to mitigate cybersecurity risks involving contractors for electoral logistics, especially those with systems directly linked to the EMB.
viii. Cybersecurity threat assessment and mitigation should be undertaken regularly by EMBs as part of an ongoing process, rather than in the run-up to ballot periods alone.
ix. Information about polling locations should be delivered from EMBs to voters in a secure and robust manner, with monitoring of the veracity and timeliness of information provided.
x. An independent agency, such as a data protection authority (DPA), should have

competences over the privacy and security of electoral data, including its processing, storage and transformation into derivative data by political parties.

xi. EMBs should take steps to ensure that only electoral roll data necessary for the intended purposes of use are transmitted to authorized actors, in a format which does not encourage inappropriate reuse or dissemination and including fingerprinting data to facilitate the tracing of data breaches.

xii. EMBs and their cybersecurity partners should identify all avenues, actors and systems which feed into and are informed by the electoral roll(s), and should map out security threats and capacities, contact points and regular procedures to check for data and system integrity.

xiii. The master copy of the electoral roll(s) should not be connected to public networks and should only be updated with additional information in accordance with procedures designed to ensure the integrity and provenance of the new information.

xiv. When engaging in data cleaning or validation, the responsible agency should keep complete tamperproof logs of all changes made and use technologies which allow such logging. This allows for detection of integrity issues and specific rollbacks if such issues are discovered.

xv. EMBs and their cybersecurity partners should ensure providers, domain and hosting services for any online registration are easily contactable, identify periods where availability is critical (e.g. near electoral deadlines) and should designate a specific team or individual as responsible to respond to system issues.

xvi. EMBs should prepare and practice backup procedures where availability attacks on critical systems might disrupt electoral processes.

xvii. Where machines are used to cast votes, EMBs should carefully consider the use of voter verified paper audit trails to enable every vote to be verified where results are disputed.

xviii. Systems to verify postal ballots should be carefully designed to maintain public trust and the confidentiality of votes.

xix. EMB officials should examine and determine how to treat every ballot rejected by automatic counting systems as invalid or uncertain.

xx. EMBs should have in place procedures for ongoing secure configuration and testing of all systems used in elections, with regular exercises to test responses to attacks.

xxi. EMBs should consider obtaining external certification of security-critical elements of election infrastructure to build public trust.

xxii. Before introducing internet voting systems in elections, EMBs should assess very carefully the cybersecurity risks they introduce, as well as the extensive mechanisms required to manage that risk and potential damage to voter trust in case of disputed outcomes.

xxiii. EMBs should ensure that result transmission mechanism is secure, subject to clear and strict access controls, and have appropriate levels of redundancy and backup procedures in place should components of them unexpectedly fail.

xxiv. EMBs can improve the resilience of results reporting, as well as public confidence in the results, by supporting parallel vote reporting and tabulations by civil society organizations.

xxv. EMBs should ensure software used in vote tabulation is audited and verified, and used by trained staff on appropriately secured hardware.

xxvi. EMBs websites, especially those announcing election results, should be protected

against high levels of traffic and denial of service attacks.

xxvii. EMBs should develop regularly updated processes for auditing the use of election technologies, and consider how far these processes and their results can be made accessible to observers and the public.

xxviii. EMBs and/or their cybersecurity partners should actively monitor election infrastructure for intrusions, as well as having the capability to rapidly escalate and respond during election periods at the direction of senior decision-makers.

xxix. EMBs should provide cybersecurity training for all staff, as well as career development for technical staff, partnering with local universities, regional peers and international organizations.

REPORT OF THE FINANCIAL COMMITTEE ON OVERSEAS VOTING

(A) FINANCIALS ASPECTS OF OVERSEAS VOTING (INTERNET VOTING)

The activity wise breakup of Overseas project along with its estimated costs are hereby given below:

Activities	Amount in PKR
Primary Site	
A) Software Development + Databases (Hexa-Data, Licenses of Oracle, Softwares, Windows, HCI Licensing and MS Office, Software Development Tools & Controls)	900 Million
B) Infrastructure – Indicative List Tier-4 Data Centre Compliant Civil Works, Power Backup from Two Sources, Air Conditioning, UPS, Generators, Stabilizers etc.	250 Million
C) Network Equipment – Indicative List (Managed Switches, Routers, Firewalls, Antivirus etc.)	200 Million
D) Information Security – Indicative List (IPS/IDS/DDoS solutions, Labs/Security Operations Centre)	200 Million
E) Human Resource (35 to 40) – Indicative List i. Network Administrators / Infrastructure Specialists ii. Software Developers iii. Information Security Specialists iv. Projects Managers	200 Million (per annum)
Sub Total	1.75 Billion
F) Disaster Recovery Site (DR) at Different Geographical Location	750 Million
Grand Total	**2.50 Billion Approx.**

(B) FINANCIAL DETAILS OF OVERSEAS VOTING (INTERNET VOTING):

Software Development + Databases:

To prepare the Internet/Online Voting solution for Overseas Pakistanis, ECP need to develop the software and acquire: -

a) Database solutions (Engineered Systems);
b) Licenses of databases;
c) Third party software;
d) Operating systems;
e) HCI Licensing and other tools & controls.

For this purpose, approximately 900 million rupees are required.

Infrastructure:

Without any solid & standard infrastructure, no online system can be made safe, secure & operational successfully. Therefore, there is need to deploy required infrastructure as a baseline so that it can serve the purpose of handling the Online Voting Solution. This would require:

a) Tier-4 compliant Data Center;
b) Civil work;

c) Power from two different sources;
d) Proper cooling system;
e) UPS, Generators and Stabilizers;
f) Fire alarm and extinguishers etc.

To accomplish this, approximately 250 million rupees would be required.

Network Equipment:

To make the network secure and to keep it live & running, network connectivity and various network equipment are required like Managed Switches, Routers, Firewalls etc. This will incur an approximate cost amounting to rupees 200 million.

Information Security:

In order to secure the systems, networks, databases and infrastructure deployed at the Data Centre, complete solution having the capability to detect and respond to cyber security is mandatory. For this purpose, system information and event management (SIEM) solutions are implemented which require:

a) Trained security professionals;
b) Intrusion Detection System/Intrusion Prevention Systems (IDS/IPS);
c) Network Operation Centre (NOC);
d) Security Operation Centre (SOC);
e) Forensic Lab;
f) DDoS Services;
g) 3rd Party Online Security Services.

Estimated cost of this solution will be approximately 200 million.

Human Resource:

Technical operations teams are required to run the I-Voting system once it is deployed. Operations are mainly categorized as follows:

a) Network administration,
b) Database administration,
c) Infrastructure development & maintenance,
d) Software development,
e) Information security,
f) 24/7 operations and
g) Project management.

Hiring of such resources is prerequisite for smooth operations of the system. It will cost approximately 200 million.

Disaster Recovery Site

To ensure business continuity, a disaster recovery site is essentially required to keep the system running in case of any disaster or outage at the primary site. For this purpose, nearly same level of infrastructure and other resources are required at the disaster recovery site as in primary site. This include data center infrastructure, hardware and software, networking, information security systems, physical security, human resource (optional) etc.

REPORT OF THE LEGAL COMMITTEE ON OVERSEAS VOTING

The Legal Committee has drafted following vital legal amendments that need to be addressed during legislations are as under:

Existing Laws	Proposed Amendments	Rationale of Legislation before Incorporation of Electronic Voting Machine
Chapter V "CONDUCT OF ELECTIONS TO THE ASSEMBLIES"		
94. Voting by Overseas Pakistanis.— (1) Notwithstanding anything contained in this Act or rules made thereunder, the Commission shall with the technical assistance of National Database and Registration Authority (NADRA), any other authority or agency, enable overseas Pakistanis, in prescribed manner, subject to secrecy and security, to exercise their right to vote during general elections in Pakistan. (2) In this section, 'Overseas Pakistani' means a citizen of Pakistan under the Pakistan Citizenship Act, 1951 (II of 1951) or holder of National Identity Card for Overseas Pakistanis under the National Database and Registration Authority ordinance, 2000 (VIII of 2000) who is working or residing abroad permanently or temporarily for not less than six months.		The amendment in Section 94 does not expressly prescribe any manner or mode of voting by overseas Pakistanis subject to secrecy and security. The Election Commission of Pakistan after conducting pilot projects in terms of Section 94 of the Elections, Act 2017 submitted its report to the Parliament. However, nothing has been heard about the fate of the report. In absence of any legislation providing any mode of voting, it will not be possible for Election Commission of Pakistan to enable overseas Pakistanis to vote.

BIBLIOGRAPHY

Bibliography of specialist resources consulted in producing this report:

1. Secretariat, Commonwealth. Cybersecurity for Elections: A Commonwealth Guide on Best Practice. https://thecommonwealth.org/sites/default/files/inline/Cybersecurity_for_Elections_PDF_0.pdf.
2. Consultancy for the Analysis, Design, and Implementation of Internet Voting for Overseas Pakistanis. Minsait Report for Ministry of Information, Technology & Telecommunications, https://www.ecp.gov.pk/documents/reports/Final%20report%20by%20Minsait%20Final.pdf.
3. Edgeworth, Linda. Best Practices and Pitfalls in the Procurement Of New Technologies for Elections. 2008, https://www.ifes.org/sites/default/files/best_practices_and_pitfalls_in_the_procurement_of_new_technologies_for_elections.pdf.
4. Findings and Assessment Report of Internet Voting Task Force (IVTF) on Voting Rights of Overseas Pakistanis . 2018, https://www.ecp.gov.pk/ivoting/IVTF%20Report%20Executive%20Version%201.5%20Final.pdf.
5. Handbook For the Observation of New Voting Technologies. OSCE, https://www.osce.org/files/f/documents/0/6/104939.pdf.
6. International Electoral Standards Guidelines for Reviewing the Legal Framework of Elections. International IDEA, https://www.idea.int/sites/default/files/publications/international-electoral-standards-guidelines-for-reviewing-the-legal-framework-of-elections.pdf.
7. Schmidt, Adam. Application of Election Technology: Considerations for Election Administrators, Practitioners and Policy Makers. ifes.org/sites/default/files/application_of_election_technology.pdf.
8. "Shared Security, Shared Elections: Best Practices for the Prevention of Electoral Violence - World." Relief Web, https://reliefweb.int/report/world/shared-security-shared-elections-best-practices-prevention-electoral-violence.
9. Technology In Elections. https://www.eac.gov/sites/default/files/eac_assets/1/6/EMG_chapt_17_august_26_2010.pdf.
10. Yard, Michael. Direct Democracy: Progress and Pitfalls of Election Technology. https://www.ifes.org/sites/default/files/20111026_direct_democracy_progress_and_pitfalls_election_technology_yard_0.pdf.
11. Introducing Electronic Voting: Essential Considerations (https://www.idea.int/sites/default/files/publications/introducing-electronic-voting.pdf)
12. Challenges & Opportunities for the implementation of e- voting in Nigeria. (https://www.eces.eu/en/posts/evoting-nigeria)
13. https://www12.senado.leg.br/radio/1/noticia/2020/11/16/tse-avalia-voto-online-ou-por-celular-para-eleicoes-de-2022
14. https://www.jagranjosh.com/general-knowledge/cost-and-place-of-manufacturing-of-evm-in-india-1555398297-1
15. Election Commission looks to develop mobile voting technology to track down 'Lost Votes'. https://government.economictimes.indiatimes.com/news/digital-india/election-commission-looks-to-develop-mobile-voting-technology-to-track-down-lost-votes/74171792

Annex-A

F. No. 3(2)/2021-IT
ELECTION COMMISSION OF PAKISTAN
****

Secretariat,
Constitution Avenue, G-5/2,
Islamabad, the 23rd November, 2021

O R D E R

The Hon'ble Chief Election Commissioner of Pakistan is pleased to re-constitute the Electronic Voting Machine (EVM) Technical Committee under the chairmanship of Secretary ECP. The Committee will inspect the feasibility of EVM for their usage in upcoming General Elections with the following mandate as amended below:-

(i) To determine the international standards, best practices, and technologies that are to be employed in the election process;

- Electronic Voting Machine
- Biometric Verification System

(ii) To define processes and procedure for the employment of EVM;
(iii) To define the exact scope of work related to EVM;
(iv) To define the policy, process and procedures for the acquisition of EVMs ensuring that best international standards are followed;
(v) To hire the services of third party audit firm to prepare specification for proposed solution, develop mechanism and procedure for acquisition, implementation and testing of EVM in Pakistan as per best practice;
(vi) To determine objectively from time to time whether the usage of EVM is possible within the stringent timelines before GE-2023 and also highlight to all stakeholders for its implementation;
(vii) To prepare Expression of Interest (EOI)/ Request for Proposal (RFP) in the light of legal framework and as required by PPRA rules;
(viii) To examine and analyze any future enabling requirements as and when needed;
(ix) To assess any activity / process with the assistance of 3rd party audit expert entity, if and when required.

2. The composition of the EVM Committee is as under:-

1)	Secretary	Chairman
2)	Special Secretary	Member
3)	Additional Secretary (Admn)	Member
4)	Director General (IT)	Member
5)	Additional Director General (Elec-I)	Member
6)	Additional Director General (Elec-II)	Member
7)	Additional Director General (Law)	Member
8)	Additional Director General (Admn)	Member
9)	Director (Electoral Rolls)	Member
9)	Deputy Director (Software)	Member/Secretary
10)	Dr. Syed Taha Ali, Assistant Professor, NUST	Co-opted Member
11)	Dr. Syed Ahmed Pasha, Assistant Professor, Air University	Co-opted Member
12)	Dr. Basit Shahzad, Dean, Faculty of Engineering & CS, NUML	Co-opted Member

3. The Committee will prepare draft Evaluation Report of Electronic Voting Machine along with recommendations. The report of the Committee will be placed before the Hon'ble Election Commission. In addition, sub-committees may be formulated as and need basis particularly focusing on pure technical side of the EVM.

4. The Hon'ble Chief Election Commissioner of Pakistan may modify the composition of the Committee or pass any other order to its mandate at any time.

By the Order of Hon'ble Chief Election Commissioner of Pakistan.

(Fahad Hussain Farooqi)
Deputy Director (Software)

F. No. 3(2)/2021-IT
ELECTION COMMISSION OF PAKISTAN
****

Secretariat,
Constitution Avenue, G-5/2,
Islamabad, the 7th December, 2021

O R D E R

In partial modification of this office order of even number dated 29th November 2021, the Hon'ble Chief Election Commissioner of Pakistan is pleased to rename the Electronic Voting Machine (EVM) Technical Committee as Electronic Voting Machine (EVM) and Overseas Voting Technical Committee with an additional mandate of Overseas Voting solution under the chairmanship of Secretary ECP. The Committee will inspect the feasibility of EVM and Overseas Voting for their usage in upcoming General Elections with the following mandate as amended below:-

	Mandate	Responsibility
(i)	To determine the international standards, best practices, and technologies that are to be employed in the election process; o Electronic Voting Machine o Biometric Verification System o Implementation of Overseas Voting solution	PMU, I.T and Election Wings
(ii)	To define processes and procedure for the employment of EVM and Overseas Voting solution;	PMU, I.T and Election Wings
(iii)	To define the exact scope of work related to EVM and Overseas Voting solution;	PMU, I.T and Election Wings
(iv)	To define the policy, process and procedures for the implementation of Overseas Voting solution and acquisition of EVMs technologies and its implementation ensuring that best practices and international standards are followed;	PMU, I.T, Election Wings and MoST
(v)	To hire the services of third party audit firm to prepare specification for proposed solution, develop mechanism and procedure for acquisition, implementation and testing of EVM and Overseas Voting solution in Pakistan as per best practice;	PMU, I.T and Election Wings
(vi)	To determine objectively from time to time whether the implementation of Overseas Voting solution and usage of EVM is possible within the stringent timelines before GE-2023 and also highlight to all stakeholders for its implementation;	PMU, I.T and Election Wings
(vii)	To prepare Expression of Interest (EOI)/ Request for Proposal (RFP) in the light of legal framework and as required by PPRA rules;	PMU, I.T, Law, Budget, Admn and Election Wings
(viii)	To examine and analyze any future enabling requirements as and when needed;	EVM Technical Committee
(ix)	To assess any activity / process with the assistance of 3rd party audit expert entity, if and when required.	EVM Technical Committee

2. The composition of the EVM Committee is as under:-

1)	Secretary	Chairman
2)	Special Secretary	Member
3)	Additional Secretary (Admn)	Member
4)	Director General (IT)	Member
5)	Additional Director General (Elec-I)	Member
6)	Additional Director General (Elec-II)	Member
7)	Additional Director General (Law)	Member
8)	Additional Director General (Admn)	Member
9)	Director (Electoral Rolls)	Member
9)	Deputy Director (Software)	Member/Secretary
10)	Dr. Syed Taha Ali, Assistant Professor, NUST	Co-opted Member
11)	Dr. Syed Ahmed Pasha, Assistant Professor, Air University	Co-opted Member
12)	Dr. Basit Shahzad, Dean, Faculty of Engineering & CS, NUML	Co-opted Member

3. The Committee will prepare draft Evaluation Report of Electronic Voting Machine along with recommendations. The report of the Committee will be placed before the Hon'ble Election Commission. In addition, sub-committees may be formulated as and need basis particularly focusing on pure technical side of the EVM.

4. The Hon'ble Chief Election Commissioner of Pakistan may modify the composition of the Committee or pass any other order to its mandate at any time.

By the Order of Hon'ble Chief Election Commissioner of Pakistan.

(Fahad Hussain Farooqi)
Deputy Director (Software)

F. No. 1(2)/2021-ADG(Budget)
ELECTION COMMISSION OF PAKISTAN
****

Secretariat,
Constitution Avenue, G-5/2,
Islamabad, the 19th November, 2021

O R D E R

It is circulated that the Hon'ble Chief Election Commissioner is pleased to constitute Committee with the mandate to examine, study and analyze financial implications of the Electronic Voting Machines and I-Voting System as well as other election related matters. The Committee is also tasked to propose cost effective solution in terms of piloting the project as well as usage of actual machines / i-voting system during the forthcoming General Elections-2023.

2. The composition of Committee is as under:-

I.	Additional Secretary (Admn), ECP Sectt:	Convener
II.	Additional Director General (Elec-I), ECP Sectt:	Member
III.	Additional Director General (Budget), ECP Sectt:	Member
IV.	Director (MIS), ECP Sectt:	Member
V.	Deputy Director (Budget), ECP Sectt:	Member
VI.	Deputy Director (GS), ECP Sectt:	Member/Secretary

3. The Committee may co-opt any other officer for assistance towards performance of its functions.

By order of the Hon'ble Chief Election Commissioner.

Addl: Director General (Budget)

F. No. 23(34)/2021-Law
ELECTION COMMISSION OF PAKISTAN
****

Secretariat,
Constitution Avenue, G-5/2,
Islamabad, the 19th November, 2021

O R D E R

For reviewing the bills passed in the Joint Session of the Parliament on 17th November, 2021, regarding use of Electronic Voting Machines (EVMs) in the forthcoming General Elections; on right of vote to overseas Pakistanis with other amendments, and their repercussions, applicability, future legal challenges, if any, alongwith recommendations with regard to amendments in the relevant law and Rules, the Hon'ble Election Commission has constituted a Committee comprising following officers of the Commission:-

i.	Muhammad Arshad, DG (Law)	Chairman
ii.	Zafar Iqbal Hussain, Special Secretary	Member
iii.	Muhammad Khizer Aziz, DG (IT)	Member
iv.	Khurram Shahzad, ADG (Law)	Member
v.	Asif Ali Yasin, Director (ER)	Member
vi.	Saima Tariq Janjuha, DD (Law)	Member/Secretary
vii.	Adil Kahlon, Legal Consultant	Member
viii.	Muhammad Amjad, AD (Law)	Member

3. The Chairman of the Committee has mandate to substitute or add other Members in the Committee for assistance of the Committee at any stage.

By order of the Hon'ble Election Commission of Pakistan.

(Saima Tariq Janjuha)
Deputy Director (Law)

Annex-B
2

REGISTERED No. M - 302
L.-7646

The Gazette of Pakistan

EXTRAORDINARY
PUBLISHED BY AUTHORITY

ISLAMABAD, SATURDAY, DECEMBER 4, 2021

PART I

Acts, Ordinances, President's Orders and Regulations

NATIONAL ASSEMBLY SECRETARIAT

Islamabad, the 3rd December, 2021

No. F. 22(32)/2021-Legis.—The following Act of *Majlis-e-Shoora* (Parliament) received the assent of the President on the 2nd December, 2021 is hereby published for general information:—

ACT NO. LV OF 2021

AN

ACT

further to amend the Elections Act, 2017.

WHEREAS it is expedient further to amend the Elections Act, 2017 (XXXIII of 2017) in the manner hereinafter appearing;

It is hereby enacted as follows:—

Price: Rs. 5.00

[1739(2021)/Ex. Gaz.]

Scanned with CamScanner

1. **Short title and commencement.**—(1) This Act shall be called the Elections (Amendment) Act, 2021.

(2) It shall come into force at once.

2. **Amendment in section 94, Act XXXIII of 2017.**—In the Elections Act, 2017 (XXXIII of 2017), hereinafter referred to as the said Act, in section 94, for sub-section (1), the following shall be substituted, namely:—

"(1) Notwithstanding anything contained in this Act or rules made thereunder, the Commission shall, with the technical assistance of National Database and Registration Authority (NADRA), any other authority or agency, enable overseas Pakistanis, in prescribed manner, subject to secrecy and security, to exercise their right to vote during general elections in Pakistan.".

3. **Amendment in section 103, Act XXXIII of 2017.**— In the said Act, for section 103, the following shall be substituted, namely:—

"**103. Electronic voting.**—Notwithstanding anything contained in this Act or rules made thereunder, the Commission shall, with the technical assistance of any authority, or agency, procure and use in prescribed manner, subject to secrecy and security, stand-alone electronic voting machines in general elections in Pakistan.".

TAHIR HUSSAIN,
Secretary.

PRINTED BY THE MANAGER, PRINTING CORPORATION OF PAKISTAN PRESS, ISLAMABAD.
PUBLISHED BY THE DEPUTY CONTROLLER, STATIONERY & FORMS, UNIVERSITY ROAD, KARACHI.

Scanned with CamScanner

Gantt Chart

WBS #	TASK TITLE	Dependency	DURATION (working days)
1	**STEERING COMMITTEE FOR EVM PROJECT**		
1.1	Strategize and oversee technical activities		
1.2	Present detailed vision for EVMs in Pakistan		10
1.3	Draft detailed Roadmap for project		21
1.4	Constitute relevant teams to undertake key activities		15
1.5	Engage partners and stakeholders to assist with ECP tasks		
1.6	Draft EOI/RFP/TOR for Hiring Third Part Audit Firm		45
1.7	Prepare Activities Plan for Third Party Audit/Certification of EVM		45
1.8	Issue periodic progress reports to stakeholders	1.5	
1.9	Benchmark for Evaluation – What are we evaluating against?		10
1.10	High level analysis of various EVMs used in other countries		10
1.11	Investigate application of new EVM security technologies to Pakistan	1.2	7
1.12	Compile list of best practices applicable to Pakistan	1.2	7
1.13	Evaluation of already procured Smartmatic Machines		7
1.14	Evaluation of MoST machines		7
1.15	Comparative Analysis	1.10, 1.13, 1.14	5

WBS #	TASK TITLE	Dependency	DURATION (working days)
1.16	Map security properties of EVMs to threat model for Pakistan	1.12	5
1.17	Vulnerability Analysis of Available EVMs		120
1.18	Comparative Analysis of Popular EVM Models for Pakistan		120
1.19	Voter Verification Mechanisms		120
1.20	Deployment Study for Risk Limiting Audits in Pakistan		120
1.21	EVMs in Pakistan: Specifications and Requirements		120
1.22	Prototype EVM		120
1.23	Pilot Studies: Condut Multi Pilot on new EVMs		120
1.24	Detailed analysis of components and supply chain	1.15	120
1.25	Present recommendations, feasibility report and way forward	1.16, 1.17	120
1.26	Prepare EVM requirements and Final Technical Specifications	1.18	120
1.27	Share and get feedback from stakeholders on requirements/technical specifications	1.19	120
1A	**SETUP RESEARCH & DEVLOPMENT WING**		**140**
1A.1	Structuring and Team Building		140
1A.2	Initiate Hiring (First Round and Second Round)		140
1A.3	Setup Working Space and Procure Essential Equipment		140
1A.4	Orientation and Training of New Staff		140
1A.5	Create Activity Plan in Consultation with Stakeholders/Donors		140

WBS #	TASK TITLE	Dependency	DURATION (working days)
1A.5.1	Devise Strategy to engage with Donor Bodies (UN, IFES etc)		140
1A.5.2	Devise Strategy to engage with Research Partners (PIDE, MoST etc)		140
1A.5.3	Call for Working Groups and Public Requests for Comments		140
1A.5.4	Conduct Sessions Regularly		140
1A.5.5	Strategy and Roadmap to Engage with other Election Management Bodies, Observation Trips and Technology Transfer		140
1A.5.6	Issue detailed roadmap for ecosystem for EVMs and for overseas voting		140
2	**HIRING OF THIRD PARTY TECHNICAL AUDIT FIRM FOR EVM**		**120**
2.1	Appointment and designation of RFP/tender review staff		21
2.2	Estimation and availability of Budget		44
2.3	Preparing RFP/Tender document for Hiring Audit Firm Specialized in Electronic Voting Machine/Electronic Voting		12
2.4	Preparation of RFP/tender document		44
2.5	Preparation of evaluation procedure		34
2.6	Publication of RFP/tender		0
2.7	Pre-bid Meetings		34
2.8	Answer to bidders questions		34
2.9	Receiving and opening proposals		0

WBS #	TASK TITLE	Dependency	DURATION (working days)
2.10	Review and technical evaluation of proposals		24
2.11	Financial evaluation of proposals		10
2.12	Selection of best bidder		0
2.13	Contract Signing		0
3	**EVM PROCUREMENT PHASE**		**109**
3.1	Legal framework review and adjustments		
3.2	Generation and aproval of final EVM Specs		
3.3	Appointment and designation of tender review staff		
3.4	Estimation and availability of Budget		
3.5	Preparation of tender document		
3.6	Preparation of evaluation procedure		
3.7	Vetting of Tender from Stakeholders		
3.8	Publication of tender		
3.9	Pre-bid Meetings		
3.10	Answer to bidders questions		
3.11	Receiving and opening proposals		
3.12	Review and technical evaluation of proposals		
3.13	Financial evaluation of proposals		
3.14	Presentation and evaluation of prototypes from selected bidders		
3.15	Selection of best bidder		

WBS #	TASK TITLE	Dependency	DURATION (working days)
3.16	Contract Signing		0
4	**PROJECT MANAGEMENT UNIT**		**41**
4.1	Constitution of Project Management Team		
4.2	Project Management Plan/Timelines/Work Breakdown Structure		
4.2.1	Create Work Breakdown Structure		
4.2.2	Review Work Breakdown Structure with Project Team		
4.2.3	Create project activities list and resources assignments		
4.2.4	Review and adjust final activities for final schedule		
4.2.5	Schedule approved and Baseline Set		
4.2.6	Review and Adjust Project Management Plan		
4.3	Resource Planning		
4.3.1	Create organisational chart and RACI (Responsibility assignment matrix)		
4.3.2	Create Communication management plan		
4.4	Risk Management Plan		
4.4.1	Identify risks and mitigation plan		
4.4.2	Review risks and mitigation plan with team		
4.4.3	Create Risk log		
4.5	Quality Control and Assurance Plan		
4.5.1	Define Acceptance Criteria and Quality Metrics		
4.5.2	Create Quality Metrics Scorecard		

WBS #	TASK TITLE	Dependency	DURATION (working days)
4.6	Monitoring and Controlling		
4.6.1	Schedule Weekly Status Meeting		
4.6.2	Scehdule Executive Project Status Meeting		
5	**DESIGN/DEVELOPMENT PHASE**		**130**
5.1	Requirements gathering and refinement	3	10
5.2	Industrialization of machine prototypes	5.1	20
5.2.1	Ideation and final concept development	5.2	45
5.2.2	Design and production of final hardware prototype	5.2.1	45
5.2.3	Presentation of prototype and final hardware acceptance	5.2.2	10
5.3	Firmware and Software development (development and quality assurance)	5.2.3	70
5.4	Massive tests	5.3	21
5.5	Presentation of prototype and final hardware and software acceptance	5.4	9
6	**HARDWARE PRODUCTION PHASE FOR PILOTING (SMALL SCALE)**		**60**
6.1	Procurement of components for hardware production	5.5	25
6.2	Small Scale Production of EVM devices for Piloting	6.1	15
6.3	Shipping and delivery	6.2	20
7	**TESTING PHASE FOR PILOTING (SMALL SCALE)**		**117**
7.1	Solution Acceptance Testing	6.3	15

WBS #	TASK TITLE	Dependency	DURATION (working days)
7.1.1	Source Code Review and demonstrations of EVM to Stakeholders		10
7.1.2	Acceptance of EVM by Stakeholders (Trust Building Measures)		5
7.2	Preparation for Actual Pilot of EVM in Multiple Bye-Elections	7.1	**10**
7.2.1	Mandate/ Purpose of Pilot Testing and Benchmarks		10
7.2.2	Identification of Evaluation criteria and observation benchmark		10
7.2.3	Preparation of Team of Researchers and oversight actors		10
7.3	Constitution of EVM Inspection Team	7.1	5
7.3.1	Advisors from Industry/Academia		5
7.3.2	IT & Admin personnel from ECP		5
7.3.3	EVM Technical Experts from Vendor/3rd Party Audit Firm		5
7.4	Preliminary Inspection	7.3	10
7.4.1	Storage condition		15
7.4.2	Counting of Equipment		15
7.5	Detail Inspection	7.3	10
7.5.1	Battery/Power		15
7.5.2	O/S Firmware		15
7.5.3	EVM Software/Firmware/Election Management Software Version Check		15
7.5.4	Security and Vulnerability Testing of EVM		15
7.6	Preparation of logistics and security plan and execution	7.5	10
7.7	Preparation of Technology Transfer/ Training Plan	7.1	10

WBS #	TASK TITLE	Dependency	DURATION (working days)
7.8	Technology Transfer Training	7.7	21
7.8.1	Election Management Software		60
7.8.2	Ballot Preparation		60
7.8.3	Machine Preparation including Time Synchronization		60
7.8.4	Bulk loading and Data Extraction		60
7.8.5	Reporting		60
7.8.6	EVM Operation		60
7.8.7	EVM Troubleshooting and Repair		60
7.8.8	System and Software Application e.t.c.		60
7.9	Identification of Electoral Area/Constituency	7.2	7
7.10	Targeted Public Outreach Plan	7.9	27
7.10.1	Social Media		27
7.10.2	Print and Electronic Media		27
7.10.3	Awareness session for public, media and other stakeholders		27
7.10.4	Development of Leaflets		27
7.11	Execution of Public Outreach Plan	7.10	15
7.12	Preparation of required SOPs	7.2	15
7.13	Preparation of Electoral data	7.9	21
7.14	User Level Training	7.7	20
7.14.1	Appointment of Technical,Support and Operational Staff		20

WBS #	TASK TITLE	Dependency	DURATION (working days)
7.14.2	Training of Polling staff		20
7.14.3	Training for Troubleshooting/Help desk staff		20
7.15	**Rollout of Pilot Project**	7.14, 7.6	**23**
7.16	Compilation of Post Election Observation Report of all stakeholders	7.15	15
7.17	Create report and recommendations on technical/ functional/procedural findings of EVM Piloting for incorporating in full scale implemetation	7.16	20
7.18	Implement pilot recommendations in final EVM Specification and design	7.17	20
8	**HARDWARE PRODUCTION PHASE (FULL SCALE)**		**100**
8.1	Procurement of components for hardware production	7	30
8.2	Full Scale Production of EVM devices for Election	8.1	45
8.3	Shipping and delivery	8.2	22
9	**ELECTION READINESS PHASE**		**180**
9.1	Warehousing Set up	1.19	80
9.1.1	Warehouse requirements and design		45
9.1.2	Warehouse Set up		100
9.1.3	Warehouse Manpower Recruiting and Training		90
9.1.4	Warehouse Consumables and Supplies Procurement		49

WBS #	TASK TITLE	Dependency	DURATION (working days)
9.2	Hiring/Appointment and Training of Technical,Support and Operational Staff	1.19	196
9.3	Preparation of Training Plan	7.1	23
9.4	EVM Readiness and final QA	8.3	44
9.4.1	Preparation of Electoral data		44
9.4.2	Configuration of EVM		44
9.4.3	Audit/Certification of EVM		44
9.4.4	Source Code Review and demonstrations of EVM to Stakeholders		44
9.4.5	Security and Vulnerability Testing of EVM		44
9.4.6	Acceptance of EVM by Stakeholders (Trust Building Measures)		44
9.5	Logistics and Distribution	9.4	21
9.6	Users Trainings	9.3	60
9.6.1	Training of Polling staff		50
9.6.2	Training for Troubleshooting/Help desk staff		50
9.6.3	Training of Technical Admininstrators on Election Management Software/EVM		50
9.7	Pre Election Audit	9.4	66
10	**ELECTION DAY**	**9**	**21**
10.1	Election Day support	9.7	21
11	**POST ELECTION AND PROJECT CLOSE PHASE**	**10**	**20**

WBS #	TASK TITLE	Dependency	DURATION (working days)
11.1	Reverse Logistics	10.1	20
11.2	Post Election Audit	11.1	20
11.3	Project Closure	11.2	20
12	**DIGITAL TRANSFORMATION EXECUTIVE PROGRAM: FROM MANUAL ELECTION TO VOTING WITH EVM (CHANGE MANAGEMENT)**	**3**	**314**
12.1	Capacity building on election deployments		88
12.2	Visiting election related customers		300
12.3	Touring developing installations		44
12.4	Touring manufacturing installations		44
12.5	Election project managements training		66
12.6	Analyse the organisational and team capabilities needed to support a digital-ready electoral body in a EVM enviroment		66
12.7	Develop personal, actionable plans to address the strategic, organisational and innovation-based opportunities you face transforming from manual to electronic elections		66
12.8	Acquire a concrete view of key strategic drivers of digital transformation with EVM		314
12.9	Learn about innovation capabilities of the EVM and to generate more insights on how to implement the technology		66

Roadmap: Electronic Voting Machines for Pakistan

Key Steps	Document	Objective	Dependencies	Research Questions to be Addressed in this Phase	Inputs	Output	Organization	Recommendations	Requirements	Estimated Duration	Timeline* **
1	**Threat Model for Electronic Voting Machines in Pakistan**	Precisely define baseline security requirements for EVMs in Pakistan	-	1. Describe the ecosystem of Pakistan's voting system - list key actors, processes, and data units 2. Describe current threats to the existing voting system 3. What are the key procedural and process inefficiencies and shortcomings? 4. Differentiate between procedural and technological resolutions to these threats	1. An investigation of failures and irregularities in General Elections of 2013 and 2018 2. Threat models for similar environments, e.g. India/Bangladesh/Africa n countries	Study clearly defines the threat model and inefficiencies in the electoral system in Pakistan that will be addressed by EVMs	**Lead:** ECP **Assisted by:** 1. election observer bodies (e.g. FAFEN) 2. extensive input from stakeholders via consultation	This document must include detailed process flows for attacks/threats that we hope to address using EVMs. For each attack, there must be a discussion on: 1. procedural remedies (if they exist) 2. how other countries have addressed these issues (if faced)	stakeholder consensus is essential for this report	2 months	0-2 months
2	**Vulnerability Analysis of Available EVMs**	To undertake a rigorous security analysis of the EVMs acquired from Smartmatic	-	Detailed analysis of available EVMs 1. security properties 2. international best practices 3. suitability for Pakistan 4. cost-benefit analysis	1. Detailed specifications document 2. Details of manufacturing and supply chain	Study gives a complete picture of pros and cons of Smartmatic EVMs	**Lead**: ECP R&D Wing	It would be instructive to pilot this EVM in small-scale elections if possible to assess usability and logistics.		2 months	0-2 months
3	**Comparative Analysis of Popular EVM Models for Pakistan**	Detailed comparison of popular EVM types across various metrics to judge suitability for local deployment	1	Popular EVM models for developing countries (India-button-press, Brazil-keypad, Iraq/Philippines-scanning) 1. Investigate security properties and vulnerabilities for each model. 2. Investigate on-ground operational requirements for each EVM model (transport, storage, handling, configuration, maintenance, etc.) 3. Conduct pilots for each model to measure usability. Pilots should be conducted in non-political elections (e.g. organizational polls, trade bodies, bar associations, etc.) Care must be taken to ensure statistically significant results. 4. Formulate dispute-resolution strategies for each model 5. Investigate legal framework for each model 6. Detailed cost-benefit analysis for each model (including overall costs for logistics, handling, manpower)	1. Specifications documents for each EVM type 2. Security analyses from research literature 3. Reports from existing pilots and deployments	Study gives stakeholders a comprehensive picture on pros and cons of each EVM type as well costing figures	**Lead:** ECP **Assisted by:** 1. research-intensive organizations (e.g. universities) 2. technical organizations (e.g. NITB)	Existing pilot studies and reports prepared inhouse by ECP are typically not of high quality, they lack rigorous security and statistical analysis. It is highly recommended they partner with a research organization for this exercise or train their staff in the required skills.		6 months	2-8 months
4	**Voter Verification Mechanisms**	Feasibility study of various options (biometrics, smart cards, CV techniques)	-	What are the false acceptance and false rejection rates of each of the voter verification technologies? How do these vary for the population of Pakistan? What is the relative cost of each of the options for voter	1. Specifications documents for each voter verification mechanism 2. Security analyses from research literature 3. Reports from existing pilots and deployments	Study gives stakeholders a comprehensive picture on pros and cons of each voter verification mechanism as well costing figures	Lead: ECP Assisted by: 1. research-intensive organizations (e.g. universities) 2. technical organizations (e.g. NITB)	There is extensive literature that explores access controls such as biometrics, smart cards, tokens etc		6 months	2-8 months

Annex-D

Key Steps	Document	Objective	Dependencies	Research Questions to be Addressed in this Phase	Inputs	Output	Organization	Recommendations	Requirements	Estimated Duration	Timeline* **
5	**Deployment Study for Risk Limiting Audits in Pakistan**	Investigate and adapt RLAs for local deployment	-	1. Pilot RLAs in existing polls (by-elections, LG polls, etc.) - multiple pilots for different RLA methodologies 2. Investigate on-ground operational requirements 3. Studies to investigate citizen mental models for RLAs 4. Formulate dispute-resolution strategies 5. Investigate legal framework	1. RLA schemes proposed for Indian EVMs	Document that serves as a guide for RLA inclusion in the electoral framework	**Lead:** ECP **Assisted by:** 1. research-intensive organizations (e.g. universities) 2. technical organizations (e.g. NITB)	Personnel will have to be trained to run RLAs and E2EV systems.		4 months	8-12 months
6	**Deployment Study for E2EV voting in Pakistan**	Investigate and adapt verifiable voting for local deployment	-	1. Pilot EVMs with verifiable voting in non-political settings (bar association polls, chambers of commerce, etc.) 2. Investigate on-ground operational requirements 3. Studies to investigate citizen mental models for verifiable voting systems 4. Formulate dispute-resolution strategies 5. Investigate legal framework 6. Trial different technical options for bulletin board - e.g. Internet-based bulletin board, SMS service, etc. 7. Trial different code visualization options - e.g. alphanumeric text, images, emojis, etc.	1. Develop or procure EVMs with verifiable voting capability specifically for this exercise	Study to examine feasibility of verifiable voting in a local setting, as well as measure verifiability rates, and check how citizens understand this technology and derive mental models	**Lead:** ECP **Assisted by:** 1. research-intensive organizations (e.g. universities) 2. technical organizations (e.g. NITB)	Prior research work on verifiable voting trials, measuring verifiability rates, and mental models can help with developing a template for this exercise but care must be taken to adapt for our own ground realities, e.g. language, culture, etc. If this exercise fails, e.g. if the verification rates are too low or the process is incomprehensible to voters, the system will need to be redesigned and the pilot conducted again		4 months	8-12 months
7	**EVMs in Pakistan: Specifications and Requirements**	Define technical and functional specifications and processess for EVMs to be deployed in Pakistan	[1] [2] [3][4]	This phase describes the proposed EVM 1. Map security properties of EVM to threat model [1] 2. Describe detailed technical and functional specifications of proposed EVM 3. Describe workflow and processes for deployment and elections 4. Describe workflow and processes for storage, maintainence and handling 5. Describe security checks and audit processes 6. Include measures to incorporate future technology (e.g. citizen smart cards) 7. Describe RLA and verification processes 8. Propose dispute resolution strategies 9. Propose changes to legal framework	[1] [2] [3] [4] Research Literature	First iteration on technical Specifications including functional requirements, non-functional requirements hardware and software requirements	**Lead:** ECP **Assisted by:** 1. research-intensive organizations (e.g. universities) 2. technical organizations (e.g. NITB)	This documentation must be of high quality and conform to appropriate international standards for technical documentation	stakeholder consensus is essential for this report	3 months	8-11 months

Annex-D

Key Steps	Document	Objective	Dependencies	Research Questions to be Addressed in this Phase	Inputs	Output	Organization	Recommendations	Requirements	Estimated Duration	Timeline* **
8	**Prototype EVM**	Develop prototype EVM	[5]	Develop prototype EVM for pilot purposes and also address further questions: 1. Derive precise costing figures for manufacturing/procuring EVMs 2. Document production supply chain and procurement/manufacturing processes 3. Are there security threats in the supply chain? 3. Can the EVM design be modified to further improve security and/or reduce costs without impacting functionality? 4. Devise adequate Quality Assurance checks and processes	[1] [2] [3] [4] Research Literature	Report evaluating the prototype and whether the goals were met or not	**Lead:** ECP **Assisted by:** 1. research-intensive organizations (e.g. universities) 2. technical organizations with small-scale manufacturing capability (e.g. NIE)			4 months	11-15 months
9	**Pilot Studies**	Conduct multple pilots using new EVMs	[6]	Pilot the proposed EVM in non-political and political settings: 1. Collect feedback on usability 2. Record performance of these machines in the field 3. Observe process flow and procedures with a view to proposing improvements 4. Modify EVMs or processes in response to feedback from 1, 2, 3 5. Undertake multiple pilots in rural and urban areas to derive statistically significant results which reflect Pakistan's diverse population.	The pilot must be evaluated on multiple dimensions such as technical, social, legal, usability, process efficiency. For this formal observation of the pilots is necessary, so that by the end there is enough data to decide on the outcome	Series of pilot processes to fine-tune EVM design and workflow and operational procedures for the field	**Lead:** ECP **Assisted by:** 1. research-intensive organizations (e.g. universities) 2. technical organizations (e.g. NITB)		Stakeholders must be regularly briefed about the outcomes of these trials, ideally at every iteration	2 months	15-17 months
10	**Feedback and Improvement**	Incorporate chnages to rectify the issues identified in the EVMs in the first pilot before going into production	[7] [8] [9] [10]	1. What were the limitations and weaknesses evident in the electronic voting machine and associated processes? 2. What was the end users that is the voters perspective?	Survey consisting of diverse stakeholders, public call for comments, engaging with academia, media and collecting as much feedback as possible	A document that defines the changes that need to be made in the EVM to overcome the issues faced in the first pilot	Lead: ECP Assisted by: 1. research-intensive organizations (e.g. universities) 2. technical organizations (e.g. NITB)	Constant feedback cyclical process		3 months	17-20 month
11	**Second Round of Pilots**	To iron out any remaining issues after the first round of improvements made according to the feedback received	[7] [8] [9] [10] [11]	1.What are the remaining limitations, weaknesses in the system? 2. Do we need to go for another round of change in specifications? 3. What are the outstanding challenges that can be left for later updation	the result of first pilot, the documents detailing the changes made, further observation from second pilot	Series of pilot processes to fine-tune EVM design and workflow and operational procedures for the field	**Lead:** ECP **Assisted by:** 1. research-intensive organizations (e.g. universities) 2. technical organizations (e.g. NITB)		Stakeholders must be regularly briefed about the outcomes of these trials, ideally at every iteration	2 months	20-22 months
12	Finalized specifications	**Procurement**						Issue detailed roadmap for ecosystem for EVMs and for overseas voting		-	-

*Many of these actiivties are independent of each other and maybe undertaken in parallel.

Annex-E

David Jefferson

Computer Scientist, Lawrence Livermore National Laboratory Board of Directors, Verified Voting Foundation Board of Directors, California Voter Foundation
d_jefferson@yahoo.com

If I can shop and bank online, why can't I vote online?

1. Introduction

Many people look forward to the introduction of some form of Internet voting in public elections. They like the idea of voting online, all electronically, from their own personal computers or mobile devices, whenever and from wherever they wish. Proponents argue that Internet voting would offer greater speed and convenience, particularly for overseas and military voters, and might offer new possibilities for disabled voters as well. Some believe that voter participation would increase, particularly among young people because of their familiarity and comfort with online media. The idea of convenient voting any time from any computer or mobile device has wide appeal.

However, computer and network security experts are virtually unanimous in agreement that online voting is an exceedingly dangerous threat to the integrity of U.S. elections. There is no known way to guarantee that the security, privacy, and transparency requirements for online elections can all be met with any practical technology, not now and not in the foreseeable future. Anyone from a disaffected misfit individual to apolitical partisan to a foreign national intelligence agency can remotely attack an online election, modifying or filtering ballots in ways that are undetectable and uncorrectable, or just disrupting the election and creating havoc. There are a host attack methods that can be used singly or in combination. In the cyber security world today almost all of the advantages are with attackers, and any of these attacks can result in the wrong persons being elected, or initiatives wrongly passed or rejected.

Nonetheless, enthusiasts point to the fact that millions of people regularly bank and shop online every day without apparent problems. They are often convinced that online voting can be similarly easy by the fact that a voting transaction superficially resembles an ecommerce transaction. You connect your browser to the appropriate site, authenticate yourself, make your choices with touches or a mouse click, then click on a final confirmation button, and you are done! And since all of the potential attacks on online voting alluded to above apply equally to online shopping and banking,

[1] *Analyses and views stated herein are drawn from my expertise as a computer scientist working on national security applications and are my own. They are not to be ascribed to my employer, Lawrence Livermore National Laboratory, which takes no position on these issues*

and they seem secure enough, what is the difference? It is thus natural to ask, *"If it is safe to do my banking and shopping online, why can't I vote online?"*

This is a very fair question, and it deserves a careful answer because the reasons are not obvious. Unfortunately it requires substantial development to explain fully. But briefly, the answer is in two-parts:

1 It is *not* actually safe to conduct ecommerce transactions online. It is in fact very risky, and more so every day. Essentially all the same risks, and then some, apply to online voting.

2 The security, privacy, transparency and other requirements for voting are structurally different from, and much more stringent than, those for ecommerce transactions. Even if ecommerce transactions *were* safe, the security technology underpinning them do not suffice for voting. Voting security and privacy requirements are unique in ways that have no analog in the ecommerce world.

The rest of this essay expands upon these two points.

2. Ecommerce transactions are not, in fact, "safe"

Why do security experts say that ecommerce transactions are not safe when millions of people do them every day, mostly without problems? The question needs to be refined: "Safe for whom?" and "What degree of safety is required"?

2.1 Online threats

Ecommerce transactions may be relatively safe for consumers, but they certainly are not safe for financial institutions or merchants. Banks, credit card companies, and online merchants lose billions of dollars a year in online transaction fraud despite huge investments in fraud prevention and recovery. Consumers have the illusion that ecommerce transactions are safe because merchants and banks don't hold them financially responsible for fraudulent transactions when they are innocent victims. Instead businesses absorb and redistribute the losses silently, passing them on in the invisible forms of higher prices, fees, and interest rates. Businesses know that if consumers had to accept online losses personally, most online commerce would collapse, so they routinely hide the losses. It is a sound business strategy.

But ecommerce fraud is very real, and many fraud techniques that are directly applicable to online voting. A common pattern starts with theft of *credentials*, e.g. names, account numbers, credit card numbers, passwords, or answers to personal challenge questions. The theft can be initiated through phishing scams, drive-by malware installation, key loggers, data stolen from hacking into major commercial establishments, or other means, and such tricks can just as easily be used to steal online voting credentials.

Recently a malware family named Zeus has been in the news.[4] It installs malware on PCs that is specifically designed to wait until you connect to your bank and then it steals your bank account number and password as you type it into your browser. The Zeus botmasters use those credentials to transfer money out of your accounts and to fake your online financial statements to hide the theft from you for as long as possible.

It makes no difference that you have a "secure" connection to your banking site because the malware operates inside your own computer and it can see and modify everything you type while it is still in the clear, before it is encrypted for secure transmission. There are now illicit businesses that help people set up Zeus botnets, or rent time on one already created. Unfortunately most peopleare completely unaware of such online threats.

Zeus exemplifies what could easily happen if online voting becomes widespread. Eventually someone, perhaps a partisan political operative or a foreign intelligence agency, will deploy a similar botnet to infect perhaps hundreds of thousands of voters' computers and steal their credentials or modify their votes invisibly, right as they are being transmitted. Again, having a "secure" connection to the remote election server will make no difference at all. There is generally no effective way to prevent such an attack, and no effective recovery. Banks, online merchants, and high tech companies that do business online have huge security budgets to defend themselves against cyber attacks, and even so they are frequently victimized. If these organizations with such great expertise and capability in computer and network security can be successfully attacked, then no voting system vendor or local election administration has any realistic chance of successfully defending against similar threats.

The cost to an attacker of conducting a remote online attack has declined drastically over the last few years as various programming templates, libraries, and toolkits for malware production have become widely available. One recent study demonstrated that it was possible to duplicate even very sophisticated attack vectors like Stuxnet, the malware that did great damage to Iranian nuclear centrifuge facilities, in about two months time for under $20,000.[6] We are now in a very different threat environment than we were even a few years ago.

2.2 Degrees of safety required for ecommerce and voting

What level of security is sufficient to protect elections? The scale of fraud that ecommerce and electoral systems can tolerate are very different. In the ecommerce world if one out of every thousand transactions is lost or fraudulent it is not really a vital concern. Banks, merchants and

[7]

purchasers routinely deal with online revenue losses over 10 times higher than that , and have manytools to deal with the loss. As unjust and frustrating as it may be, no catastrophic consequence ensues from a small ecommerce fraud rate.

But in the voting world we are all familiar with the cases where, within about one decade, a senator, a governor, and a president were all elected by margins much smaller than one vote in a thousand. Election outcomes are thus *very sensitive to small errors or frauds* in a way that ecommerce systems simply are not. Small changes in vote totals sometimes have national or global consequences. Election security is thus a matter of *national security*, and the security standards have to be designed to reliably prevent, detect, and correct even very small problems and attacks. That level of security and reliability is not needed and not cost effective for ecommerce systems.

3. Voting security, privacy, and transparency requirements are structurally different from those for ecommerce transactions

The second point of our argument is that the security, secrecy, and transparency requirements for online voting transactions are structurally very different from, and generally much stricter than, those for ecommerce transactions. The security mechanisms that make ecommerce transactions relatively safe (for consumers at least) are not sufficient to guarantee the safety of online voting.

3.1 Auditability, detectability and correct ability of problems

The first major distinction is that we can at least eventually *detect* ecommerce errors and fraud, but we may never know about online election fraud. In the ecommerce world problems are reliably detected because of such practices as receipts, double entry bookkeeping, and financial audit records kept by both sides of every major transaction. Even in the absence of those practices it will be detected eventually when some transaction that should succeed unexpectedly fails because an account is out of money.

But in most kinds of online elections there is nothing that corresponds to receipts, double entry bookkeeping, or meaningful audit trail information. Security experts routinely call for an independent, end-to-end audit trail that can be used to verify that the electronic ballots received by election officials are identical to those the voters sent, and that none were forged, lost, or modified in transit. But the only reliable way to accomplish this with current technology is for voters to send verified paper copies of their voted ballots back to their local election officials, and for the officials to use those copies in a formal risk limiting audit procedure.[9] That would actually solve most of the security problems associated with online voting (though not the privacy problems). However, most advocates of Internet voting oppose such a paper-based audit requirement because the additional burden on voters to mail back paper copies of their ballots is essentially equivalent to sending an ordinary paper absentee ballot, which is what most of them wish to avoid. Yet without a meaningful end-to-end audit trail a well-constructed attack may lead to the attackers' choice of candidates being elected and *there may well be no way to know that anything happened at all*.

Even if there is suspicion of a problem there will be no way to prove or disprove it. Because of ballot secrecy, even if there were strong evidence that *particular* persons cast illegal ballots, or their ballots were tampered with, officials cannot know *which* ballots to remove from the count. Hence, fraudulent online voting will often be *undetectable,* and almost certainly *uncorrectable* even if detected.

3.2 Structural differences between the security requirements for voting and ecommerce transactions

There are several ways in which the security requirements for voting are strictly stronger than those for financial transactions. Eligibility checking is one. In the ecommerce world essentially anyone, including criminals, non-citizens, and minors, is allowed to buy and sell online. Non-human entities, e.g. corporations, government agencies, and estates, are free to engage in ecommerce transactions as well. And there are usually no residency requirements for ecommerce transactions. But those factors all play a role in determining eligibility to vote, and are verified (in principle at least) at the time of voter registration. An online voting system thus must determine that the voter is legally registered in the jurisdiction in which he or she is casting a vote.

Then there is the issue of proxy transactions. In the ecommerce world you can freely authorize someone else to act as your agent for purchases or funds transfers simply by giving them your credit card number, security code, and password. For larger transactions you can accomplish the same thing by setting up a joint bank account, signing a contract, appointing a trustee or guardian, granting power of attorney, etc. But in the voting world you are *never* permitted to transfer your right to vote to anyone else, at least not in the U.S. No one is legally allowed to act as your proxy to vote for you on your behalf — not even your spouse or guardian or caregiver, and not even with your written permission.

The prohibition of double voting is a third election security requirement that has no analog in the ecommerce world. You are free to engage in as many ecommerce transactions as you please, but you may cast only one ballot per election. Enforcement of the double vote prohibition is actually somewhat complex because it has to cover not just voting a second time online, but also voting a second time by paper absentee ballot or in person at the polls. And it should also prevent you from casting two votes in different jurisdictions in the same election, though that is difficult to enforce.

3.3 Authentication and identity determination

Because of the need for eligibility checking, proxy vote prevention, and double vote prevention an online voting system must *verify the actual identity of voters*. We need a strong identity verification mechanism because if an attacker can figure out how to cast one illegal vote online through a weakness in the identity verification, then he can probably automate that attack to cast thousands of phony votes. But reliably verifying the actual identity of a potential voter remotely through the Internet is a difficult and unsolved problem in the U.S. The U.S. does not issue national identity cards with private keys embedded in them. Nor do election jurisdictions keep a database of faces, fingerprints, or other biometric data (except for ink signatures) about registered voters, and even if they did computers today are not equipped to capture and transmit them securely. It is not sufficient for the voter to just present a password or to answer to a challenge question (e.g. "What city were you born in?"). Any such data might be given away, guessed, cracked, stolen, or sold, and enables *automated* online buying and selling or stealing of such voting credentials.

In most states voters prove their eligibility to vote when they register and provide an ink signature sample for use later use. Voters prove their identity again when they vote, either at the polls or via paper absentee ballot, by duplicating that ink signature on record in the registration database. Some states are now going even further and requiring voters to provide photo ID documents at the time of voting. But we cannot get a wet ink signature from a voter through the Internet to compare against the registration records, nor can the voter present his or her face along with a matching photo ID or passport. *As of now there is no reliable infrastructure in place to verify over the Internet the actual identity of a person sitting at a PC or holding a mobile device*.

In contrast, for an ecommerce transaction we only have to verify that the person doing the transaction is *reasonably certain to be authorized to use the financial account he is charging to*, which is a much lower requirement. There is no strong identification requirement for ecommerce transactions. All that is really required for an online transfer of funds out of your bank account is the name, account number, and password associated with the account. *There is no strong verification of the actual identity of the person doing the transaction*. Or when you sign up for an ecommerce account, e.g. at amazon.com, they ask for your name and address, but they do not ask for a picture, or an ink signature, or your driver's license, or passport, or other strong proof of identity. They never check those, and have no way to do so. To make a purchase from Amazon all that is *really* required is reasonable evidence that you are in possession of some (any!) valid credit card. You demonstrate that by giving the name on the card, the account number, security code, expiration date, and password, but you do not need to present and strong ID. If the transaction goes through, the purchase is complete. Online merchants do like to know who their customers are for marketing purposes, but when it comes down to it they will generally sell to anyone who can type in numbers and passwords for a valid account and valid credit card. It is good business practice. If the credit card turns out later to have been stolen, the problem will be sorted out after the fact.

3.4 Privacy and secrecy requirements

The privacy requirements for ecommerce and for voting transactions are fundamentally different. An ecommerce transaction is generally *symmetric* between buyer and seller, with both parties in theory fully aware of all the details of what is being bought and sold, for what price, with what warranties, and who has what rights to void the transaction, etc. For larger transactions there is usually an exchange of official paper, e.g. signed contracts or receipts, with all the relevant transaction details so that in case of a dispute either the buyer or seller can *prove* to a third party (e.g. a court) exactly what the transaction was supposed to be so the dispute can be resolved.

But it is not the same with voting transactions. The voter of course knows the details of his votes, but election officials must not. Officials know the names of those who voted and the contents of the cast ballots, but they are never supposed to know exactly who cast which ballot. This is a strong requirement for partial blindness on the part of one side in the transaction that has no analog in the ecommerce world. Furthermore, although each voter knows how he personally voted and is free to tell anyone, he is not allowed to have any *proof* of how he voted that could convince a third party. This inability to prove how you voted is the most powerful protection we have against the threat of vote selling and vote coercion, and is a requirement unique to voting. I know of no other security situation in which people are completely free to *disclose* a fact that they know (how they voted), but are not permitted to have any *proof* of that fact that can convince someone else that they are telling the truth.

3.5 Irreversibility and risk management

Vote fraud is much less manageable than ecommerce fraud. There is no election analog to the natural business practice of "spreading the cost" or "spreading the risk". There is no "insurance" that one can buy to cover those losses. There is just no way at all to compensate for damage done by fraud to an election.

The unusual vote privacy rules have strong risk management consequences. As noted earlier, if for some reason officials learn after the fact that a particular person has succeeded in casting an illegal ballot there is no way to find it to remove it from the count. In the U.S. and most other countries once a voting transaction is complete it cannot be undone even in principle, so a voting transaction is *irreversible*.

In the ecommerce world, however, we go to some lengths to make sure most transactions are reversible. Merchandise can be returned, money can be refunded in whole or in part, records can be corrected. For that reason people feel free to take prudent risks with online financial transactions based on the reputation of the merchant or the credit history of the buyer. But there is no reversibility of voting transactions, and no concept of "reputation" or "credit worthiness" in the election world to help manage risk.

These differing vulnerabilities to failures and fraud lead to very different security approaches in online transaction software. For election security there is a very strong imperative for *up front, absolute multilayered prevention of errors and fraud*. For ecommerce there is usually much reduced need for strong security barriers up front because problems can usually be corrected later and those that cannot can be absorbed.

3.6 Transparency requirements

The flip side of privacy is *openness* or *transparency*, and once again, the requirements are completely different for ecommerce and for online voting. In the ecommerce world a person buying something online is entitled to know everything about his particular transaction, but nothing about other people's transactions. A buyer is not entitled to know how many other transactions there are, what the merchant's revenues or profits are, who else the merchant sells to, or what price others pay for the same goods or services, and he has no right to audit the books of the merchant he is dealing with.

In the voting world, however, most of this is reversed. Complete election information is (or should be) open to all. Election officials report not just the names of the winners, but also exactly how many votes were cast and how many each candidate received down to the precinct level. The list of exactly who voted is also usually public, and in some jurisdictions so are the original ballot images. In principle *all* information bearing on the outcome of an election that does not compromise vote privacy is (or should be) public. Candidates, parties, and the public are entitled to participate in open audits, challenges, and recounts so that everyone, especially losing candidates, can be satisfied that the election was conducted according to law and the votes were counted accurately. Election officials are thus accountable to candidates and to the public for the integrity of every relevant detail of an election, whereas merchants are usually accountable only to buyers, and then only for each buyer's own transactions.

3.7 Fraud motivation patterns and national security

Finally we must take notice of the fact of life that the motivations for fraud are profoundly different in the commercial and electoral worlds. In an ecommerce situation all transactions are essentially independent. A buyer has no particular incentive to spoil or tamper with another buyer's online purchase since two buyers rarely have conflicting interests. In any case the problem would almost certainly be detected and corrected. And it is hard to imagine a motive for another nation to bother messing with many

Americans' ecommerce transactions when, if it is inclined to some kind of cyber attack, there are so many other more immediately damaging targets.

But the situation is completely different with voting. There is a powerful partisan incentive to block or change other people's votes, especially if it can be done without detection. The motivation to *automate* that process to affect thousands of online votes is that much greater. Such attacks can be done for tens of thousands of dollars or less, while the monetary value of changing the outcome of an election can be hundreds of millions or billions of dollars or more. The nonmonetary value can be even more immense. With online voting the danger is actually much worse because anyone on Earth, including foreign governments, could derive great benefit from tampering with with U.S. elections, especially since it is unlikely the attackers will be brought to justice. Online voting fraud is thus a *national security risk* in a way that ecommerce fraud simply is not.

4. Conclusion

The sum of all of these considerations is simple. Although ecommerce transactions and online voting transactions are superficially similar, the security, privacy, authentication and transparency requirements for online voting are much more complex and stringent. The acceptability of small losses and the strategies for managing risk must be very different. And it is hard to grasp the full implications of the fact that online elections might be compromised and the wrong people elected via silent, remote, and automated vote manipulation that leaves no audit trail and no evidence for election officials or anyone else to even detect the problem, let alone fix it.

These points are all pretty basic, and they are not going to change for the better any time soon. While there is plenty of research going on in the computer security community to try to deal with the security and privacy problems of Internet voting, there is no technology on the horizon that is going to resolve them all in the foreseeable future. For the time being we simply cannot provide satisfactory security for online voting even though we can for online commerce.

5. Acknowledgement

Thanks to Prof. Candice Hoke for invaluable help in framing these issues.