THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

April 1, 2019

There is No Ghost in the Indian EVM

Or why if protocols are followed, hacking is close to impossible

By: Prabir Purkayastha,Bappa Sinha

No machine is hack-proof but the unique design of India's EVMs minimises such a possibility and if all the protocols are adhered to manipulation is highly unlikely. However VVPATs must be on a large enough scale to convince us of the integrity of the process.

For the past two decades now, the Election Commission of India (ECI) has used Electronic Voting Machines (EVMs) during polling. However, it is only in the last couple of years that doubts have been raised about whether EVMs can and have been manipulated by the ruling Bharatiya Janata Party (BJP) to rig elections. Quite often we hear that if so many countries have rejected EVMs, why should India adopt this at all? Is this not a threat to our democracy?

Many are sceptical of using such machines in elections, arguing that India, like many other countries, should return to paper ballots. The ECI has categorically rejected a return to paper ballots, and has said that taking all procedures into account, it is sure that fixing the elections by tampering with the EVMs cannot happen.

While any machine can be hacked, we believe that with the technological safeguards—in the design of EVMs and the processes followed during the design, coding and manufacturing of EVMs—along with the elaborate system of procedural checks in place that include the participation of political parties, it is unlikely that large-scale EVM rigging can be done. This article describes and discusses both these aspects: the technical design of the EVM and the procedures in place that ensure that large-scale rigging of these voting machines is improbable.

We also discuss the validity of the allegations and experiments made to demonstrate that the EVMs can be hacked. Finally, we discuss the importance of conducting a meaningful, Voter Verified Paper Audit Trail—or VVPATs—that have been mandated by the Supreme Court to be used in the elections along with the EVMs. What should be a realistic approach to tallying VVPAT paper slips with EVM vote count? Demands that a more extensive VVPAT be carried out are now being heard in the Supreme Court.

Types of Voting Machines and International Experience

There are two types of electronic voting (e-voting) machines: direct recording electronic (DRE) voting machines, and remote electronic voting using the internet (also called i-voting).

Why have EVMs been opposed in other countries, and why do we feel that India’s case of EVMs is different? A number of countries are introducing or are thinking of introducing what they call “internet voting”. This means that the voter can vote in the elections without going to the booth – she would be able to access the voting system through the internet. As we now know, any connection to the internet would not only allow the person to vote, but also provide an entry point for hackers. Therefore, no EVM that connects to the internet is ever going to be a safe system for the elections.

The second issue is that again in most countries where EVMs have been sought to be introduced, they have been designed using a standard PC as the base machine with custom coding for converting it into an EVM. Worse, most of these machines, even when they do not allow internet voting, allow internet connectivity for various purposes, including remote initialising, tallying of votes, etc. Further, such machines are well known, and so are their security holes. Any hacker worth the name can hack into these machines relatively easily.

The Dutch machine—NEDAP/Groenendaal ES3B—has been extensively studied by researchers (Gonggrijp and Hengeveld 2006). Ron Gonggripp is the founder of the Group “We don’t trust voting machines”. These machines were extensively used in various countries including Germany. They have all the problems that we have identified here – they have a MS-Windows operating system, have external serial and printer ports, and a maintenance mode to access virtually anything in the machine. They even emitted radio waves that could be detected from a distance of a few metres and used to find out who was voting for which candidate. Obviously such a machine is easy to hack. After the entire software toolkits of NSA and the CIA have been dumped on the internet, backdoors to systems with standard operating systems like MS-Windows, and the ability to hack them is that much easier. However, the criticism of these machines cannot automatically be translated to the Indian EVMs because the Indian machines neither have an operating system nor are they connected to the internet.

It is instructive to note that even when the German court struck down the use of NEDAP EVMs, it said that it was open to an EVM that would meet the explicit criteria in German law that are required for verification of voting.

> [T]he Indian EVM is a unique and suis generis machine.

It is also not true that EVMs are used only in India. There are a few countries that use EVMs – Brazil, Estonia, and Venezuela – being among them. Estonia uses internet voting, while Brazil and Venezuela has DRE based voting machines. Venezuela also uses VVPATs with their EVMs. But as is argued below the Indian EVM is a unique and suis generis machine.

> The key feature of the EVMs in India is that in essence they are giant calculators. They do not have programs that can be changed without physically altering the machine; they do not even have an operating system.

The US too uses EVMs, though only in some states and local levels. The election processes in the US are controlled at the local and state levels, and there is no uniformity in these processes. What is far more prevalent in the US is for voters to bring their printouts of the ballot including their votes as cast, and then optically scan these printouts. These optically scanned votes are then automatically tallied and the results declared based on this tallying of the scanned printouts. However, the physical ballots are also preserved and can be counted in case of disputes. Unlike in India, in the US, there is no uniformity in either the election procedures across the country nor is there an authority like India's Election Commission that oversees the entire election process from the local to the country level.

The key feature of the EVMs in India is that in essence they are giant calculators. They do not have programs that can be changed without physically altering the machine; they do not even have an operating system. Therefore, one major pre-requisite for hacking—of being able to change the program externally—does not exist in the system. The second important feature is that there is no internet connection in the system. Therefore, the EVMs cannot be manipulated either through the internet or as is being argued with a WiFi device.

In this sense, Indian EVMs are different from most other voting machines being sought to be introduced, particularly in the western world, where labour saving in the elections, ease of voting etc., have been the major consideration. A discussion of the design and technical safeguards in the design and manufacture will help explain the special nature of Indian EVMs

Technological Safeguards

The design of the EVMs used in India is based on some key design principles that make the usual modes of attack on such machines unachievable. The ECI mandated that the EVMs should be stand-alone and "one time-programmable" machines, which are neither computer controlled nor connected to the internet or any network at any point of time.

The EVMs used in India are therefore quite unique in this fashion as compared to EVMs used in various western countries. The Indian EVMs can be categorised as a special class of DRE machines that are not connected to the internet.

The fact that the Indian EVMs are standalone with no provision of connecting them to the internet or any external network by itself prevents any kind of "networked" attacks on them. This category of attacks is the most common one faced by electronic or digital equipment since connection to an external network of any kind allows attackers to hack machines remotely without direct physical access.

As Indian EVMs do not have any wired network connectors such as RJ-45 connectors and also do not have wireless receivers/transmitters such as WiFi, mobile signals, Bluetooth, etc, potential attackers cannot remotely connect to these machine and hack them.

The other key design principle is that the software used in these machines is burnt into a "One Time Programmable" chip that makes it impossible to alter or tamper with the software on these machines. As its name implies, a One Time Programmable chip can only be programmed once at the time of manufacture and cannot be reprogrammed subsequently. So the software programmed in the chip cannot be modified without replacing the physical chip itself by another.

> [T]here is a rigorous set of processes that is followed during the design, coding and manufacturing of the Indian EVMs, which ensures the sanctity of the design, and manufacturing processes of the hardware and software.

This is unlike regular PCs or servers where the operating systems and other software running on the computers are stored on drives which can be rewritten. Viruses and other malicious software often modify the original software stored in these drives in order to “hack” the machines. Hence the only way these machines can be hacked is if the original software programmed into these EVMs itself was compromised or hardware components of the EVMs are replaced in the field.

We argue that there is a rigorous set of processes that is followed during the design, coding and manufacturing of the Indian EVMs, which ensures the sanctity of the design, and manufacturing processes of the hardware and software. Also, the elaborate administrative procedures mandated for the transport, handling and operations of EVMs before, during and after elections make it very unlikely for the hardware to be replaced on a scale large enough to affect state and national elections.

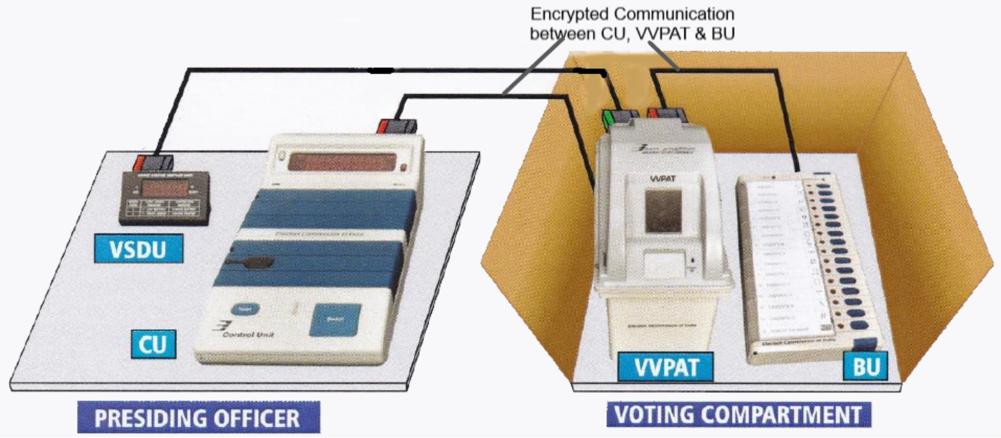

Figure 1: EVM Components. Original Diagram from ECI’s EVM & VVPAT Status Manual.

Figure 1 shows the deployment of the various components of an EVM. The EVM consists of a control unit (CU) that is placed on the presiding officer’s desk. This CU is connected to the Voter Verifiable Paper Audit Trail (VVPAT) printer that is then connected to the ballot unit (BU). The VVPAT printer and the BU are kept in the voter booth. The VVPAT status display unit (VSDU) is kept with the presiding officer and displays the status of the VVPAT printer. With the latest version of VVPATs, the VSDU is no longer required as its functionality has been incorporated into the VVPAT printer unit.

In order for a vote to be cast, the presiding officer must first enable the BU by pressing a button on the CU. The BU becomes active only after this is done and the voter can cast his/her vote by pressing a candidate button once on the BU. On a button press, the LED next to the button lights up and a long beep can be heard indicating that the vote has been recorded. The VVPAT simultaneously prints a small slip of paper that carries the symbol, name and serial number of the candidate chosen by the voter. This slip is visible for seven seconds in the viewing window.

Once one vote has been cast, the BU becomes inactive and does not respond to any more button presses till the presiding officer schedules the next vote by again, enabling the BU from the CU. Vote stuffing is not possible due to the feature that the CU cannot accept another vote in less than 12 seconds. Votes are date and time stamped, and no votes can be cast before or after the poll. These safeguards contain the likelihood of booth capture and ballot stuffing which used to be a problem before EVMs were introduced. Since the BU becomes unresponsive once one button is pressed, it is not possible to send secret codes to the CU using a series of button presses as was suggested during a demo organised by the Aam Aadmi Party in Delhi.

It is not that just because of the 12-second delay, booth capture cannot happen now it is just that the speed at which the “ballot stuffing” occurs will be slower. Earlier, one gang could go around from booth to booth serially capturing booths and stuffing the ballot boxes. The delay between successive button presses makes this process longer and therefore more difficult.

> The design, engineering and manufacturing processes are such that it is quite difficult for a single person or a small group of people to compromise the integrity of the software or the EVM machines as a whole at the engineering or manufacturing stage.

The ECI over time has added new features to the EVMs to further enhance their security and integrity. These include features like time stamping of BU key presses, digital certificates that are used by the different components of the EVM—CU, BU and VVPAT—to authenticate each other and which would stop working if paired with a fraudulent component. The communication between these components is encrypted in the M2 and M3 versions of EVMs that are currently in use (Status Paper on Electronic Voting Machine). This renders very unlikely attacks on the EVMs by tapping into the connecting wires between the components and inserting digital signals to change votes.

Design, Engineering & Manufacturing Processes

The design, engineering and manufacturing processes are such that it is quite difficult for a single person or a small group of people to compromise the integrity of the software or the EVM machines as a whole at the engineering or manufacturing stage.

The software of EVMs is developed in-house by a selected group of engineers in the defence ministry PSU, Bharat Electronics Ltd. (BEL), and in the PSU under the Department of Atomic Energy, Electronic Corporation of India Ltd. (ECIL) independently of each other. After completion of software design and development, testing and evaluation of the software is carried out by an independent testing group as per the software requirements specifications. This ensures that the software has been written to meet only the requirements laid down for its intended use.

Typically, programs are written by engineers in a programming language. This is called the source code that is human readable. Thereafter, the program is converted (“compiled” in technical parlance) into machine code which actually runs on the machine and is not human readable.

The “source code” for the EVMs is stored under controlled conditions at all times. Checks are in place to ensure that it is accessible only to authorised personnel. This is not to argue that such machine codes cannot be converted back to source form (or decompiled as it is called in technical language), but it is an additional barrier to hacking of the EVMs.

After completion of successful testing, only the machine code is given to the micro-controller manufacturer for writing it in the micro-controllers. (The micro-controllers effectively constitute the CPU of the EVM.) The source code is never handed over to anyone outside the software group of PSUs.

The micro-controller manufacturer initially provides engineering samples to PSUs for evaluation. These samples are then assembled into the EVM, evaluated and verified for functionality. Bulk production clearance by the PSU is given to the micro-controller manufacturer only after successful completion of this verification.

During production in the factory, functional testing is done by the production group according to the Quality Assurance (QA) plan that has been laid down. Samples of EVMs from production batches are regularly checked for functionality by the QA group, which is an independent unit within the PSUs.

After production, the EVMs are shipped to states for storage as directed by the ECI. All movement of EVMs is done through an EVM Tracking Software (ETS). Containerised trucks or sealed trucks with proper locking arrangements that are sealed using paper seals are used for transporting EVMs and VVPATs. These trucks are tracked using GPS. On receipt of the EVMs, the district election officers (DEOs) are supposed to video-graph the process of receipt of EVMs and then store them in strong rooms at the district headquarters.

Administrative Procedures

The ECI has put in place a detailed set of administrative procedures for the handling of EVMs before, during and after the elections. It is the combination of the technical design of the EVMs along with these processes that have to be examined when we talk of the low likelihood of EVM hacking. Without these physical checks in which political parties are also expected to participate, we cannot talk about the safety or otherwise of electronic voting.

> [E]nsuring the integrity of the EVMs does require the political parties and their representatives playing an active role at many of the crucial stages.

Pre-election procedures for EVMs start around 200 days before elections are held. As can be seen in Table 1, there is a comprehensive set of pre-election procedures to ensure that there is no tampering with the EVMs.

However, ensuring the integrity of the EVMs does require the political parties and their representatives playing an active role at many of the crucial stages.

An example is the set of preparations that happen 3 to 6 months before the polling date, depending on whether elections are being held for state or national elections. These procedures are critical for verifying the integrity of the EVMs and are therefore held in the presence of representatives of political parties.

The first of these procedures is the First Level Checking (FLC) of EVMs that is done at the district level by the engineers of the manufacturers. This is held in the presence of political parties' representatives. Since this happens some months before the state and national elections, political parties are often not aware of, or even if they are aware, they are not geared towards meaningfully participating at this stage of the process.

However, this is the only stage where it is possible to examine the internal parts of the EVMs to examine if suspicious modifications have been done to them. So it is crucial to send trained representatives at this stage.

After this, around three weeks before the polling date, the randomization process of EVMs is done to allocate EVMs to constituencies. Since, the position of a political party in the Ballot Unit is done alphabetically by candidate names, the position of the party on the Ballot Unit is different for each constituency. The randomization process ensures that any conspiratorial attempt to favour a particular political party by hacking EVMs and fixing a particular slot in the Ballot Unit will be thwarted.

Table 1. EVM Preparation Procedures Prior to Elections

Process	**Timeframe**	**Details**
Allocation of EVMs	200 days before polling	EC orders and allocates EVMs to States where elections are to be held.
Dispatch of EVMs	180 days before polling	EVMs are shipped in sealed trucks & tracked using GPS & ETS software.
First Level Checking (FLC)	3 to 6 months before polling	EVM Internal parts are examined by engineers of manufacturers. Mock poll conducted & CU sealed.
1st Stage Randomization	3 weeks before polling	EVMs are assigned to constituencies using ETS Software.
2nd Stage Randomization	2 weeks before polling	EVMs are assigned to polling booths.
Candidate Setting	After last day of Candidate Withdrawal	Ballot paper is fixed on BU. Candidate names are ordered in alphabetical order. Mock poll conducted & BU sealed.

There are likewise elaborate sets of protocols that govern operations on the polling day, then for storage and finally on counting day. These are summarised in Tables 2 and 3.

Table 2. Polling Day Procedures for EVMs

Process	**Details**
EVM Serial Numbers	Candidates should share the machine serial number of the EVMs (CU, BU & VVPAT) allotted to the specific polling station with their polling agents so that they can inspect the EVM/VVPAT to their satisfaction before the commencement of mock poll. Presiding officers should be asked to show the machine number to the agents present before the commencement of the mock poll.
Mock Poll	Mock poll is conducted at every polling station by the presiding officer by casting at least 50 votes in the presence of the polling agents. After which the presiding Officer tallies the result in the CU with the count of the VVPAT paper slips in the presence of the polling agents and confirms that the results tally for each candidate.
Actual Polling	After the mock poll is over, paper seals are put on the CU to block access to all buttons on the CU except those that are used for the conduct of the poll. These paper seals are allowed to be signed by the polling agents. It is only after this that polling can commence.
Close of Polling	After the close of polling, the presiding officer presses the “Close” button on the CU in the presence of polling agents. No votes can be polled after that in the EVM. The entire EVM is sealed. Polling agents are allowed to put their signatures on the seals. Candidate representatives travel behind vehicles carrying EVMs from polling stations to counting storage rooms. In addition to this, the strong rooms where EVMs are stored for counting are also sealed and secured fully by Central Armed Reserve Police Force guards round-the-clock. Additionally, candidates are allowed to put their own seals on the strong rooms and keep a around the clock watch.

Table 3. Counting Day Procedures

Process	**Details**
Serial Number & Seal Checks	Before the start of counting, the CU serial number & the Unique ID of the various paper seals are verified from records and shown to the counting agents. In EVMs, the poll start & end date, and time displayed on the CU should be verified from the record and shown to the polling agents.
Non-display of result due to the presiding officer not pressing the “Close” button.	In case any CU does not display the result due to the presiding officer in the polling station not pressing the “Close” button at the close of poll, the CU should not be included in counting and a report filed for these CUs.
Mismatch of total votes tally	In case the total votes polled as displayed by the CU does not tally with the total votes polled mentioned in the form filed by the presiding officer, the matter should be referred by the returning officer to the Election Commission for its decision.
Application for VVPAT paper slip counting	After the announcement of the results, any candidate or their counting agents may make an application for counting the printed VVPAT paper slips in any or all polling stations. The returning officer then passes an order on whether or not the VVPAT paper slips should be counted.

Claims of Hacking of Indian EVMs

In spite of the many safeguards that are in place – in design, manufacture and administrative – there have been claims that the Indian EVMs can be tampered with

A number of claims of EVMs being hacked have been made in India. It started in 2010 with J Alex Halderman of the University of Michigan in the US and his students (Prasad et al 2010) replacing parts of the machine and showing that it was possible – by changing the hardware – to change either the voting or the vote counts stored in the EVM. This could also be done remotely.

> There has never been any doubt that if the EVM hardware can be changed, of course it becomes a different machine.

A similar exercise was shown by Aam Aadmi Party (AAP) in May, 2017. In a demo, they showed essentially what Halderman and his team had done: change the hardware and then used the changed hardware to “hack” the EVM.

There has never been any doubt that if the EVM hardware can be changed, of course it becomes a different machine. In such a machine, it is easy to provide an external wireless interface through which results can be altered. Or pre-program a result, say, of transferring 10% votes from the number 1 position to say the number 3 position on the voting pad of the ballot unit of the EVM.

In the Indian EVMs, we vote by pressing a key on the keypad that has the name of the candidate and her party symbol displayed on that particular key. As the names on the keypad are allocated alphabetically, the position of the parties is not fixed on the voting pad. It changes from constituency to constituency based on the initials of the candidate. That means the BJP could be in 3rd position in one constituency on the voting keypad, and on the 1st position in another. For a hack by a particular political party to succeed, the hardware has to be first custom re-configured to match the constituency-wise position of that political party. Or the machine must have a wireless interface that can be dynamically controlled during or before the voting.

> The question is whether a large scale physical hacking of 1.6 million EVMs – the numbers involved in the Lok Sabha elections – is possible. Even if 10% of such EVMs are physically hacked, that still means physically tampering with as many as 160,000 EVMs.

That a physical hack of the Indian EVM can achieve this has never been disputed by anybody, including the ECI. The question is whether a large scale physical hacking of 1.6 million EVMs – the numbers involved in the Lok Sabha elections – is possible. Even if 10% of such EVMs are physically hacked, that still means physically tampering with as many as 160,000 EVMs.

After the AAP demonstration of “hacking” , the ECI issued a challenge to political parties to show that the EVM could INDEED be hacked. They set out very restrictive conditions, virtually saying, “Hack the EVM without touching it”. By posing a “challenge” and talking about “hackathons”, the EC unnecessarily created an adversarial relationship between itself and the political parties.

The issue is not whether or not EVMs can be hacked. The issue – as some of the parties have argued – is the need to examine the system in entirety, including the EVMs, the physical and human checks, to be certain of its integrity. This should have been done in a cooperative manner and not in the way the ECI conducted its so-called EVM hackathon challenge.

A history of EVM hacking will not be complete without mentioning the recent fiasco involving a shadowy figure who claimed that there was a criminal conspiracy in the public sector BEL to modify the software/hardware of the EVM. According to this claim, a wireless processor had been incorporated into the EVM and A low frequency wireless signal could be used to change the election results. This was initially touted as a high-profile press event in London, where “experts” would bring an EVM and show how it could be hacked.

The event turned into a fiasco. There were no EVMs. The US “expert” wasn’t there in person. Instead, we had a person on videoconference, most of whose face was covered as he spoke to the camera from a dark room. It had all the makings of a cheap B-grade Bollywood movie. This “expert” then claimed that 12 of his team were gunned down in Hyderabad so as to keep this hacking mode secret, and he went on to say that this hacking could be done by using a low frequency signal in the range of 7-390 Hz. Just to understand how absurd this claim is, we need to know that a signal in this range would need an antennae of several kilometres to process the wireless signal and get information (Sinha 2019). This is as absurd as the claims of some of our ministers – including the Prime Minister – of genetic engineering, and flying rockets and aircrafts in the age of the Mahabharata.

VVPAT Tallying

There has been a serious debate regarding verifiability of electronic voting, both from legal and technical considerations. Most of the legal challenges have hinged on the issue of verifiability under the law. While the laws may vary from country to country, the technical issue of computer security is common to all countries. Even though Indian EVMs are much more difficult to hack, no one can argue that they are completely hack proof. So the issue of verifiability that EVMs have not been hacked should be a consideration in Indian elections as well.

However, the way the VVPAT is being treated by the ECI is as if it is a legal burden they are carrying, and they are taking token measures to fulfil the letter of the law, and not its real content.

Why is verifiability important? Bruce Scehneier (2018), a well-known security expert states the problem quite well,

Elections serve two purposes. The first, and obvious, purpose is to accurately choose the winner. But the second is equally important: to convince the loser. To the extent that an election system is not transparently and auditably accurate, it fails in that second purpose.It is not enough that justice—in the elections—is done, it must be seen verifiably to be done. And this includes a paper audit capability as well.

The VVPAT was introduced in 2013 to essentially serve this purpose. Several political parties and civil society groups had demanded the ability to validate EVM results and also create a paper trail to record the voting preferences of voters so that in case of a dispute over the EVM or their tallies, the paper trail could be used in a court of law. In 2013, the Supreme Court ruling on a writ petition directed the ECI "to incorporate a system of paper trail/paper receipt in the Electronic Voting Machines (EVMs) as a convincing proof that the EVM has rightly registered the vote cast by a voter in favour of a particular candidate."

> We believe that the demand made by different political parties and other organisations to count a certain percentage of VVPATs in each assembly constituency is correct.

Currently, the ECI mandates the physical tallying of VVPAT paper slips with the EVM results of only one EVM per assembly constituency. We feel this is inadequate to detect EVM discrepancies or rigging, were they to actually happen. Nor does this suffice to show transparency and establish the credibility of the voting process. We believe that the demand made by different political parties and other organisations to count a certain percentage of VVPATs in each assembly constituency is correct. Demands have been made to count anywhere between 10% to 50% of VVPATs.

We feel that as an alternative, a statistical sampling principle could also be considered to come up with a percentage of EVMs that should be counted in each assembly constituency to ensure that the probability of detecting rigging is, say, more than 99%. However, such a method should be discussed and the final decision should be seen to be credible. It is not enough to submit an affidavit by, say, a professor in Indian Statistical Institute, to the Supreme Court and shelter behind an authority figure. As we have said, the issue of the VVPAT is as much about verification as of the credibility of the electoral process. So tallying of VVPATs should be such that the parties and the electorate are convinced of the integrity of the electoral process. The ECI has to understand the need for this, instead of standing on its prestige.

Additionally, close elections, for example, elections where the winning margin is less than 1% of the total votes polled, all VVPATs slips of that particular constituency should be physically tallied with the EVM counts.

> It is not our argument that Indian EVMs are hack proof. No machine built by anybody, however competent they are, can be made free from hacking by skilled hackers.

Adopting such steps will go a long way in alleviating the fears in people's minds about EVMs. Tallying of votes in a certain number of VVPAT is as much about the optics of a fair elections and the confidence of the people in its fairness.

Conclusions

It is not our argument that Indian EVMs are hack proof. No machine built by anybody, however competent they are, can be made free from hacking by skilled hackers. We have argued that it will require physical access to the machines – whether in the factory or outside – to carry out this hacking.

As we have described in detail while discussing the administrative procedures, the EVMs have to pass the various verification procedures that involve representatives of political parties. These checks require that political parties understand and have an informed participation in these processes. Apart from physically verifying the EVMs, there are also randomisation procedures that involve the presence and participation of political party representatives.

Therefore, hacking such a system can be done only with a massive conspiracy, and with either the wilful participation of the opposition parties in this conspiracy, or their complete ignorance of what is going on.

That is why we believe that to keep the elections and our EVMs free from hacking are not only the task of the ECI, but also of the political parties. This is where we need an informed opposition to play its due role in the process.

Finally, elections must not only be fair but also seen to be fair. Therefore, our argument is that the ECI must not use the VVPAT as just an ornament forced on it by the Supreme Court, and do a token verification. It should do a real verification by tallying the paper slips of the VVPATs with the electronic count in the EVM. Only then will the ECI be able to put to bed the suspicions people have of their votes being hijacked by a ghost in the machine.

References:

Schneier, Bruce (2018): “Securing Elections,” 20 April.

Hari K Prasad, J Alex Halderman, Rop Gonggrijp, Scott Wolchok, Eric Wustrow, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati (2010): "Security Analysis of India’s Electronic Voting Machines," 29 July.