Policy Watch

No. 6

Making Electronic Voting Machines Tamper-proof: Some Administrative and Technical Suggestions

K. Ashok Vardhan Shetty

THE HINDU CENTRE
for
Politics and Public Policy

The Hindu Centre for Politics and Public Policy, Chennai, is an independent platform for exploration of ideas and public policies. As a public policy resource, our aim is to help the public increase its awareness of its political, social and moral choices. The Hindu Centre believes that informed citizens can exercise their democratic rights better.

In accordance with this mission, The Hindu Centre's publications are intended to explain and highlight issues and themes that are the subject of public debate, and aid the public in making informed judgments on issues of public importance.

Cover Photo: An Electronic Voting Machine and VVPAT unit displayed during a press conference at the Deputy Commissioner's office in Mangaluru, Karnataka, on April 3, 2018. File Photo: H.S. Manjunath.

Making Electronic Voting Machines Tamper-proof: Some Administrative and Technical Suggestions

K. Ashok Vardhan Shetty

THE HINDU CENTRE
for
Politics and Public Policy

TABLE OF CONTENTS

ABSTRACT

The Election Commission of India (ECI) has been consistently claiming that its Electronic Voting Machines (EVMs) are unique and that tampering is not feasible *under real election conditions* with its security protocol and administrative safeguards in place.

Notwithstanding the ECI's claims, at various points in time, the entire spectrum of political parties in India [including BJP and Congress] have expressed their reservations about the integrity of its EVMs. There have also been demands to revert to paper ballots. Confidence in the integrity of EVMs is important for voters to trust the outcomes of elections. The ECI cannot allow this confidence to be eroded.

It is true that Indian EVMs cannot be hacked because they are not connected to any network and their software is 'burnt' into the CPU and cannot be rewritten after manufacture. But what if dishonest insiders and criminals get physical access to the EVMs and replace the EVM's non-hackable CPU with *a look-alike but hackable CPU* that can be programmed to count votes dishonestly together with an embedded Bluetooth device that allows it to be remote controlled? All the features and safeguards relied on by the ECI can be easily negated by *insider fraud* for which there is scope at three stages: (1) at the EVMs manufacturing stage, (2) at the district level, during the long non-election period, when the EVMs are stored in archaic warehouses in multiple locations with inadequate security systems, and (3)at the stage of 'first level checks' prior to an election when the EVMs are serviced by authorised technicians from the EVM manufacturers.

The threats are real but luckily, the remedies are simple and effective: (1) use of Authentication Units *before the polls* to weed out counterfeit/tampered EVMs, and (2) effective use of Voter Verified Paper Audit Trail (VVPAT) system *at the time of counting* to guard against EVM tampering or malfunction. Both are essential. But the ECI has dragged its feet since 2006 in procuring Authentication Units, and has prescribed a minuscule sample of one EVM per Assembly Constituency for hand-counting of VVPAT slips which *is grossly inadequate, statistically unsound, and nearly as bad as not implementing VVPAT at all.*

In this Policy Watch, **K. Ashok Vardhan Shetty,** a former Indian Administrative Service (IAS) officer, examines the vulnerabilities of EVMs in the light of the ECI's claims thereof, the adequacy of its security protocol and administrative safeguards, and the risks due to the perfunctory implementation of VVPAT systems as done in the recent Assembly Elections. He provides several practical administrative and technical suggestions to make Indian EVMs tamper-proof. His interest in this matter is strictly apolitical and nothing more than preserving the integrity of India's electoral process and enhancing its credibility in the eyes of political parties and voters.

I. THE PENROSE CONDITIONS

In his book "Shadows of the Mind" (1994), Roger Penrose, the globally renowned British mathematician and authority on Artificial Intelligence, visualised the hi-tech rigging of an election as follows1. The date of a long-awaited election approaches. Numerous opinion polls are held over a period of several weeks. To a very consistent degree, the ruling party trails by three or four per cent but all the polls taken together have a much smaller margin of error, of less than two per cent. Polling day arrives and passes, the polls being held with electronic voting machines. When the votes are counted, the result is a complete surprise to almost everyone. The ruling party is back with a comfortable majority, having achieved its target of eight per cent over its nearest rivals. Yet the result is false. The vote-rigging has been achieved by a highly subtle means, namely, a computer virus. The virus was cleverly programmed to steal votes from other parties and give the ruling party precisely the majority it needs. The virus does more than just steal votes; it self-destructs, leaving no record whatsoever, bar the evil deed itself, to indicate its previous existence.

Two necessary conditions: In the 24 years since Roger Penrose wrote the above, such a scenario has already become a reality. Penrose wrote that for such an electoral fraud to succeed, two conditions are necessary:

(i) The voting machine is *programmable*. (That is because a virus can infect only a programmable computer).

(ii) The vote-counting process is *not checked by humans* at any stage.

It follows from Penrose's first condition that an ideal Electronic Voting Machine (EVM) should be a stand-alone, non-networked machine with a Central Processing Unit (CPU) whose software is 'burned' into it and cannot be programmed after manufacture or manipulated in any manner. Indian EVMs answer to this description. They are more like calculators than computers and are not connected to any network (wired or wireless) including the Internet, and *if they retain their physical integrity*, they cannot be hacked. But what if dishonest insiders and criminals get physical access to the EVMs and replace the EVM's non-hackable CPU with a look-alike but hackable CPU that can be programmed to count votes dishonestly together with an embedded Bluetooth device that allows it to be remote controlled?

The probability of successful tampering may be low but it is non-zero.

What if this replacement is done at the manufacturing stage itself for a certain percentage of machines? The probability of successful tampering may be low but it is *non-zero*. It is therefore important to analyse the security protocol and administrative safeguards that the Election Commission of India (ECI) has put in place and see if they are adequate to prevent such physical tampering of EVMs.

It follows from Penrose's second condition that relying entirely on machine counting without any physical check by humans, at least in part, may leave the system vulnerable to attacks that can go undetected. So, in case of electronic voting, there should be provision for an *additional verifiable record* of every vote cast in the form of 'paper print-outs' which should then be *hand counted* and tallied with the machine total *for at least a sample of the EVMs deployed*. This is what the EVMs fitted with *Voter Verified Paper Audit Trail* (VVPAT) seek to achieve. If vote stealing has been done by replacing the non-hackable CPU of an EVM with a look-alike but hackable CPU, then such fraud can be detected by the hand counting of VVPAT paper slips for a sample of the EVMs. It follows that VVPAT is an absolute imperative and any discussion should centre on the *statistically significant sample size of EVMs for which hand counting of paper slips should be done.*

II. TYPES OF VOTING SYSTEMS

There are broadly five types of voting systems in use around the world:

(i) **Paper Ballots that are hand counted.** Paper ballots are the simplest to understand; they can preserve the anonymity of the voter; voters can be confident that their votes have been correctly recorded; and recounting of votes is possible. Paper votes are immune to all kinds of cyberattacks and there is no malware that can steal them while appropriate safeguards can be put in place to prevent and detect human mischief. Hence this system has transparency, verifiability and accountability. But there are usually a worrying number of invalid votes and hand counting is a laborious and time-consuming process, especially in a country like India where population is very high and literacy level is low. [The risk of booth capture and stuffing of ballot papers has been drastically reduced with enhanced police security for polling stations; nor is this risk completely eliminated in EVMs where 'vote stuffing' is still possible to the extent of 12 votes per minute].

(ii) **Machine-readable Paper Ballots that are scanned and electronically counted using Optical Mark Recognition (OMR) technology.** Machine-readable paper ballots have all the advantages of the paper ballot system *minus* the delays associated with hand counting thanks to OMR technology. In order to guard against possible hacking of the OMR counting machine, the totals are verified by running the ballots through a second OMR counting machine simultaneously, and their accuracy further confirmed by hand counting a certain percentage of the ballots. Several States in the US have adopted this and others are moving towards this 'best practice'.

(iii) **Direct Recording Electronic Voting Machines (DREs) or 'paperless EVMs'.** At one time, DREs were the most commonly used type of EVMs around the world. In these, the voting is typically done by pressing a button, and the votes are recorded digitally in the memory unit of the DRE, and the counting is done electronically. While DREs have many advantages including ease of operation, reduction of invalid votes cast and speeding up the counting, they also have some glaring disadvantages.

A Direct Recording EVM of the kind used in India consists of a Control Unit (left) and a Ballot Unit (right) connected by a cable. The Control Unit is operated by the election staff while the voters cast their ballot on the Ballot Unit. Photo: The Hindu Archives

First, DREs are 'black boxes' in which it is impossible for voters to verify whether their votes have been recorded and counted correctly. In other words, DREs fulfil Penrose's second condition for occurrence of fraud.

Second, as DREs suffer from the lack of transparency and verifiability, trusting the accuracy of their vote tallies calls for 'a leap of faith'. It is true that small pre-election 'mock polls' are conducted in front of all party representatives to 'prove' that the DREs are working properly. Such pre-election mock polls might protect against *non-malicious malfunction* of EVMs. But they afford very little protection against sophisticated attacks where the dishonest, look-alike CPU has been programmed to cheat only after several hours have passed or after the EVM has recorded hundreds of votes, or if it carries a malicious programme (a Trojan) that is activated at a particular stage of the polling/counting process.

Third, with DREs, recounting is meaningless as it will simply yield the same total.

Fourth, there is the risk of the votes cast being permanently lost due to equipment malfunction.

The Federal Constitutional Court of Germany, in a landmark judgment in March 2009, held the use of paperless EVMs in Germany unconstitutional[1]. The Court ruled that all essential steps in an election are subject to public examinability unless other constitutional interests justify an exception. When EVMs are deployed, it must be possible for the citizens to check the essential steps in the election process and to ascertain the results reliably and without special expert knowledge. The standard the Court set for this purpose was that there should be a provision whereby "the votes are recorded in another way besides electronic storage" and there is "retraceability" of the election result independently of the electronic count. In other words, the Court ruled that EVMs are unconstitutional so long as there was no provision for an additional verifiable physical record of every vote cast.

(iv) **Direct Recording Electronic Voting Machines with Voter Verified Paper Audit Trail (DRE-VVPAT).** In these machines, the voter gets to view for a few seconds a paper receipt for his vote before it drops into a box, and he can verify if his vote has been recorded correctly. The DRE does the machine counting and the VVPAT 'paper slips' of a certain percentage of randomly sampled EVMs are hand counted to check the correctness. If the two totals don't tally, the VVPAT slips of some more or all of the EVMs may be hand counted. The replacement of paperless EVMs with VVPAT EVMs is imperative for the following reasons:

(a) to increase citizens' confidence that their votes have been correctly recorded,
(b) to allow for a partial or total recount using the 'paper slips',
(c) to test whether the votes have been correctly counted by tallying the result of the hand count with that of the machine count, and
(d) to provide a back-up in case of loss of votes due to equipment malfunction.

(v) **Internet-based Voting or Online Voting.** This is most vulnerable to cyber-attacks and is not suited for elections to Legislatures and is rarely used.

[1] **Federal Constitutional Court of Germany. 2009**. English version of the judgment dated March 3, is available at:
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html
[Note: All URLs were last accessed on August 29, 2018.]

India has so far tried out voting systems (i), (iii), and (iv) - in that order.

There is a school of thought which considers Machine-readable Paper Ballots that are electronically counted using OMR technology superior to EVMs with VVPAT for the following reasons.

First, paper ballots are considered the 'gold standard' of voting. That is why they are still in use in many advanced countries like the UK, Japan, Canada, and Singapore while others like Germany, Netherlands, and Ireland have reverted to paper ballots after experimenting with EVMs for some time. Machine-readable paper ballots retain all the advantages of paper ballots minus the delay in counting. Here, the primary ballots are in paper form and the secondary ballots are in electronic form whereas in EVMs with VVPAT, the primary ballots are in electronic form and the secondary ballots are in paper form. *Paper is more secure than electronic memory and primary paper ballots are superior to secondary paper ballots.*

Election officials mix up ballot papers at a counting centre in Chennai on May 8, 1996. File photo: The Hindu Photo Archives

Second, the principle of *secrecy of ballot* is a sacred one that must not be compromised, even slightly. In the old system, paper ballots from different ballot boxes were mixed together, thoroughly shuffled and packed into bundles of 50 ballots each, and then counted. This succeeded in *masking* booth-wise voting trends which would otherwise be relied upon by political parties to (i) check the effectiveness of their campaign strategies (both legal and illegal), and (ii) target collective reprisals

against voters from those booths where the party fared badly. But with EVMs, the information is freely available on ECI's website as *"Booth Level Data"*! This is manna from heaven for political parties because it enables them to know exactly how many supporters and opponents they have in each booth and incentivises illegal activities such as bribing of voters or targeting of opponents.

What is even worse is that the EVM machine *records in its memory the time at which each vote is cast*. This time-series data can become available to political parties due to insider collusion. A polling booth agent can note down the precise time at which each voter has cast his or her vote and later compare this with the time-series data from the EVM to find out who had cast votes for whom. This may be laborious but is not impossible. *This can completely destroy the anonymity of the vote* and can be used to target reprisals against individual voters. But in the case of machine-readable paper ballots, it is possible to mix them and shuffle them and pack them into bundles of 50 before counting them so that booth-wise voting trends are masked. And, since paper ballots are used, no digital time-series data are available for anybody to find out who voted for whom. Unlike some countries where the OMR scanning is done in the polling stations itself, in India it would have to be done centrally in the Counting Hall.

Third, as the VVPAT unit is an electro-mechanical (printing) device, breakdowns are quite likely. In the recent past, on an average, about 15 per cent of the VVPAT units reportedly broke down on polling day in India. While replacements are made available, there have been several cases of polling stations going ahead with the polling without the VVPAT units where there was shortage of or undue delay in replacements. Even if the quality of VVPAT units supplied is improved and the staff trained properly in their use and the percentage of breakdowns on the polling day is reduced to, say, 5 per cent, that would still be an unsatisfactory state of affairs. The ECI will be faced with the dilemma of either putting the voters to hardship by ordering repolling in these polling stations where the VVPAT units had failed and couldn't be replaced, or of ignoring these polling stations while selecting EVMs randomly for the purpose of hand counting of VVPAT slips. Both options are unsatisfactory, the second more so. There is the danger that potential attackers, operating in collusion with dishonest insiders, will ensure that the VVPATs sent to those polling stations which have the rigged EVMs do not work properly so that the VVPAT slips of these EVMs are not taken up for hand counting, thereby defeating the very purpose of introducing VVPAT. But in the case of machine-readable paper ballots that are electronically counted using OMR technology, there is no electro-mechanical device such as the VVPAT unit that can breakdown in a polling station and so the danger discussed above doesn't exist.

Going back to paper ballots *with hand counting* as demanded by some political parties is out of the question but machine-readable paper ballots that can be rapidly counted with OMR technology is certainly an option worth considering. When India has already invested so much in EVMs with VVPAT, the wisdom of switching over to this option may be open to question. In my opinion, the ECI should have adopted this 'best practice' from various countries around the world on its own. Instead, it was reluctant to switch over from paperless EVMs, and was compelled to adopt EVMs with VVPAT pursuant to a Supreme Court directive, and ended up with what was a second-best option. But the violation of the principle of *secrecy of ballot*, at least in principle, is a serious matter and the ECI needs to address this issue and consider switching over to the Machine-readable Paper Ballots system *in a phased manner* when the present VVPAT EVMs become old and need to be replaced. In fact, the ECI can introduce it straight away for the postal ballots that are cast by polling staff and servicemen working outside the places where they are registered as voters. The ECI can then not only speed up the counting of postal ballots but also trial the implementation of the new system

Machine-readable ballots rapidly counted with OMR technology is an option worth considering.

III. ELECTION ADMINISTRATORS Vs. COMPUTER SCIENTISTS

In his celebrated essay *"Two Cultures"*[2] (1959), the British writer C.P. Snow had lamented the cultural divide that separates two great areas of human intellectual activity, "the sciences" and "the arts." He wanted that practitioners in both areas should build bridges, to further the progress of human knowledge and to benefit society. A similar cultural divide exists between "election administrators" and "computer scientists" around the world regarding the electronic security of DREs or paperless EVMs; they just can't see eye to eye. The controversy over DREs dates back to the early 2000s and is world-wide (i.e. not just limited to India).

According to election administrators, it may be possible to modify an isolated DRE in a laboratory but that does not prove anything. The question is whether any tampering is feasible involving a large number of machines *under real election conditions* with the security protocol and various administrative safeguards in place. They think that computer scientists have no practical experience of conducting elections and that they exaggerate the security concerns and that the "omnipotent hacker" is a myth perpetuated by novels and movies. They believe that there is "safety in numbers" and physically tampering with a large number of EVMs is difficult because there are so many of them.

On the other hand, computer scientists think that election administrators are *status quoists* who are clueless about Information Technology and the vulnerability of paperless EVMs to a range of hardware and software attacks and the evolving nature of the threats. With DREs, frauds may be undetectable and those who have been declared the losers are left with no recourse to verify results. Computer scientists think that election administrators harbour a secret fear that the legitimacy of the election process would be undermined if such attacks are proved and so they resort to "security through obscurity" by not making the hardware and software of the EVMs available for testing for vulnerabilities by external electronic security experts. A standing joke among computer scientists is that election administrators simply don't want others to know just how bad their hardware and software are!

[2] **Snow, C.P**. 1959. *Two Cultures,* the Rede Lecture, available at http://s-f-walker.org.uk/pubsebooks/2cultures/Rede-lecture-2-cultures.pdf , Cambridge University Press.

Both election administrators and computer scientists would do well to take C.P. Snow's advice and build bridges in the interest of developing a sound and secure electronic voting system.

Ethical hacking of EVMs: *Ethical hacking* is a common practice in the software industry. Google, Apple, Microsoft, Facebook and Twitter invite hackers to find flaws in their code and offer attractive rewards (called 'bug bounties') to those who find them. The US government has done likewise with programmes like "Hack the Pentagon". But election administrators and EVM manufacturers (both government-owned and private) around the world have been reluctant to submit their machines to such ethical hacking.

The annual "DEFCON Computer Security Conference", which is the largest and longest-running conference of its kind, invites hackers from all over the world to Las Vegas, US, to display their skills.

A team competing in the CTF contest at DEFCON 17 in Las Vegas. Photo: The Hindu Archives

In the aftermath of fears that Russians had used hacking techniques to influence the 2016 US Presidential election, about 30 EVMs were made available in a 'Voting Village' to professional hackers *for the first time* in the 25th DEFCON Conference held in July 2017. Some of the EVM models had been in use in US elections till recently while others are still in use.

The hackers were allowed to probe, deconstruct and even open the equipment over a period of three days in order to understand how they work and how they could be compromised by attackers.

The results were sobering. By the end of the conference, every piece of equipment in the Voting Village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources showed that they could undermine the confidentiality, integrity, and availability of these systems. Moreover, a closer physical examination of the machines highlighted several supply chain vulnerabilities. Many machines were found to use cheap generic chips (CPUs) that could be bought over the counter instead of specially customised chips that would be difficult for hackers to lay hands on. There were multiple cases of foreign-manufactured internal parts including hardware developed in China. The hackers documented the various vulnerabilities of the EVMs in the form of a report. The 'Voting Village' concept will be a regular feature of DEFCON Conferences hereafter and this should keep the EVM manufacturers in US (all of whom are in the private sector) on their toes.

By the end of the conference, every piece of equipment in the Voting Village was effectively breached.

In contrast, the Election Commission of India (ECI) conducted a 'Hackathon' in June 2017 in which participating groups of not more than three members each (foreign experts not allowed) were given just four hours. The participants were not allowed to open the EVMs but could use a combination of keys on EVMs or communication devices such as cell phones and Bluetooth to tamper with the machines to change the results. The conditions imposed by ECI were clearly unfair and its 'challenge' was boycotted by most Indian political parties. If the ECI is really confident that its EVMs are tamper-proof, then it should send them to the next DEFCON Conference for scrutiny by ethical hackers!

IV. THE EVM CONTROVERSY IN INDIA

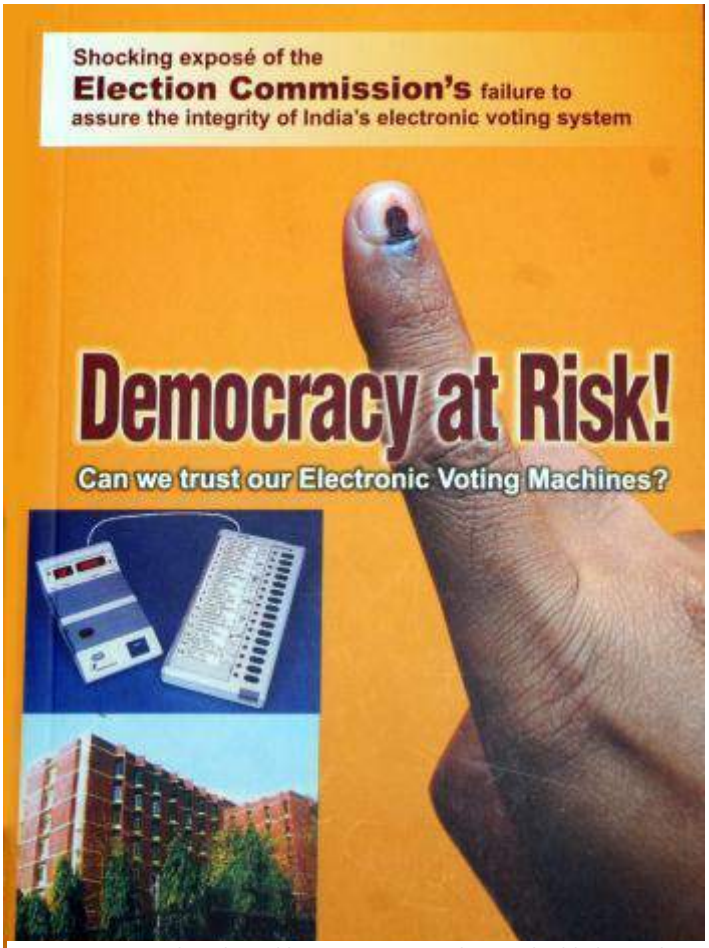
In India, the Election Commissioners are very eminent persons whose capability, sincerity, neutrality and integrity are beyond question. They have been trying their best to conduct free and fair elections and have introduced far-reaching electoral reforms. They are held in high esteem by political parties and citizens alike. But like election administrators around the world, they have been criticised for underestimating the gravity of electronic security issues. The ECI, for its part, has been consistently claiming that its EVMs, security protocol and administrative safeguards are time-tested, robust, secure and tamper-proof. According to it, Indian EVMs are unique and any comparisons with the EVMs used elsewhere in the world are misplaced. Notwithstanding the ECI's claims, at various points in time, the entire spectrum of political parties in India [including the Bharatiya Janata Party (BJP) and the Congress] have expressed their reservations about the integrity of its EVMs.

Elections are the bedrock of democracy. Confidence in the integrity of EVMs is important for voters to trust the outcomes of elections and the legitimacy of governments formed as a result of them. If the concerns about EVM security become widespread, that confidence could be eroded whether or not those concerns are well-founded. The ECI cannot allow that to happen and must retain an open mind that some of the concerns may be true and take expeditious steps to resolve the issues.

BJP the first to raise concerns about EVMs: In India, doubts about paperless EVMs were first raised by the BJP in the aftermath of the 2009 Lok Sabha polls, in which the Congress-led United Progressive Alliance (UPA) came back to power with a decisive mandate. The BJP believed that this happened because of EVM-rigging in favour of the Congress. In 2010, BJP ideologue G.V.L. Narasimha Rao wrote a very well-researched and persuasive book titled *"Democracy at Risk – Can we trust our Electronic Voting Machines?"*[3] with a foreword by the party's senior leader, L.K. Advani, and a message by Chandrababu Naidu, then a key ally. The book claimed to be a "shocking exposé of the Election Commission's failure to assure the integrity of India's electronic voting system". It highlighted the various vulnerabilities in paperless EVMs and made out a convincing case for the adoption of EVMs with VVPAT. Narasimha Rao also made a startling claim that during election

[3] **Rao, G.V.L.N. 2010.** *Democracy at Risk! Can we trust our Electronic Voting Machines?* Published by Veta. http://www.indianevm.com/book_democracy_at_risk_2010.pdf

season, "fixers" with "authorised access to EVMs" approach politicians with offers to rig machines in favour of a candidate or a party for a sum of Rs. five crore. But the ECI did not budge and persisted in its stand that tampering of EVMs was not possible under real election conditions.



Democracy at Risk authored by G.V.L. Narasimha Rao highlighting the faults in use of Electronic Voting Machines (EVMs) in New Delhi on February 12, 2010. File Photo: V.V. Krishnan. The Hindu Archives

Supreme Court mandates VVPAT:

In 2009, BJP leader Subramanian Swamy filed a Public Interest Litigation (PIL) before the High Court of Delhi seeking the implementation of VVPAT but the Court said that it was a policy matter and left it to the Parliament or the ECI to take a decision on VVPAT. The case went up to the Supreme Court. In 2013, the Supreme Court passed an order mandating the use of VVPAT EVMs, and directed the ECI to implement them in a phased manner. The Supreme Court observed[4]:

> "From the materials placed by both the sides, we are satisfied that the "paper trail" is an indispensable requirement of free and fair elections. The confidence of the voters in the EVMs can be achieved only with the introduction of the "paper trail". EVMs with VVPAT system ensure the accuracy of the voting system. With an intent to have fullest transparency in the system and to restore the confidence of the voters, it is necessary to set up EVMs with VVPAT system because vote is nothing but an act of expression which has immense importance in democratic system".

[4] **Supreme Court of India. 2013.** Judgment dated October 8, 2013 in *Dr. Subramanian Swamy vs Election Commission of India* in 3 Civil Appeal No. 9093 of 2013 is available at https://indiankanoon.org/doc/113840870/

The Supreme Court stopped short of setting a time table for the ECI to implement its ruling in full. After a delay of nearly four years, the ECI deployed EVMs with VVPATs in all polling stations in select State Assembly Elections only from 2017 onwards. The ECI has planned to conduct all future Assembly Elections and the 2019 Parliamentary Elections only with VVPAT EVMs. But there is a worrying backlog in the supply of VVPAT units by Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited (ECIL), the two public sector undertakings (PSUs) that manufacture EVMs and VVPAT units in India. Until June 19, 2018, the ECI had received only about 43 per cent of the EVMs and *only 22 per cent of the VVPAT units* that it had placed orders for. The deadline for 100 per cent supply is end-September 2018.

The ECI plans to conduct all future elections only with VVPAT EVMs but there is a backlog in supply.

The shoe is on the other foot: Ever since the BJP came to power in the Centre in 2014, it has been the turn of the Opposition parties to claim that EVMs are being rigged in favour of BJP, and the chorus became louder after the BJP's landslide victory in the Uttar Pradesh and Uttarakhand Assembly elections in 2017. There were no such claims when the Aam Aadmi Party (AAP) won a landslide in the Delhi Assembly elections in 2015 or the 'Mahagatbandhan' of Janata Dal–United (JDU), Rashtriya Janata Dal (RJD) and Congress won the Bihar elections in 2015 by a big margin. This led to the criticism that the Opposition parties were "sore losers" who raised the bogey of EVM-rigging only when they lost an election and remained silent when they won it. Recently, Mamata Banerjee, the Chief Minister of West Bengal, brought 17 Opposition parties together to make a joint representation to the ECI that the 2019 Parliamentary elections should be fought with paper ballots since EVMs could be rigged and were not trustworthy.

Opinions on the issue of EVM-tampering are sharply polarised in India today with the BJP now claiming that tampering is not possible and many Opposition parties expressing the contrary viewpoint. If it is any consolation, things are pretty much the same in the US and elsewhere. As Marian Schneider of the US non-profit *"Verified Voting"* has observed[5]:

> "I don't think this is a political issue. Everybody gets elected on the same equipment, regardless of their party. So making sure that that equipment is working well, making sure that we can verify the results so that the outcome is correct is important to everyone."

[5] Quoted in "*Spooked by election hacking, states are moving to paper ballots" by Zaid Shoorbajee, Cyberscoop, March 12, 2018.*
https://www.cyberscoop.com/paper-ballots-election-security-electronic-voting-machines/

It must be noted that the threats to the integrity of our electoral process need not come only from ruling parties of the day in the Centre or the States; they could come from foreign attackers also. The allegation of Russian interference in the 2016 US Presidential elections on behalf of President Donald Trump, which is under investigation by the *U.S. Senate Select Committee on Intelligence,* shows that this danger is real, and that elections are now on the front lines of cybersecurity. Other potential attackers are terrorists who may wish to disrupt elections in order to spread confusion and distrust or rogue employees of EVM manufacturers who may do it for money.

V. PERFUNCTORY IMPLEMENTATION OF VVPAT

Ideally, the controversy over EVMs should have been laid to rest once the Supreme Court had ordered the implementation of EVMs with VVPAT in 2013. If this has not happened, it is partly due to the inordinate delay in procurement of VVPAT units and partly due to the ECI's questionable action of prescribing a minuscule sample of EVMs for hand-counting of VVPAT slips.

After some initial press reports stating that VVPAT slips may be counted in respect of 10 per cent or 5 per cent of the EVMs, the ECI threw a bombshell by ordering the hand counting of VVPAT slips *only for one randomly chosen polling station (i.e. one EVM) per Assembly Constituency* in the Assembly Elections for Gujarat and Himachal Pradesh held in December 2017 and Karnataka in May 2018. This worked out to just 182 out of 50,128 polling stations (or 0.36 per cent of the EVMs) in Gujarat; to just 68 out of 7,521 polling stations (or 0.90 per cent of the EVMs) in Himachal Pradesh; and to just 224 out of 56,696 polling stations (or 0.40 per cent of the EVMs) in Karnataka. *Such a low percentage defeats the very purpose of introducing VVPAT and is fraught with all the risks of conducting elections with paperless EVMs.*

Statistically Unsound: Consider a hypothetical example where 4 Assembly Constituencies P, Q, R and S have 50, 100, 200 and 300 polling stations in them respectively. The ECI's action of prescribing a uniform sample size of "one polling station (EVM) per Assembly Constituency" cannot obviously be correct for all the 4 constituencies. Since the number of polling stations in an Assembly Constituency varies widely from State to State and even within a State, the sample size should clearly be different for different Assembly Constituencies and bear a relation to the number of polling stations in the constituency.

In fact, there cannot even be a uniform per centage for sample size for all Assembly Constituencies as per standard statistical sampling theory. As we shall show shortly, if 'N' is the Population Size and 'n' the Sample Size, then the smaller the value of N, the greater will be the value of n/N (i.e. the Sample Size *relative* to the Population Size). Thus, smaller States and smaller constituencies will have *relatively* larger Sample Sizes when expressed as a fraction of Population Sizes.

There are ready reckoners based on *standard statistical sampling theory* which can tell us as to what would be the *Margin of Error* for the chosen Sample Size for a given *Population Size* and a given *Confidence Level.*[6] Taking the total number of polling stations in the State as the Population Size and the total number of EVMs taken up for hand counting of paper slips (which is equal to the number of Assembly Constituencies in the State) as Sample Size, and assuming Confidence Levels of 95 per cent and 99 per cent, Table 1 shows the resulting Margins of Error for the ECI-prescribed sample size in respect of Gujarat, Himachal Pradesh and Karnataka.

Table 1
Margins of Error for ECI-prescribed Sample Size

State	Population Size (Total Number of Polling Stations)	Sample Size (Number of EVMs chosen for hand counting = Total number of Assembly Constituencies)	Confidence Level (%)	Margin of Error (%)
Gujarat	50,128	182	95	**7**
			99	**10**
H.P	7521	68	95	**12**
			99	**16**
Karnataka	56,696	224	95	**7**
			99	**9**

It is evident that the ECI-prescribed sample size for hand-counting of VVPAT slips is far too small leading to very high margins of error which are unacceptable in a democracy. It is open to legal challenge on this score. The ECI seems to have chosen the sample size arbitrarily when, in fact, its selection should have been grounded in standard statistical sampling theory.

Ready reckoners based on standard statistical sampling theory can also tell us as to *what should be the statistically significant Sample Size*[7]. for a given *Population Size,* a given *Confidence Level and* the chosen *Margin of Error.*

[6] A Web-based ready reckoner which can calculate the *Margin of Error* for a given *Population Size*, *Sample Size* and *Confidence Level* based on standard statistical sampling theory is available at https://www.surveymonkey.com/mp/margin-of-error-calculator/?ut_source=mp&ut_source2=sample_size_calculator

[7] A Web-based ready reckoner which can calculate the statistically significant *Sample Size* for a given *Population Size*, *Confidence Level* and the chosen *Margin of Error* based on standard statistical sampling theory is available at

It is suggested that the ECI should choose the Population Size (N), the Confidence Level and the Margin of Error in such a way that the *resulting* Sample Size (n) is *reasonable* (neither too small nor too large), *statistically sound* and *administratively viable*.

- The Population Size (N) can be either the total number of polling stations i*n the State as a whole* or the total number of polling stations *in each Assembly Constituency*.
- The Confidence Level can be either *99 per cent* or *95 per cent* but not less. In my opinion, a Confidence Level of 95 per cent would be adequate.
- The Margin of Error can be either *1 per cent* or *2 per cent* but not more. In my opinion, a Margin of Error of 2 per cent is adequate.

For our hypothetical Assembly Constituencies P, Q, R and S (having 50, 100, 200 and 300 polling stations in them respectively), if we assume a Confidence Level of 95% and a Margin of Error of 2%, then as seen from **Table 2**, the resulting sample size is nearly as large as the population size. *So an Assembly Constituency is not an appropriate unit for the purpose of Population Size*

Table 2
Statistically Significant Sample Sizes if Assembly Constituency is the unit for Population Size

For Confidence Level of 95% and Margin of Error of 2%

ASSEMBLY CONSTITUENCY	POPULATION SIZE (N) [TOTAL NUMBER OF POLLING STATIONS IN THE CONSTITUENCY]	SAMPLE SIZE (N) [NUMBER OF EVMS TO BE HAND COUNTED]
P	50	49
Q	100	97
R	200	185
S	300	267

Hence the ECI should treat the State as a whole as the unit for the purpose of Population Size, and arrive at the Sample Size (using the ready reckoner) for a Confidence Level of 95 per cent, and a Margin of Error of 2 per cent. **Table 3** suggests the sample sizes under these conditions.

https://www.surveymonkey.com/mp/sample-size-calculator/?ut_source=mp&ut_source2=margin_of_error_calculator

Since this sample is for the State as a whole, the ECI must do stratified sampling by treating each Assembly Constituency as a 'stratum' and apportion the total sample among the various Assembly Constituencies in proportion to the number of polling stations in each Constituency.

Table 3
Statistically Significant Sample Sizes if the State as a whole is the unit for Population Size

For Confidence Level of 95% and Margin of Error of 2%

State	Population Size (N) [Total Number of Polling Stations in the State as a Whole]	Sample Size (N) Required for the State as a Whole [Number Of EVMs to be chosen for Hand Counting]	% of Sample Size W.R.T. Population Size	*Average* Number of EVMs to be Hand Counted Per Assembly Constituency
Gujarat	50,128	2,292	5	13
H.P	7,521	1,821	24	27
Karnataka	56,696	2,304	4	10

The *average number of EVMs to be hand counted per Assembly Constituency* has been indicated so as to give an 'order-of-magnitude' figure vis-a-vis the present figure of one EVM per constituency. For example, in Karnataka, *on an average*, 10 EVMs *should* have been hand counted per Assembly Constituency instead of the 1 EVM that was actually hand counted. As already stated, the *actual number* will vary from constituency to constituency.

If the ECI desires, it may refine the stratified sampling further by identifying appropriate *sub-strata* in order to make the samples truly representative of the constituency as a whole. A typical Assembly Constituency may have several different groups (or 'sub-strata') of polling stations each with *different levels of vulnerability*: urban, semi-urban, rural, those in remote hilly/desert/forest areas, those with very heavy voter turnout (> 80 per cent), those with moderate voter turnout (50 per cent to 80 per cent), those with low voter turnout (<50 per cent), and so on. (There could be some overlapping among these groups).

Let us say that the following sub-strata are chosen: (1) polling stations with heavy voter turnout (>80%), (2) polling stations with moderate voter turnout (between 50% and 80%), and (3) polling stations with low voter turnout (< 50%). The ECI may further apportion an Assembly Constituency's sample among these 3 sub-strata in proportion to the number of polling stations falling within each of the sub-strata.

It is best that the ECI do the necessary calculations and communicate to the Chief Electoral Officer (CEO) of the State the sample size for hand counting of EVMs' VVPAT slips (1) for the State as a whole, (2) for each Assembly Constituency, and (3) for each of the sub-strata within the constituency (if any prescribed)

Why is the ECI reluctant? What could be the reasons for the ECI's reluctance to order the counting of VVPAT slips for a larger sample of EVMs? I see a few plausible justifications (in italics) and have offered my responses to the same:

- *The EVMs used in India are reliable and tamper-proof and counting VVPAT slips of more than one polling station per Assembly Constituency is a waste of time and effort.*

  Any electronic equipment is *inherently* subject to equipment malfunction and too much trust in the EVM's reliability would be misplaced. Hand counting of an adequate sample of VVPAT slips offers protection not just against the possibility of EVM tampering but also against the possibility of EVM malfunction which can result in wrong totalling and change of election outcomes just as EVM tampering can. Administrative safeguards notwithstanding, why trust paperless EVMs which lack transparency and verifiability? After all, VVPAT is an additional safeguard, a very critical safeguard, which can help detect frauds that would otherwise go undetected. Conducting elections without VVPAT is like trying to eliminate accounting frauds and mistakes by eliminating the ability to detect them i.e. by eliminating the audit department whereas choosing a minuscule sample of EVMs for hand counting VVPAT slips is like severely downsizing the audit department so as to render it ineffective!

- *The hand counting of a larger sample of VVPAT slips can lead to delays of several hours or even a couple of days in the announcement of results.*

  Surely, in something as important as ensuring the integrity of the election process, a delay of a few hours or even a couple of days shouldn't matter at all? When the entire election process, from the date of announcement to the date of counting, lasts for 2-3 months, there is no reason why unseemly hurry should be shown only in the case of counting. In the rush to declare results and the winners, the ECI cannot turn a blind eye to the possibilities of wrong totalling due to EVM malfunction or EVM tampering.

- *Why count a larger sample of VVPAT slips when the voters have already verified their VVPAT slips at the time of polling?*

  Video recordings of voter behaviour during actual elections in India and elsewhere have revealed that most voters do not verify their choices by reading the VVPAT slip after casting their vote. There are many illiterate voters, and even among the literate voters, many are not techno-savvy, and may not verify the VVPAT slip within the window of 7 seconds available.

It will require plenty of voter training to make the voters verify the VVPAT slip immediately after casting their vote. So, the absence of complaints from voters must not be treated as evidence that the EVMs are functioning properly.

According to some critics, the ECI is perhaps afraid that too much transparency and pro-active counting of VVPAT slips for a larger percentage of polling stations may show up many EVMs to be faulty and do great harm to the prestige of the Commission and raise a question mark about the sanctity of past elections! They allege that the ECI's action of ordering the counting of VVPAT slips for less than 1 per cent of the EVMs for the Gujarat, Himachal Pradesh and Karnataka Assembly elections must be seen in this light! I am sure that this is not the case.

Wrong signal: When only one EVM per Assembly constituency is chosen for the counting of VVPAT slips, the ECI is sending the wrong signal to the election personnel, from the District Magistrate–cum-District Election Officer (DM-DEO) downwards, that *it is not serious about VVPAT and regards it as an unwanted appurtenance thrust upon it by the Supreme Court at the behest of certain conspiracy theorists*. The Presiding Officers and the Polling Officers in several polling stations are likely to be negligent in repairing/replacing the VVPAT machines then and there, and may try to chance their luck by hoping that their particular polling station will not get picked for counting of the VVPAT slips. The danger is greater in villages and in remote areas. My enquiries with DM-DEOs and Election Observers have revealed that in the past, on an average, about 15 per cent of the VVPAT units did not function properly on polling day, and that the ECI had orally instructed them to carry on with the polling without VVPAT in case of shortage of replacements.

In the past, on an average, about 15 per cent of the VVPAT units did not function properly.

It is important that the Supreme Court's order of 2013 must be implemented properly both in letter and spirit in all future elections. The ECI must therefore direct DM-DEOs to strictly ensure that all the VVPAT systems in every polling station function properly, failing which there shall be repolling.

Some suggestions: The following related suggestions are proposed for the kind consideration of the ECI.

- There should *not* be a uniform sample size of EVMs for the hand counting of VVPAT slips for all Assembly Constituencies. The ECI should arrive at the statistically significant sample size for the *State as a whole* for a Confidence Level of *not less than* 95 per cent and a Margin of Error of *not*

more than 2 per cent using a ready reckoner. This sample may then be apportioned among the various Assembly Constituencies in proportion to the number of polling stations in each Constituency. The sample size becomes very large if the adopted Confidence Level is 99 per cent or the Margin of Error is 1 per cent and may be administratively unviable.

- The random sample of polling stations for the hand counting of VVPAT slips should be decided by draw of lots on the morning of the counting day (or as close to the counting day as possible). The lots should be drawn by the DM-DEO in the presence of the candidates or their authorised representatives.

- The hand counting of VVPAT slips of the chosen sample of polling stations should be commenced at the same time as the electronic counting and run parallel to it.

- The Election Manual permits the losing candidate to apply to the Returning Officer (RO) for a recount with the VVPATs, but it is not mandatory for the RO to accept. The RO may reject the request in writing whereupon the losing candidate has to follow the usual appeal procedure which is time consuming and unproductive. If the margin of victory is less than, say, 2 per cent, the ECI may make it mandatory for the RO to order a hand recount with VVPAT slips of all the polling stations.

- Irrespective of the margin of victory, if the discrepancy between the machine-counting total and the hand counting total in respect of the selected sample of EVMs taken together is considered statistically significant as per standard methods of statistical Hypothesis Testing, then the ECI may order the hand counting of VVPAT slips in all the polling stations.

The ECI will be doing the nation and itself a favour if it accepts the above suggestions, especially with regard to increasing the sample size for hand counting of VVPAT slips. They must be implemented from the next batch of Assembly Elections due in December 2018-January 2019. The downside is that it may take a little longer to complete the counting process but it is a non-issue. *The upside is that it will reinforce the confidence of the voters in the electoral process and effectively silence the critics of the ECI.* If the ECI persists with its minuscule sample of EVMs for hand counting VVPAT slips, an adverse inference is liable to be drawn against it and it may lose the perception battle.

VI. THE VULNERABILITY OF INDIAN EVMs

In 2010, a team led by J. Alex Halderman, Professor of Computer Science, University of Michigan, US, managed to get hold of an Indian EVM unofficially and published a paper titled *"Security Analysis of India's Electronic Voting Machines"*[8]. This was the first, independent, rigorous assessment of the security risks associated with Indian EVMs. It described the EVM's design and operation in detail, and evaluated its security in light of relevant election procedures. It pointed out many vulnerabilities that the ECI's "Technical Experts Committee" had failed to do.

According to the paper, while the simple hardware design and the minimal software of Indian EVMs made certain software-based attacks less likely than in their counterpart Direct Recording EVMs in the West, they made a different set of highly dangerous attacks far easier. Such attacks which can steal votes and violate the secrecy of the ballot can be carried out by dishonest election insiders or other criminals with only brief physical access to the machines. The authors also demonstrated two such attacks. They observed:

> "Using EVMs in India may have seemed like a good idea when the machines were introduced in the 1980s, but science's understanding of electronic voting security and of attacks against it has progressed dramatically since then, and other technologically advanced countries have adopted and then abandoned EVM-style voting. Now that we better understand what technology can and cannot do, any new solutions to the very real problems election officials face must address the problems, not merely hide them from sight."

The ECI and the two manufacturers of EVMs (BEL and ECIL) dismissed the findings of the research paper by Prof. Halderman *et al* with the standard reply that while it may be possible to tamper with an isolated EVM in a laboratory, tampering with a large number of machines is not feasible *under real election conditions* with the security protocol and various administrative safeguards that the ECI has put in place.

It is therefore necessary to examine the various features of the Indian EVMs (of the non-VVPAT variety) and the adequacy or otherwise of the ECI's security protocol and administrative safeguards. This assumes significance in the light of the perfunctory implementation of VVPAT systems by the ECI in the recent Gujarat, Himachal Pradesh and Karnataka Assembly Elections. In this

[8] **Halderman, J.A. et al**. 2010. *Security Analysis of India's Electronic Voting Machines* is available at https://indiaevm.org/evm_tr2010.pdf

connection, the ECI's *"Status Paper on Electronic Voting Machines"*[9] and its press release titled "*FAQs on Security Features of the ECI-EVMs*"[10] are worth reading.

It is true that ECI's (paperless) EVMs are stand-alone, non-networked machines that are not connected to the Internet at any point of time and cannot therefore be hacked. But then, the paperless EVMs (or DREs) used all over the world are also "stand-alone" machines like Indian EVMs and are not part of any network though they may differ in certain other features. As German software expert Dr.Ulrich Weisner, who won the case against EVMs in Germany leading to their ban, observed:

> "(EVMs)…banned in the Netherlands, Ireland and Germany are not networked…they were similar to the Indian EVMs and worked stand-alone with no connection to Internet or other networks during the election and counting phase. The lack of the network connection was one of the (invalid) reasons given by the vendor and by authorities in the three countries why the machines could not be hacked. The vendor also claimed that his devices were not real computers but 'special purpose devices' which were designed to only count votes and could not be used for any other purpose….It is common sense that someone who has sufficient access to open the Indian EVMs and replace the software or hardware can implement virtually any functionality, including vote stealing functionality, that is only activated under certain circumstances and would not be spotted in tests."[11]

The ECI is largely correct when it claims that the software ('firmware') of its EVMs cannot be manipulated in any manner. The greater the lines of code, the greater the scope for manipulation. The software of Indian EVMs is *minimal*, and it is *One Time Programmable (OTP)* that is 'burned' into the EVM's CPU and cannot be re-written after manufacture. But this design also has certain disadvantages.

The flip side of the minimalist software is that it does not attempt to cryptographically protect the *voting data* stored in the electronic memory of the EVM's Control Unit which are therefore *unsecured*. Even though some of the world's best brains develop the software of Microsoft, Apple and Google, there are still several bugs and security issues in their software which are corrected (and new features

---

[9] **Election Commission of India**. 2017. *Status Paper on Electronic Voting Machine (EVM)* is available at http://eci.nic.in/eci_main1/current/StatusPaperonEVM_09052017.pdf

[10] **Election Commission of India**. 2017. Press release dated April 9, 2017 on *FAQs on Security Features of the ECI-EVMs.* Available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=160754

[11] Quoted in G.V.L. Narasimha Rao's book (page 25) vide Note 4 above.

added) by software updates that are automatically downloaded via the Internet and installed. The flip side of OTP software and EVMs not being part of any network including the internet is that bugs and security issues cannot be fixed and new features cannot be added until a new *generation* of EVMs is developed. These bugs may cause occasional (non-malicious) equipment malfunction such as flipping of votes, loss of votes, wrong totalling etc. which can change election outcomes just as EVM tampering can and which cannot be detected and corrected without VVPAT.

Further, the software used in ECI's EVMs is 'burnt' into the CPU by *two foreign chipmakers* (Microchip Technology Inc., US and Renesas Electronics Corporation, Japan), after which they are shipped to India for assembly into the EVMs. This is a rather serious supply chain vulnerability. The EVM manufacturers (BEL & ECIL) cannot 'read back' their contents to verify the integrity of the software. They can only carry out 'functionality tests' on the EVMs to check whether they are working properly. This is called *'black box testing'*. According to Arnold B. Urken, who founded the first voting-machine testing lab called Election Technology Laboratories, *'white-box testing'*—eyes-on examination of the firmware of the EVMs—should be mandatory if certification is to mean anything. Indian EVMs do not fulfil this condition, a shortcoming highlighted by Rao in his book[12].

While it is true that Indian EVMs cannot be hacked because they are not connected to any network including the internet and their software is OTP that cannot normally be manipulated after it is 'burnt' into the CPU, *this holds good only so long as the EVMs retain their physical integrity*. In other words, their strengths can be easily negated by the simple act of replacing the non-hackable CPU with a look-alike hackable one! Further, by embedding a Bluetooth device or a micro-transmitter in the substitute, look-alike CPU, it will be possible for an attacker to manipulate the EVM through remote devices. *Once these two things are done, EVM security goes out the window*.

Indian EVMs cannot be hacked only as long as they retain their physical integrity.

Prof. Halderman *et al* have shown that such replacement of CPU can be done very easily if dishonest insiders and criminals can get physical access to the EVMs even for a short while. Since Indian EVMs use cheap generic chips rather than the more secure customised chips, the replacement is rendered easier. The substitute, look-alike CPU could have a Trojan embedded inside it. This Trojan can remain dormant till the elections, be activated during the elections to steal votes, and be made

[12] **Ibid.**

to 'disappear' after elections. This would result in the 'perfect election fraud' that Roger Penrose had envisaged, one that can neither be detected before the elections nor proved after the elections, unless VVPAT is used.

The researchers have stated that not just the CPU, but the *Motherboard* (card which contains the CPU) can also be replaced *with a look-alike but dishonest Motherboard*. What is more, attackers can also build *identical looking but dishonest Ballot Units* and *Control Units* and substitute them for the Commission's EVMs. Even if the CPU is genuine, the attackers can build a *dishonest Display Board* replacing the real Display Board in the Control Unit by adding a hidden microcontroller (chip) that can intercept vote totals and substitute fraudulent results. Prof. Halderman *et al* demonstrated physically how the "dishonest display attack" can be done. Since the voting data stored in the electronic memory of the Control Unit is *unsecured* (due to the minimalist software of the CPU), it can be manipulated by the *temporary application* of a malicious hardware. The researchers also demonstrated physically how a "clip-on device" can manipulate the electronic memory, steal votes and violate ballot secrecy.
Some other possibilities of fraud can also be envisaged:

- Replacing the cable (connecting the Ballot Unit and the Control Unit) with a dishonest look-alike cable carrying a tiny embedded chip with a Bluetooth device that can be programmed with vote stealing software and operated remotely. While fiddling with the CPU, Motherboard or Display Board in the Control Unit may attract some suspicion, replacing the cable connector can be a simple and smooth affair for those who want to subvert elections. It can be done relatively easily by couching it as routine maintenance and it will not excite the suspicion of potential whistle-blowers. Furthermore, cables are not considered high security items and therefore can be manufactured locally, through outsourced private suppliers, who could be more easily compromised.

- Embedding a vote-stealing Trojan in the chips supplied to BEL and ECIL. This mischief can be done by rogue employees at the foreign chipmakers' end, and BEL and ECIL may not be in a position to detect the same.

- Hacking the databases of voters in States (which typically have few IT support staff and little, if any, cybersecurity expertise) so as to modify the printed voter lists that are prepared from these databases. Selectively omitting the names of small groups of voters – by community, caste or locality, for example – can play havoc on polling day. This is alleged to have been the *modus operandi* of Russian interference in the 2016 U.S Presidential Election.

Many computer scientists can list dozens of other plausible ways to compromise EVMs. *Thus, the ECI's claims about Indian EVMs being 'different' and 'tamper proof' do not seem to withstand rigorous scrutiny.* There are a startlingly large number of security issues that render its EVMs susceptible to fraud and which can alter election results without the ECI being any the wiser.

It must be noted that the fact that certain vulnerabilities (as pointed out above) exist in the EVMs doesn't necessarily mean that the EVMs have been tampered with or the attacks have already happened. It only means that the *potential* for attacks exists and the vulnerabilities must be suitably addressed. While protecting a Head of State, security officials will have to find all possible vulnerabilities and protect him or her against everything whereas the potential assassin has to find only one unprotected vulnerability. The same logic applies to EVM security. The ECI should adopt a policy of "Better safe than sorry". EVM security is nearly as important as national security.

The ECI would be making a serious mistake if it underestimates the kind of ingenious electronic security breaches that are possible or if it thinks that Indian politicians are not 'hi-tech' enough to resort to such manipulations. Given the high stakes involved, the possibility of our political parties engaging the best brains in India and abroad to perpetrate such 'hi-tech' frauds cannot be ruled out! The recent controversy over the manipulation of personal data from *Facebook* by the UK-based firm *Cambridge Analytica* for election campaigning, and reports that Cambridge Analytica may have worked with political parties in India have triggered a massive political row, with both the Congress and the BJP accusing the other of having used its services.

VII. THREE SECURITY LOOPHOLES

The ECI's strategy to prevent electoral fraud relies on the physical security of EVMs, the secrecy of their firmware, the integrity of election insiders, and various administrative safeguards (such as randomisation of allotments of EVMs to States and polling stations, among others). While the strategy looks impressive *on paper*, it will succeed only if the election insiders can be fully trusted.

Insider Fraud: The ECI appears to ignore or underestimate the danger that *these administrative safeguards can be easily negated by insider fraud*. As in currency printing presses, banking, insurance, gambling casinos, university examinations, etc., insider fraud is an insidious and ever-present danger with EVMs, and the best laid plans of the ECI can go awry! There is no justification to trust insiders in the election ecosystem any more than trusting the insiders in currency printing presses, banking, insurance, gambling and examinations ecosystems where sophisticated frauds continue to occur despite equally good safeguards as the ECI's being in place, if not better ones.

The recent *Punjab National Bank-Nirav Modi scam* (involving issue of thousands of fraudulent Letters of Undertakings causing a loss of about Rs.13,000 crores) is a good example. Notwithstanding the many 'safeguards' theoretically in place – periodic reconciliations, internal audit, statutory audit, RBI inspections, Ministry representatives and independent Directors on PNB's Board etc - a massive scam went on for nearly seven years before coming to light. This scam was rendered possible by the collusion between bank insiders and Nirav Modi, with the former even sharing the top-secret SWIFT password with the latter and not making the relevant entries in the Core Banking System!

In my assessment, there is scope for insider frauds at three stages:

A. At the EVMs manufacturing stage.

B. At the district level, during the non-election period, when the EVMs are stored in archaic warehouses in multiple locations with inadequate security systems.

C. At the stage of 'first level checks' prior to an election when the EVMs are serviced by 'authorised technicians' from BEL and ECIL.

Each of these security loopholes will be discussed in greater detail below.

A. EVM manufacturing stage: In the US, all EVM-manufacturers are in the private sector and some of them are big donors to the Republican Party. Doubts have been expressed as to whether the manufacturers can be trusted to play fair, especially in a scenario where their frauds cannot be detected (as with paperless EVMs). In an article in *"The Hindu"* titled *"Are electronic voting machines tamper-proof?"* (2010)[13], BJP leader Subramanian Swamy had stated: "After Hugo Chavez won the 2004 election in Venezuela, it came out that the government owned 28 per cent of Bizta, the company that manufactured the voting machines." Now, if you can't fully trust a company of which government is a part owner, can you trust companies of which government is full owner?!

The ECI's argument that unlike other countries where EVMs are manufactured in the private sector, Indian EVMs are manufactured by "the reliable" Central public sector undertakings (BEL and ECIL) is not fully correct. *First*, the key process of 'burning' of the EVM firmware has been outsourced to two private, that too foreign, chip-making companies (Microchip Technology Inc., USA and Renesas Electronics Corporation, Japan).

The argument that EVMs are manufactured only by reliable Central public sector undertakings is not fully correct.

Second, it is naïve to believe that with public sector undertakings (PSUs), secrecy will be maintained and insider frauds cannot happen! (Let us not forget that Punjab National Bank is a public sector bank)! Knowing how PSUs work in India and the huge interference in their functioning by the concerned Ministries of the Government of India where even a Joint Secretary pushes the top officers of the PSU around and where the threat of harassment by CBI and CVC looms large over those who don't toe the Ministry's directives, I am of the strong opinion that BEL and ECIL are as vulnerable as, if not more than, a private manufacturer. I think that there is a non-zero probability of occurrence of any of the following scenarios without the ECI's knowledge:

- *Scenario 1*: Enormous political pressure is brought to bear upon the top management of BEL and ECIL by the ruling party of the day in the Centre to secretly manufacture a certain percentage of EVMs in which the regular non-hackable CPU is replaced with *a look-alike but hackable CPU* that can be programmed with vote stealing software; it will also have an embedded Bluetooth device so that it can be operated remotely. These altered EVMs may be passed off as a new batch. If only a few key employees collude, such a fraud would be difficult

[13] **Swamy, S. 2009.** Are electronic voting machines tamper-proof? *The Hindu*, June 17. Available at https://www.thehindu.com/todays-paper/tp-opinion/Are-electronic-voting-machines-tamper-proof/article16579547.ece

to detect. Going by the general administrative culture prevailing in the government or PSUs in India, it would take a rare CEO indeed to withstand that kind of political pressure.

- *Scenario 2*: A few *key employees* of the two EVM manufacturers, driven by the same ideology as the ruling party of the day in the Centre or any other political party, may resort to this kind of tampering *without the knowledge of the top management of BEL and ECIL*. These 'key employees' could be those engaged in the development of the EVMs' firmware or in the assembly of the EVMs.

- *Scenario 3*: A few *rogue employees* of the two PSUs may do it for the sake of money, *again without the knowledge of the top management*. Rao cited instances of politicians being approached by technocrats from the 2 PSUs promising to rig the EVMs for a fee. While we don't know if there is any truth in these allegations, they are not impossible to envisage.

- *Scenario 4:* The vendors (many of them with political affiliations) supplying key components – Display Board, cable connector, etc - to BEL and ECIL can be compromised. This includes the two foreign private chip makers who have been assigned the security-sensitive job of fusing the firmware onto the CPUs that go into the EVMs. *This can also happen without the knowledge of the top management.*

In my opinion, there is a major loophole at the EVM manufacturing stage which can potentially be exploited by the ruling party of the day in the Centre. Due to its lack of familiarity with technical matters, the ECI has delegated a number of crucial functions regarding the conduct of elections – like manufacturing, checking and maintenance of EVMs – to the EVM manufacturers. It has reposed blind trust in the two PSUs and has no means of verifying if they are playing foul. It is naïve to believe that things cannot go wrong in BEL and ECIL and that they will police themselves. (By this logic, things cannot go wrong in PSU banks or in University examinations). The concerned personnel of the EVM manufacturers together with their suppliers and other authorised agencies have also become 'election insiders', and the ECI's lax administrative and technical control over them makes insider frauds easier to commit and difficult to detect. As Rao observed in his book:

There is a major loophole which can be exploited by the ruling party of the day in the Centre.

> "All this begs a simple question: are we running "faith based" elections that we should "trust" all these insiders and not question their actions shrouded in mystery? We cannot pride ourselves

being a vibrant democracy if our election results are reduced to merely our faith in agencies involved in the conduct of elections."[14]

Eight years after Rao wrote the above, things are pretty much the same.

B. During storage at the District level: The second security loophole is at the district level when EVMs are stored during the long non-election period in archaic warehouses in several locations in the district. This decentralised way of storing EVMs and the long periods of non-use increases the risk of theft and tampering and reduces the chances of detection.

As compared to the two EVM manufacturers and related agencies, the ECI exercises far greater control over the *election officials* of various States but only during the period of conduct of elections. It is during the long non-election period when ECI's supervision is light that such frauds may happen.

Finding suitable storage places is very difficult in some backward districts and the quality of the rented warehouses is highly variable. Notwithstanding the 'strong room' and the 'double lock system' and the 'annual physical verification of the EVMs', it is not unreasonable to presume that some election officials in the district – from the security staff upwards - can collude with the ruling party of the day in the State (or any other political party if it is more techno-savvy) to allow access, steal some EVMs, and skilfully replace the seals on the locks of the warehouse with or without the knowledge of the DM-DEO.

In a country like India renowned for its 'jugaad' where duplicates of anything and everything are made, it would be naïve on anybody's part to think that counterfeit EVMs can never be made *by reverse engineering the stolen EVMs*. Reverse engineering of the EVM hardware as a whole or any individual component thereof is rather easy. But can the secret firmware of the EVMs also be reverse engineered? The ECI's claim is that the secret firmware is OTP and 'burnt' into the CPU and it cannot be read, copied out, altered and refed into the CPU at all. But according to Prof. J. Alex Halderman *et al*, reverse engineering the secret firmware is possible given enough time and resources, and it could be revealed by one well-funded attacker with access to a single EVM. To quote the authors:

It would be naïve on anybody's part to think that counterfeit EVMs can never be made by reverse engineering.

[14] Vide Note 4 above.

> "While more involved than modifying source code, reverse engineering firmware of such low complexity is not difficult and has been done (sometimes within a few weeks) with other voting systems in the context of academic research".[15]

The feasibility of reverse engineering firmware even though it is 'burnt' into the CPU has been recognised by the U.S Court of Appeals, Ninth Circuit, in the case of "*Syntek Semiconductor Co., (Taiwan) versus Microchip Technology Inc., (USA)"* in April 2002[16]. Thus the 'unreadable and unalterable' secret firmware is also not a fool proof security feature as claimed by the ECI. It may be noted that Microchip Technology Inc., USA, is one of the two foreign chip makers for Indian EVMs.

Once an EVM is stolen, and given that reverse engineering of both the hardware and the software are feasible, it is possible to manufacture as many dishonest look-alikes as needed (with suitable modifications to the hardware and software to facilitate manipulation and steal votes), and substitute these counterfeit/tampered EVMs for the real EVMs in the warehouses during the non-election period, with insider collusion, and without the ECI suspecting that anything is amiss.

We can also visualise an alternative scenario where a few skilled technicians gain access to a warehouse for several days or nights in a row, with insider collusion, and working on-site, they replace the regular CPU with the dishonest look-alike CPU (programmed with a vote-stealing Trojan and with an embedded Bluetooth device) in respect of a certain percentage of EVMs.

In my opinion, there is a major security loophole during storage at the district level which can potentially be exploited by the ruling party in the State. The fact that Prof. Halderman was able to get hold of an EVM unofficially proves that the strong security for the storage of EVMs can be breached. Moreover, *RTI replies given by the Commission reveal that its EVM inventory management leaves much to be desired*. According to an article dated December 12, 2017 in *The Wire* and titled *"RTI Response raises serious questions about Security, Handling of EVMs"*, the ECI has admitted to at least 70 cases of theft of EVMs across three

There is a major security loophole during storage at the district level which can be exploited by the ruling party in the State.

[15] Vide Note 9 above.

[16] **United States Court of Appeals, Ninth Circuit**. Judgment dated April 8, 2002 in *Syntek Semiconductor Co., versus Microchip Technology Incorporated.*

States – Chhattisgarh, Gujarat and Madhya Pradesh – over successive elections[17]. Till date, no one has been convicted for theft of EVMs.

The RTI reply also revealed that there was a *very big discrepancy* between the number of EVMs that were *manufactured* by ECIL and BEL and those actually *procured* by the ECI with no satisfactory explanation as to what happened to the 'missing' EVMs. (Exports run to a few thousand machines only). For example, the discrepancy in the case of ECIL was 1,97,368 units of Control Units and 3,55,747 units of Ballot Units! This shows that there is no proper system in place for periodic reconciliation. There was also no satisfactory reply to the question as to how the old EVMs were disposed of. *So the possibility of large numbers of EVMs being out there in the wrong hands cannot be ruled out.*

There is no proper system for periodic reconciliation and no satisfactory answer as to how old EVMs are disposed of.

The ECI has issued instructions only in October 2017 for tightening security in warehouses including installation of CCTVs but it is understood that these instructions are yet to be implemented properly by most States.

C. At the stage of 'first level checks' prior to an election: The third loophole available to tamper with EVMs is when - prior to elections - all the machines are subject to *'first level checks'* in the field by 'authorised technicians' deputed by BEL and ECIL in order to detect and remedy hardware problems. These authorized technicians are also sometimes involved at various later stages of the election, such as preparing EVMs for polling and assisting officials during the count. This means a group of technically skilled insiders has full access to the machines and they could open and manipulate hardware during these checks without the knowledge of the EVM manufacturers or the ECI or the election officials. Since a large number of diverse players are involved, maintaining secrecy may not be easy but there is no gainsaying the fact that a clear vulnerability exists.

Even more alarming is the fact that there is no proper vetting of these technicians by the ECI or the EVM manufacturers. According to the same article dated 6.12.2017 in *The Wire* (referred to earlier) there is the alarming finding that ECIL had not deputed its own technical personnel but had deputed technical personnel from (outsourced) private entities and had also deputed several

[17] **Bhatnagar, G.V. 2017**. Article titled *RTI Response raises serious questions about Security, Handling of EVMs* and dated December 6, *The Wire*. Available at https://thewire.in/government/evm-tampering-rti

unauthorised non-technical persons for the 'first level checks' of EVMs - in brazen violation of the administrative and security protocol mandated by the ECI[18].

One can *anticipate* the ECI's likely comments (in italics) on the three types of security loopholes narrated in paras A, B and C above. My responses are also given below.

(i) Administration operates on 'trust' and the ECI has to have faith in the integrity of the election insiders unless something adverse comes to its notice.

The problem could be that EVM fraud may never come to the ECI's notice or it may come to its notice rather late - by which time enormous damage could have been done. The Russians have a saying: *"Trust but verify"*. The ECI cannot afford to repose blind trust in myriad players over whom it has minimal administrative control and technical control and has no means of verifying if they are playing foul. This applies specially to the two EVM manufacturers and their authorised agents.

(ii) There are far too many persons involved and any one of them can become a whistle-blower and make information public on any such misadventures.

The fraud may be known to only a few members of a tightly knit group and may not come out. The recent PNB scam shows how several insiders can collude for a long time without anyone blowing the whistle. In fact, this is true of most scams within government; they seldom come out. Moreover, the experience of whistle-blowers world-wide has been that they run a very high risk of being victimised and of their mission not succeeding, and so many a potential whistle-blower may choose to simply keep quiet.

(iii) The various scenarios of 'insider frauds' cited are far-fetched with very low probability of their occurring.

The probability is non-zero. In other words, these insider frauds with EVMs are *not impossible*. There is a common human tendency to equate the 'very difficult' with the 'impossible'. Climbing Mount Everest solo and without supplemental oxygen may seem impossible but it is 'merely' very difficult and has been done by several mountaineers. Likewise, merely because committing a fraud is very difficult, it doesn't mean that it is impossible. The only things that are impossible are those which are forbidden by the laws of nature. There is a famous saying of Sherlock Holmes: "When you have eliminated the impossible, whatever remains, however

[18] **Ibid**.

improbable, must be the truth".[19] We may modify this to come up with the following maxim: *"Since EVM tampering is not physically impossible, someone, somewhere, at some time, will find a security loophole and exploit it however improbable the tampering scenario may seem at first sight."* And, once the security is breached, the probability of EVM fraud recurring will increase greatly with time.

Remedial Measures: In my opinion, there is a fairly good chance of fraud occurring at the EVM manufacturing stage and during storage at the District level and, to a lesser extent, at the stage of "first level checks" prior to an election. The ECI will be committing a grave mistake if its strategy to prevent fraud relies too much on the integrity of the officials of BEL and ECIL and the district election officials. It needs to put in place additional systems that will help check fraud at all the 3 stages indicated above.

1. *Procurement and supply of "Authentication Units" to detect Counterfeit EVMs*:

In the electronics industry, counterfeit components and devices are a big problem. Many of the components appear genuine but are actually substandard and compromise the efficiency and functionality of the final product in which they are used. There are ways of testing electronic components and devices, and either determine that they are counterfeit or authenticate them as genuine.

At present, the ECI and the election officials have no means of sifting the genuine EVMs from the counterfeit ones. To detect such fraud, the post-2006 second generation (M2) EVMs have a provision to interface with an *Authentication Unit*. Although the EVM manufacturers had developed and tested such an Authentication Unit way back in 2006, the ECI mysteriously shelved the project.

The ECI claims that the post-2013 third generation (M3) EVMs have certain new features for (i) Mutual authentication among all components of EVMs such as Ballot Unit, Control Unit and VVPAT and (ii) Automated self-diagnostics. These new features are obviously worthless if some of the tampered EVMs were supplied by the EVM manufacturers themselves! Even when the tampering is done at the district level, if the machines were to do any such authentication *themselves*, a Trojan can be easily designed to clear this self-test. So, these *self-authenticating* features in the M3

The ECI must procure and supply one or more Authentication Units to each district.

[19] The quote is from Sir Arthur Conan Doyle's "The Adventure of the Blanched Soldier", a 1926 Sherlock Holmes story.

machines may not be of much avail to prevent fraud. What are needed are *external* Authentication Units that can interface with EVMs.

Just as counterfeit currency detector machines are imperative for verifying the genuineness of currency notes, the ECI must procure and supply one or more Authentication Units to each district to help election officials verify whether the EVMs being used in their districts are genuine EVMs supplied by BEL/ECIL or counterfeit EVMs. Not only can Authentication Units detect and weed out the counterfeit EVMs, if any, in circulation, but they will also act as a *deterrent* because the knowledge of their existence will scare off potential fraudsters. *If VVPAT can help detect frauds at the counting stage, Authentication Units can help detect counterfeit EVMs even before polling. Both systems are essential.*

Normally, the Authentication Units are supplied by the manufacturers of the electronic components/equipment. But in this case, the Authentication Units should *not* be manufactured by BEL & ECIL (since there is scope for tampering of EVMs by them) but by an independent third-party manufacturer. For this purpose, the ECI will have to direct BEL & ECIL to place their EVM models at the disposal of the third-party manufacturer who shall be bound by a confidentiality agreement.

The authentication verifications should be arranged by the DM-DEO in the presence of the contesting candidates after the 'first level checks' are over and before the date of polling. *If it turns out that all the EVMs are genuine, then it will reinforce the confidence of the voters in the electoral process and will effectively silence the critics of the Election Commission.* The days of reposing blind faith in election insiders are over. So, the procurement and supply of one or more Authentication Units to each district is an absolute imperative that brooks no further delay.

The days of reposing blind faith in election insiders are over.

2. *Completely overhauling the present method of storing EVMs during the non-election period.*

There are 640 districts in India (according to the Census of India, 2011), some of them in remote, hilly and forested areas. As mentioned earlier, finding suitable storage places for EVMs is very difficult and the quality of the rented warehouses is highly variable across districts. We have seen that the storage of EVMs during the non-election period in multiple locations in each district in archaic warehouses with poor security systems in place is a *weak link* that increases the risk of EVM tampering.

It is suggested that the ECI should move towards a kind of "2-bin storage system" wherein the long-term storage of the EVMs in between two elections shall be in a few large, high-security, *regional warehouses* and the short-term storage immediately before or during an election in the current *district warehouses*.

The ECI must invest in building 2 or 3 regional warehouses in each State. The cost of constructing such modern regional warehouses in each State is not much, and in any case, cost should not be a consideration in ensuring the integrity of our electoral process. It is obviously much easier to monitor on a long-term basis 2 or 3 large warehouses than 100-and-odd smaller warehouses scattered across a State. The fewer regional warehouses also make it much easier for the Commission to manage the *logistics* of randomization/shuffling of EVMs from one State to another.

Cost should not be a consideration in ensuring the integrity of the electoral process.

These regional warehouses must be modern buildings with CCTVs and sophisticated electronic locking systems for the strong rooms where EVMs are stored, and they should be provided with 365x24x7 *police security* of the kind given to bank vaults or mints. The Chief Electoral Officer (CEO) of each State must be made responsible for the overall custody of the regional warehouses. He can be assisted in this important function by a full-time Joint CEO drawn from the IAS or IPS.

The 'codes' for these sophisticated electronic locks should remain with the ECI or the CEO. There should be mechanisms for alerting the (local) DM-DEO, the CEO as well as the ECI through SMS and email whenever the locks are opened, closed or tampered with and for maintaining an electronic log of all activities. Necessary precautions against hacking of these electronic locking systems should be taken by engaging the best experts in the field.

The 'first level checks' of the EVMs and VVPATs that are carried out by the 'authorised technicians' of BEL and EVM before an election *must be done only in these regional warehouses under CCTV*. Written declarations of the changes, if any, carried out must be obtained from each authorised technician before his exit and counter-checked by another authorised technician so as to fix responsibility. If there are serious discrepancies between machine-counting and hand-counting in respect of a polling station, and if the forensic examination of the EVM shows that it has been tampered with, then the concerned 'authorised technicians' and their supervisors in BEL and ECIL must be taken to task. At present, control mechanisms are extremely lax.

It should be possible to implement this suggestion within three years.

3. Engaging the services of a credible electronic security firm

In place of, or in addition to, the present system of assessing the security of EVM hardware and software through a 'Technical Experts Committee' consisting of a few Professors, the ECI must consider engaging the services of a top electronic security firm of international standing and credibility (bound by a confidentiality agreement) to conduct periodic ethical hacking and other modes of attack on its electoral systems and processes, identify loopholes if any, and certify their robustness. It must also send its EVMs for ethical hacking to the Annual DEF CON Conference in Nevada, US, to check if they are really tamper-proof and get valuable insights and suggestions for their improvement.

The ECI must face the truth that BEL and ECIL are not Apple and Google, and have not exactly fired the imagination of the industrial and commercial world with their products! If Apple and Google, which engage some of the best minds in the world, are willing to pay "bugs bounty" to ethical hackers for pointing out the glitches in their products, it would be naïve to place too much trust in the EVMs manufactured by BEL and ECIL when they have not been subjected to ethical hacking. "*Build a better mousetrap, and the world will beat a path to your door"* is a well-known saying. If the EVMs manufactured by BEL and ECIL were really all that 'perfect', they would have been flooded with orders from many countries whereas their annual exports run to only a few thousands, mostly to less developed countries.

VIII. ECI's ADMINISTRATIVE SAFEGUARDS ARE NOT FOOLPROOF

In the previous chapter, we examined issues relating to physical security of EVMs, the secrecy of their firmware and the integrity of election insiders. In this chapter, we will examine the efficacy or otherwise of the administrative safeguards that the ECI has put in place to prevent electoral fraud.

The fallacy of 'safety in numbers': A favourite argument of the ECI is that there is "safety in numbers", and physically tampering with a large number of EVMs is difficult because there are so many of them. This is not correct. *A small number of closely contested seats (or 'marginal constituencies') often determine which party holds a majority in a Legislative Body, and hence it would be enough to tamper with only a small percentage (3 per cent ? 5 per cent ? 10 per cent ?) of EVMs.* A party will not put the 'counterfeit EVMs' to use in constituencies where it is very confident of winning and also in constituencies where it has no hope of winning; it may put them to use only in marginal, closely fought constituencies.

In the Hollywood movie *"The Imitation Game"*, based on the real-life story of the famous British mathematician and code breaker Alan Turing, the British were trying to decrypt the *Enigma* machine which the Nazis were using to send coded messages. Turing and his team had succeeded in decrypting Enigma but the British realised that they could not act on every decoded message or else, the Germans would realise that the Enigma had been broken. So, the British used the decoded messages to avert German attacks only on *some select high value targets* and permitted German attacks on other targets to continue in the larger interest of making Germans believe that Enigma was intact.

The same logic applies to EVM tampering. If a party resorts to it large scale or wins in constituencies where it is known to be weak, its cover will be blown! So EVM tampering will be done very selectively with only a few machines. Like computer hacking, phone tapping, secret code cracking or other similar undercover activity, EVM tampering is successful only when the victim trusts the system and continues to use the tampered system.

Randomisation of allotments: The ECI believes that the randomisation of allotments of EVMs at the national level from the EVM manufacturers to various States, and the randomisation of

allotments within a district to various polling stations are sufficient safeguards against misuse. Of late, the ECI has been diverting the EVMs used in one State election – wholly or partly - to another State to prevent mischief. It must be noted that the unique identifying number of each EVM helps, not just the ECI, but also the attackers to keep track of the movements of tampered EVMs!

Randomisation needs to be done but it is not sufficient to prevent fraud. *Randomisation will ensure only the uniform distribution of the counterfeit EVMs among all constituencies rather than their skewed distribution among a few constituencies.* If, say, N per cent of the total number of EVMs have been tampered with – in the manner discussed in paras A, B and C of chapter 7 - then randomisation of allotments will merely ensure that, *on an average*, N per cent of the EVMs in all the constituencies are likely to be counterfeit! *With the assistance of insiders in BEL/ECIL and in the district administration, and since each EVM has a unique identifying number, the attacker can know precisely which tampered EVM has been allotted to which State and district, and within a district to which polling station.* (If the attacker is also the ruling party of the day in the Centre or the States, this task is relatively easier).

Randomisation poses no problem to national parties like BJP and Congress which have a significant presence in most of the States. If they have with them the unique identifying numbers of the tampered EVMs that have been diverted, they can track them and use them in the receiving State also. It is only the regional parties which have a presence in only one State/UT that may be handicapped due to randomisation. Hence, randomisation is not really a protection against a smart and determined attacker aided by insiders.

Randomisation is not really a protection against a smart and determined attacker aided by insiders.

Candidate Ordering: To the question *"Can ECI-EVMs be manipulated by Manufacturers?",* the ECI's reply is as follows:

> "Not possible . . . The manufacturers are in no position to know several years ahead which candidate will be contesting from a particular constituency and what will be the sequence of the candidates on the Ballot Unit . . . So, any manipulation at manufacturing stage is ruled out."[20]

But this reply is misleading. It is nobody's case that BEL and ECIL can rig the machines to favour particular candidates several years ahead. What the 2 EVM manufacturers can do is to secretly manufacture a certain percentage of 'remotely operable and hackable machines' with

[20] Vide Note 11 above. Reply to Q.3 of FAQs.

look-alike but dishonest hardware and software that can be put to use at any time in the future by whoever has knowledge of which machines they are and where they are. As discussed in para A of Chapter 7, the danger is very real and it can happen without the knowledge of the ECI and may even be done by some rogue employees without the knowledge of the top management of BEL and ECIL.

The names of the contesting candidates are arranged in alphabetical order in the Ballot Unit of an EVM – first, candidates of recognised National and State political parties, then, candidates of registered but unrecognised political parties, and finally independent candidates. The final list of candidates is published only about 14 days before the date of the polling and this is the earliest a potential attacker would know the precise order of any party's candidate on the Ballot Unit. It is sometimes argued that this window is too short for an attacker to develop a Trojan and execute his plan.

The mistake with this line of reasoning is that it assumes that the tampering of the EVMs takes place just before or during polling and just before or during counting. Since the supervision gets tighter once the election schedule is announced, it makes far more sense for an attacker to do the tampering of EVMs well before the elections, as described in paras A, B and C of chapter 7, when the supervision is lax or non-existent. Hence, tightening the supervision only after the election schedule is announced may well be like the proverbial closing of the stable doors after the horse has bolted. But the *actual perpetration* of the vote stealing fraud - with the help of the tampered EVMs - may take place unnoticed on the polling day or any time before the counting begins.

The ECI seems to have assumed a particular mode of attack for which the attacker triggering the Trojan to steal the votes has to know the precise sequence of the candidates on the Ballot Unit. *But it is perfectly possible to steal votes with a simple Trojan even if the attacker doesn't know the precise sequence of candidates on the Ballot Unit.* This is because, in most constituencies, *the fight is between two major parties only* and the rest don't really matter.

Let us suppose that Party X and Party Y are the only 2 serious contestants in a constituency and that Party X knows precisely which polling stations have the tampered EVMs, and among these polling stations, it knows fairly accurately in which polling stations it is likely to come a clear first, in which polling stations it is likely to come a clear second, and in which polling stations the margin may be too close to call. An agent of Party X can trigger off the Trojan in the tampered EVM in a polling station through a remote device to become active around, say, 5.30 pm on the polling day. This Trojan could have been so programmed that pressing a button on the remote device transfers,

say, 10 per cent of the votes from the party that has polled the highest number of votes to the party that has polled the second highest number of votes. In polling stations where Party Y is likely to come first and Party X a reasonably close second, the attacker will press the button that will make the Trojan transfer 10 per cent of the votes from Y to X. When things can be done this way, it is not necessary to know the precise sequence of the party's candidate on the Ballot Unit. It is necessary to know only whether the party is likely to come first or second in the area covered by the particular polling station which field functionaries of political parties would normally know with a high degree of precision. While such vote stealing can also be done anytime during the period when the ballot boxes are stored after polling is over and counting is yet to start, it can be done easiest towards the fag end of the polling day.

The precise mode of vote stealing depends upon how the Trojan has been programmed. With a more advanced Trojan, and with the 14-day window during which the sequence of the candidates on the Ballot Unit is known, various kinds of vote transfers between candidates can be done on the polling day. It would be a grave mistake to underestimate the technical prowess of the attackers. The Trojan can also be programmed to self-destruct after doing its mischief.

Thus, the administrative safeguards that the Election Commission relies on are not foolproof and are not sufficient to prevent attacks by any determined attacker with assistance from an insider. From a conjoint reading of chapters 6, 7 and 8, it will be clear to any unbiased reader that, *even under election conditions and with all the security features and administrative safeguards in place*, it is possible to tamper with EVMs and steal votes on a scale large enough to change election outcomes. Luckily, the remedies are simple and effective: use of Authentication Units before the polls to weed out counterfeit/tampered EVMs and effective use of VVPAT at the time of counting to guard against wrong counting due to EM tampering.

IX. SUMMARY OF FINDINGS AND RECOMMENDATIONS

Let us quickly recapitulate what we have discussed so far:

- The controversy over the security of paperless EVMs is not something new (it dates back to the early 2000s) and is not confined to India (it is world-wide).

- A consensus has emerged that paperless EVMs are "black boxes" that lack transparency and verifiability. Like all electronic equipment, they are prone to equipment malfunction and tampering but the mistakes or frauds are undetectable and the losers are left with no means to challenge the results.

- There is an imperative need for an additional verifiable physical record of every vote cast, in the form of voter verified paper trail (VVPAT), a portion of which should be hand counted and compared with the corresponding machine count to see if the two totals tally. In 2013, the Supreme Court of India held that VVPAT is necessary for the conduct of free and fair elections and to restore confidence among voters that their votes have been correctly recorded and counted.

- For reasons best known to it, the Election Commission of India (ECI) has given the impression that it is not serious about VVPAT. There is inordinate delay in procurement of VVPAT units. Until June 2018, the ECI had received from BEL and ECIL *only 22 per cent of the VVPAT units* that it had placed orders for.

- The ECI's action of prescribing a minuscule sample of EVMs for hand-counting of VVPAT slips (only one EVM per Assembly Constituency, which worked out to just 0.36 per cent, 0.9 percent and 0.40 per cent respectively for the Gujarat, H.P and Karnataka Assembly Elections) is questionable, statistically unsound, and is nearly as bad as not implementing VVPAT at all. The ECI seems to have chosen the sample size arbitrarily when, in fact, its selection should have been grounded in standard statistical sampling theory. It is open to legal challenge.

- The ECI should arrive at the *statistically significant sample size* for the State as a whole for a Confidence Level of *not less than* 95 per cent and a Margin of Error of *not more than* 2 per cent using a ready reckoner. This sample may then be apportioned among the various Assembly Constituencies in proportion to the number of polling stations in each Constituency.

- There is need for stratified sampling with a random sample of one or more polling stations drawn from each of the following groups (or 'strata') of an Assembly Constituency: urban, semi-urban, rural, those in remote hilly/desert/forest areas, those with very heavy voter turnout (> 80 per cent), those with moderate voter turnout (50 per cent to 80 per cent), those with low voter turnout (<50 per cent), and so on.

- If the margin of victory of a candidate is less than, say, 2 per cent, and irrespective of the margin of victory, if the discrepancy between the machine-counting total and the hand counting total in respect of the selected sample of EVMs *taken together* is considered statistically significant as per standard methods of statistical Hypothesis Testing, then the ECI may make it mandatory to order the hand counting of VVPAT slips for all the polling stations.

- When the entire election process, from the date of announcement to the date of counting, lasts for 2-3 months, there is no reason why unseemly hurry should be shown only in the case of counting. In the rush to declare results and the winners, the ECI cannot turn a blind eye to the possibilities of wrong totalling due to EVM malfunction or EVM tampering.

- The ECI's claims that its EVMs are "unique" and that its security protocol and administrative safeguards are "foolproof" are exaggerated. All the features and safeguards relied on by the ECI can be easily negated by *insider fraud*.

- There is no justification to trust insiders in the election ecosystem any more than trusting the insiders in currency printing presses, banking, insurance, gambling and examinations ecosystems where sophisticated frauds continue to occur despite equally good safeguards as the ECI's being in place, if not better ones.

- The ECI has reposed excessive trust in BEL and ECIL and it has no means of verifying if they are playing foul. 'Trust but verify' should be the Election Commission's motto. To do this, the ECI must equip itself to exercise greater administrative and technical control over them in so far as the manufacture, checking and servicing of EVMs are concerned.

- The inventory management of EVMs leaves much to be desired and, besides thefts, there are huge discrepancies in figures of EVMs (running to lakhs!) between the ECI and the two EVM manufacturers as per RTI replies.

- Once an EVM is stolen, and given that reverse engineering of both the hardware and the software are feasible, it is possible to manufacture as many dishonest look-alikes as needed (with suitable modifications to the hardware and software to facilitate manipulation and steal votes).

- It is possible to substitute large numbers of tampered/counterfeit EVMs for genuine EVMs without the knowledge of the ECI at three stages: (i) at the EVMs manufacturing stage in BEL and ECIL; (ii) at the district level, during the non-election period when the EVMs are stored in archaic warehouses in multiple locations with inadequate security systems; and (iii) at the stage of 'first level checks' prior to an election when the EVMs are serviced by 'authorised technicians' from BEL and ECIL. There is a *fair chance* of fraud occurring at the first two stages and, to a lesser extent, at the third stage.

- The threats to the integrity of our electoral process need not come only from ruling parties of the day in the Centre or the States; they could come from foreign attackers also. Other potential attackers are terrorists who may wish to disrupt elections in order to spread confusion and distrust or rogue employees of EVM manufacturers who may do it for money.

- The "safety in numbers" argument is not correct because a potential attacker would try to steal votes and change election outcomes very selectively, with only a few machines, and only in marginal, closely fought constituencies.

- Randomisation of allotments of EVMs at the national level and within a district needs to be done but it poses no problem to national parties like BJP and Congress. If, with insider help, they have with them the unique identifying numbers of the tampered EVMs that have been diverted, they can track them and use them in the receiving State also.

- The ECI's claim that EVM manufacturers are in no position to know several years ahead which candidate will be contesting from a particular constituency and what will be the sequence of the candidates on the Ballot Unit, and so, any manipulation at manufacturing stage is ruled out, is misleading. What the 2 EVM manufacturers can do is to secretly manufacture a certain percentage of 'remotely operable and hackable machines' with look-alike but dishonest hardware and software that can be put to use at any time in the future by whoever has knowledge of which machines they are and where they are.

- In most constituencies, the fight is between two major parties only. A simple Trojan which can steal, say, 10% of the votes from the party securing the highest number of votes and transfer

it to the party securing the second highest number of votes in a polling station can be conceived of. For this, the attacker doesn't need to know the precise sequence of candidates on the Ballot Unit at all. With a more advanced Trojan, various kinds of vote transfers between candidates can be done. The precise mode of vote stealing will depend upon how the Trojan has been programmed.

- BEL and ECIL are not Apple and Google, and have not exactly fired the imagination of the industrial and commercial world with their products! The ECI would be making a grave mistake if it overestimates the security features of its EVMs and its administrative safeguards, and underestimates the technical prowess of the attackers, or if it thinks that Indian politicians are not 'hi-tech' enough to resort to such manipulations.

- *Authentication Units* can help election officials verify whether the EVMs being used in their districts are genuine EVMs supplied by BEL/ECIL or counterfeit EVMs. They also act as a *deterrent* because the knowledge of their existence will scare off potential fraudsters. They should *not* be manufactured by the EVM manufacturers (BEL & ECIL) but by an independent third-party manufacturer. (The self-authenticating features of the post-2013 M3 EVMs are not a substitute for authentication by an external device).

- Contrary to the ECI's claim, even under election conditions and with all the security features and administrative safeguards in place, it is possible to tamper with EVMs and steal votes on a scale large enough to change election outcomes. Luckily, the remedies are simple and effective: use of Authentication Units before the polls to weed out counterfeit/tampered EVMs and effective use of VVPAT at the time of counting to guard against wrong counting due to EM tampering. Both systems are essential.

- So, two immediate and important courses of action before the ECI are (1) to adopt the correct sample size of EVMs per Assembly Constituency for hand counting of VVPAT slips based on standard statistical sampling theory, and (2) to procure and supply one or more Authentication Units to *each district*. If the VVPAT and Authentication Units show that all the EVMs are genuine, then it will reinforce the confidence of the voters in the electoral process and effectively silence the critics of the Election Commission.

- Confidence in the integrity of EVMs is important for voters to trust the outcomes of elections and the legitimacy of governments formed as a result of them. The ECI cannot allow this confidence to be eroded. But if the ECI persists with its minuscule sample of EVMs for hand

counting VVPAT slips or drags its feet in the procurement of Authentication Units, then an adverse inference is liable to be drawn against it and it may lose the perception battle.

- In place of, or in addition to, the present system of assessing the security of EVM hardware and software through a 'Technical Experts Committee' consisting of a few Professors, the ECI must consider engaging the services of a top electronic security firm of international standing and credibility (bound by a confidentiality agreement) to conduct periodic ethical hacking and other modes of attack on its electoral systems and processes, identify loopholes if any, and certify their robustness.

- The ECI must also send its EVMs for ethical hacking to the Annual DEFCON Conference in Nevada, US, to check if they are really tamper-proof and get valuable insights and suggestions for their improvement.

- Over the next three years, the ECI should consider moving towards a kind of "2-bin storage system" wherein the long-term storage of the EVMs in between two elections will be in a few large, high-security, *regional warehouses* (one to three for each State) and the short-term storage immediately before or during an election in the current *district warehouses*.

- In the long-term, the ECI may consider phasing out VVPAT EVMs as and when they get old and switching over to machine-readable paper ballots that can be counted rapidly with OMR technology. This is because the latter has all the advantages of paper ballots ('gold standard of voting') minus the delay in counting and can protect voter anonymity which VVPAT EVMs can't. In machine-readable paper ballots, the primary ballots are in paper form and the secondary ballots are in electronic form whereas in EVMs with VVPAT, the primary ballots are in electronic form and the secondary ballots are in paper form. Machine-readable paper ballots are superior to EVMs with VVPAT as paper is more secure than electronic memory and primary paper ballots are superior to secondary paper ballots. In fact, the ECI can trial machine-readable paper ballots straight away for the postal ballots that are cast by polling staff and servicemen working outside the places where they are registered as voters.

[This article was updated on October 3, 2018 after it was originally published on August 30, 2018].

About the Author

K. Ashok Vardhan Shetty is a former Vice-Chancellor of the Indian Maritime University, Chennai, a Central University under the Ministry of Shipping. Before assuming charge as the Vice-Chancellor, Shetty was a member of the Indian Administrative Service (IAS), Tamil Nadu Cadre, of the 1983 batch. He held a number of key assignments including Registrar, University of Madras, Director of Collegiate Education; District Collector, Viluppuram; Director of Rural Development; Managing Director, Tamil Nadu State Marketing Corporation, (TASMAC); Secretary, Chief Minister's Secretariat; Principal Secretary, Rural Development and Panchayat Raj Department; Principal Secretary, Municipal Administration and Water Supply, among others. Successful project implementation was his forte. He was commended by the Government of Tamil Nadu several times.

Shetty has published several articles on public administration, management, E-Government, popular science, and popular mathematics in leading English and Tamil newspapers such as The Hindu, The Hindu - Tamil, The Hindustan Times, Indian Express, The Hindu BusinessLine, and (the now defunct magazine) Science Today.

He can be contacted at shetty25@hotmail.com

THE HINDU CENTRE
for
Politics and Public Policy

The Hindu Centre for Politics and Public Policy
Kasturi Buildings, 859 & 860, Anna Salai,
Chennai - 600002. Tamil Nadu, India.

Web: www.thehinducentre.com
Phone: +91-44-28576300
Email: thc@thehinducentre.com