A Mechanism to Corrupt Indian EVMs[1]

Sebastian Morris[2]

9th March 2024, Sanquelim, Goa

Keywords:

India, Democracy, Electoral Process, Electronic Voting, EVM, Paper Ballots, Corruption, Election Commission, Local Representation, Security, Choice of IT systems, Public Management, Governance, Autonomous bodies.

JEL Codes

H1, H4, H8, P1, P5, K4

Abstract

There is the possibility of a small rogue code (perhaps a mere 10 lines long) and almost undetectable being inserted by one/two persons in the know: through modifying the source code –less likely- or doctoring the compiler or processer/ ROM or through the program that controls the VVPAT (Voter Verifiable Paper Audit Trail[3]). Therefore, the presence of the rogue is likely to be in every machine and remain undetectable. The functionality of the rogue, is (possibly) that if electronic voting machines (EVMs) are queried after some (say 7) days, it gives biased results to favor a particular candidate. The favored candidate is identified by the machine (rogue) as the candidate who secures the majority say (7/10 in the first 10 votes cast or 4 out of the first 5). Otherwise, when queried before say 7 days it gives the unbiased (correct) results. Hence, all checks of the Election Commission would not be able to detect the rogue. Neither would tests prior to polling. ***All that the person in the know needs to do is urge his/her party workers to be the first to vote on every booth. Then that party gets a bias of say 5-10% in its favor.***

Current processes of the Election Commission of India (ECI) would not be able to stand in the way of the planting of such a rogue. The EVMs are not subject by the ECI with any large-scale delayed counting tests.

---

[1] NB: This paper makes no claim that EVMs have been fixed, or that there is an intent to fix the same by any political party, government, or others. It is made in the spirit of being critical, only to help the system to improve. I would like much sharper minds than mine to point out the fallacies in my argument. I would be most happy and glad to be proven wrong in the possibilities outlined above. Dated 24-03-2024, Sanquelim, Goa. (original date).

[2] Email: morrissebastian@gmail.com; morris@iima.ac.in; morris@gim.ac.in; Currently Senior Professor and Chair, Centre for Public Policy and Governance at the Goa Institute of Management. Former Professor at the Indian Institute of Management Ahmedabad. The analysis and views expressed herein are entirely mine, and mine alone.

[3] Gopinathan (2021) pointed out this possibility. For the same to have large scale effect, the corruption would have to build on the "symbol" of the one of the major parties, since only that is common across constituencies. The VVPAT would also need to be able to pass on the information through its connection with the EVM and the EVM would then be "subsidiary" to the VVPAT. If field level tests are done, the VVPAT corruption can be easily caught. The method proposed here where M3 EVMs can use the clock to give the corrupted results when queried many days later but not otherwise, means that the corruption can pass through undetected by the ECIs procedures and tests.

Paper trails being counted only on a sample basis would not be able to reveal the rogue. EVM design, manufacture, procurement of components are not parallelized, nor are they duplicated and distanced from the government of the day in truly autonomous bodies. Their production by public sector entities, which have scant autonomy from the government, introduces a conflict of interest as well. Since elections are around the corner, the paper trails of the VVPATs should constitute the vote.

SYNOPSIS

Most publicly discussed methods to corrupt Indian electronic voting machines (EVMs) are not tenable because these require many (officials) to act in cahoots. This does not mean that the system is not corruptible. It is actually possible to exploit the input to an electronic system to change its operating logic in unexpected ways. For instance, a malicious 'internal' actor could plant a rogue code within an electronic voting machine that identifies a favored candidate by analyzing patterns in the votes cast. For example, the party that knows such corruption has taken place could encourage its voters to be the earliest voters. Then the candidate who receives the dominant share (say 70%) of the first 5, 10 or 15 votes cast could be identified as the favored candidate by the rogue. The rogue code could then shift votes in favor of that candidate by a predetermined (or dynamically derived) bias, taking votes away from other top candidates on that machine. Because all tests and procedures set up by the Election Commission of India (ECI) go only up to 1500 votes (typically much less), the rogue code could also desist from shifting votes on machines where the total votes cast is less than the maximum threshold for testing -1500.

Furthermore, since the bulk of the machines in use today (M3 EVMs[4]) have a date clock, the rogue code could hide itself by only shifting votes after a sufficient amount of time has elapsed from the cast of the last vote to the count date and time, which could be around a week or more. In this case, the rogue code need be very small and simple, and could even shift votes on machines where the total votes cast is less than the check level of 1500 votes. M3 machines are typically used with much smaller numbers of total votes cast. Since M3 machines dominate the corruption via use of the date is more likely.

Since the ECI's check processes do not use test numbers beyond 1500 and there is no date--delayed count test, the existence of such a rogue code cannot be ruled out. Thus, all ECI's mock tests, and tests conducted by the electoral officers on site, security measures like sealing the machine with high security printed tape etc., are useless against such a rogue. The rogue code could be built into the compiled code. The corruption of the machine could take place at any of the several stages: in the source code (very unlikely), in the compilation – through the corruption of the compiler, through corruption or implant of other codes/circuits in the controller itself, through switching of the source code, etc.

Since the paper trails are counted only on a very small basis, they are of no value either. Moreover, in the past "small" discrepancies which are estimated to be below the winner's margin are ignored, even on the very small 1-2% of the machines where the paper trails are counted. The sampling for "First Level Checking"[5] and the protocols for testing in the field are based on the assumption of random failures; and hacking by persons external to the process. They are not designed for uncovering a purposeful internal or external (vendor) corruption of EVMs, which is what we have posited even if hypothetically. As such the rogue could have been planted in a very large number of machines, and one cannot rule out the possibility of all machines manufactured beyond a certain date being corrupted.

[4] ECI (2012).
[5] ECI (2020).

The Election Commissioners have therefore had no direct way of ensuring the reliability of the machines. They have to take on faith the veracity and robustness of the processes that have been set up by the manufacturers, advisors and vendors to the manufacturers. They are dependent on processes over which they have little control. Hence the outcome tests are all useless, against the kind of possible corruption that we have contented in this note. This would then amount to a violation of the ECs sacrosanct mandate to ensure the utmost reliability of the voting process.

The topmost priority of the ECI should be to do actual field tests in which machines are fed different sequences of voting patterns especially at the beginning, and at the end, and then check after waiting for a week or more, in keeping with the delays in counting that the ECI envisages.

At a more fundamental level, elementary reasoning, even if the probability of corruption is very low, since the consequences due to the possibilities of "wholesale corruption" are terrifying to a society committed to democracy, then such processes are not to be used. The impacts on society are also irreversible even if known many years later. Furthermore, there are strong path dependencies in the sequence of regimes. Hence, it becomes imperative to move back to paper voting, with now excellent checks possible due to CCTVs, human presence, and traceability. *Above all it is important to accept the near zero probability of "wholesale corruption" of the mandate which paper ballots provide; and reject EVMs since they have a non-negligible probability of "wholesale corruption".* Of course, even paper ballots can be corrupted through use of force/ gendarmes etc., but then we are talking of "banana republics" where in the first place there was no intent to be democratic -only to indulge in "mimicry". Even then, that the mandate has been violated would be known.

EVMs in contrast can result in "wholesale corruption" with the electorate not being able to know that corruption has taken place. Entirely different outcomes (from what should have been the true outcome – which can never be known ex-post) can be rationalized in umpteen ways and even if they differ significantly from exit polls or other well researched expectations.

In this paper we have demonstrated how "wholesale corruption" is possible, with the connivance of a mere one or two individuals in the system. This is a very dangerous risk for the ECI to take.

THE SITUATION

Indian EVMs[6] have been, among the "best" most thought through, and undoubtedly an achievement for Indian designers, and IT experts. The fact that the EVMs are superior to the early local machines that were in use in many countries does not in any way mean that are therefore not corruptible. Only that it is more difficult, reliable or robust. The "incorruptibility" of the EVMs is based on the their simplicity, as claimed by the ECI and the engineers who designed the mechanism. Even the simplest non-reprogrammable mechanism can be corrupted, though the pathways are fewer than in the case of programmable complex processors or machines.

With the second and third generation of EVMs (M3 Machines) the complexity has gone up so that the original defense based on simplicity can no longer be justified. While still free of network connectivity and wireless capability, the use of a clock provides a pathway for corruption of readouts.

[6] Cf. various FAQs on EVMs and VVPATS; ECI (2021); ECI (2008); ECI (undated); ECI (undated a); GOI (2017).

Similarly, the use of the Voter Verifiable Paper Audit Trail (VVPAT) necessarily has to have the serial number, name and symbol of the candidate[7], which when connected to the "simple" EVM renders the system corruptible through multiple pathways. The VVPAT can easily have a rogue to pass on the identity of the favored candidate perhaps through the symbol code to the EVM. The VVPAT itself is a complex machine with two parts – the printer and a display unit. It is ironic that the VVPAT was itself developed to check possible errors with the EVM and most importantly to meet the constitutional requirement that the vote of a citizen has to be convincingly demonstrated to the voter to have been his/her.[8] So the defense that the EVM cannot know the favored candidate is no longer valid in the era of VVPAT. For corruption via the VVPAT to be undetectable, the EVM itself has to be corrupted in its operations by the VVPAT and here the fact that the EVM has read-only memories could make that process less tenable than the process proposed here – essentially that the corruption has to be during manufacturing, in the design, or in the procured devices, certainly before uploading the operating program of the EVM.

Many other mechanisms for corruption have been proposed[9], but these are less tenable, and some would even be detectable by the tests laid out by the ECI. The mechanism that we have proposed does not require the VVPAT to be doctored; only that the EVM itself has a rogue. It is also minimalist, very simple, and not more than one or two persons need to act in cahoots.

THE HYPOTHESISED MECHANISM

The proposed method to corrupt the voting machine requires the involvement of only one or two persons who is/are involved in any of the stages of the actual code development, its compilation, or even at the level of the manufacture of the processor /ROM. Neither the Expert Committee of the ECI nor the ECI carries out hash tests on every machine. Even if they did and the hash tests were successful, corruption cannot be ruled out. A hash test only means that the original source code has not been tampered with, or that the compiled codes of two different machines are the same. This would require a reference compilation or a reference source code, that is true in both the code and the compilation. Clearly, if the original reference source code has itself tampered, or replaced or the reference compilation is untrue, the hash test would only reveal that the tampered code/tampered compilation is being faithfully reproduced. Even with true code and true compilation, it is still possible to have a rogue that is in a part of the hardware, and modifies the functionality of the program.

Below we outline a method of how a small sized rogue can be exploited to bias the voting as revealed by the EVM on counting day.

1. Let us say an individual with high clout and ability to corrupt, ensures that a rogue code is implanted. The obliging person could be the one who is in charge of populating all the micro-controller chips (the microprocessor of the EVM) with the compiled code, or the person compiling, or the person developing the compiler. It could even be by way of

[7] Cf. https://ceomanipur.nic.in/documents/FAQs%20on%20VVPAT.pdf (Frequent Asked Questions (FAQs) on Voter Verifiable Paper Audit Trail (VVPAT); Chief Election Officer, Manipur.

[8] On this issue, that it is the paper prints of the VVPAT print machine which are authentic in a constitutional sense has been made by many. But there has been no review or public scrutiny of the working of the VVPAT or of its communication link with the EVM. See also Gopinathan (2021) op. cit.

[9] Such as after voting manipulation by staff, last hour voting by staff in favor of particular parties. But these are not easy to take place, with a very active press, and monitoring by political parties, and the well laid out processes for the conduct of elections. There are many claims of voter registration /updating processes either cancelling out many existing voters or not registering certain groups of voters whose voting patterns are believed to not favor the incumbent government. But these are another matter that point to the need for autonomy and efficiency on the part of the ECI.

rogue instruction set on the processor itself that is activated by the startup procedure. **The rogue modifies the working characteristics of the operational program in a way that is not detectable by (all) the checks done by the Election Commission**. As such the integrity of only one /two person/s needs to be compromised to ruin the entire voting mechanism.

2. Imagine that the rogue code has the following functionality:

   a. It is a very small part of the source code / operating code, that is loaded after compilation on to the ROM /Processor/Controller and the entire code is executed by the Processor-Controller when the machine is on.

   b. It (the modified program) is present and is active on all voting machines that are made from a certain date.

   c. The rogue counts the votes cast over say the first "n" (such as a small number between 5 and 15[10]) votes whether during tests or in actual voting. All that this requires is an additional 4 or 5 registers to be part of the rogue code.

   d. If the majority (say 70%) of votes over the first "n" is in favor of say Candidate 1 then the rogue knows that Candidate 1 is the favored candidate. Thereby the pattern of the voting in the first "n" votes allows the rogue to identify the favored candidate's number (position) in the list. This is despite the fact that the EVMs and the ECs processes are such that the EVM does not store the identity of the candidates. **As such the ECs procedure of candidate order being determined from among the main parties' candidates by alphabetical order of names, i.e., randomly, cannot prevent identification.**

   e. The program as intended for its normal working also maintains a record of the cumulative votes polled for all candidates including the top 4.

   f. When checked through the usual procedures the corrupted code gives the correct record. However, it has one useful information: It now knows the identifying number of the favored candidate. Therefore, the procedures laid out by the election commission (viz. check for match with manual record of 500/1000 /1500 votes cast) will not show the error; And the claim that the EVM cannot identify candidates fails.

   g. Say there is a threshold number "m" in the rogue (which is larger than that recommended in testing) which is also part of the rogue. After the total count of "m" votes being cast any count of the machine will reveal the following counts. Assume that actual votes cast for the favored Candidate is F, for the other 3 top candidates it is N1, N2, and N3. "m" could be a number higher than 500/1000/1500[11]. Then the corrupted results (FC, C1, C2, C3) as revealed could be:

      I. FC = F*1.2 where 0.20 is the bias

      II. C1 = N1*(1-0.2*F*N1/(N1+N2+N3))

[10] Why has this number to be small but not very small? The matter will become clear as we recognise how the party in the know can exploit the anomaly.

[11] As per the latest check procedures, if the number is greater than 1500 there is no way the check processes could catch the rogue code. Even if in a few cases where a diligent officers tests with more than 1500, since he would have randomly given the test votes, and not in the specific way of giving at least 70% of the first say 15 votes to one candidate, it is highly unlikely even in this case that the rogue would be revealed. Even if in a rare instance of such extended testing, a mismatch is noticed, the diagnoses would naturally be that, that particular machine is faulty (not that there is possibility of all machines having been corrupted), given the expected way the officers and engineers are bound to think. Cf. ECI (2020).

III. C2 = N2*(1-0.2*F*N2/(N1+N2+N3))

IV. C3 = N3*(1-0.2*F*N3/(N1+N2+N3))

V. Count for all other candidates is what has been actually cast. (It could be different but then there is a risk of dramatic change from expectations in the case of candidates polling very few votes).

h. These corrupted figures along with /instead of the right numbers are stored back in the additional count registers after the threshold number of votes (m) has been cast. OR, it may also be computed (at the time the machine is queried for results) as in (g) above and displayed only when the officer queries the machine for counting. And this is what the EVM will reveal on counting day when queried. The total votes cast will always be revealed correctly. Additionally, there could be sub routines that define the above and take care to shift only from candidates who have polled large number of votes; or to avoid shifting when most, say 90% of the votes are all in favor of a single candidate. [This would insulate the machine from revealing the working of the rouge in a polling station when everybody knows that nearly all votes in that station have been cast for a particular candidate]. On the day of counting the EVM which knows N1, N2, N3 and T (the total votes cast) and also knows the identity of the favored candidate would give the numbers FC, C1, C2, C3 and etc. and T, rather than correct F, N1, N2, and N3 etc.; and T (which is correctly reported) (See point 4 below).

i. A 0.20 (20%) bias is enough to win most elections for parties with actual voting of 35-40% in two cornered contests and much less in three cornered contests. Indeed, the bias can be more intelligently placed at 0.10, or even 0.05 to have substantial impact, given the strategic voting that has become the practice among the masses. It could also be determined dynamically based on the true voting to corrupt the same in a Bayesian consistent way, though such "niceties" could make the rogue somewhat larger. This complication in corruption is not necessary since the modus operandi of the rogue guarantees that it remains hidden.

j. In the context of representational democracy which is "first past the post", small swings in voting are what change governments and very rightly so.[12] And contests in India for a variety of reasons tend to become multi-cornered. As such even a much smaller bias could effectively corrupt the entire results.

k. The rogue code is small enough to be of no more than a few score lines of code.

l. While I have said first " n" could be 10/15, it could even be larger or smaller, but not much larger. It could easily be smaller.

m. An imprinting that builds on the voting pattern between say the 50th and 56th vote cast while possible would make it very difficult to exploit through the normal operation of the booths. See Point (3) below. *Hence we are confident that the corruption if any is likely to use the patterns in the first set of votes cast.*

3. Recall that the rogue is guaranteed to be able to identify the favored candidate, as long as the first, say 7 out of 10, or 4 out of 5 votes are cast in favor of the (favored) candidate. The rogue could also be so constructed as to assume that the candidate receiving the first vote is the favored candidate. This is possible though less likely. Let us imagine there is a party where the cadres are willing to go and cast their votes first thing on voting day. An innocuous call to that effect

[12] Popper, Karl (1997), "On the Theory of Democracy", Chapter 8 pp. 81-98, in Popper, Karl (1997).

can be given, by party functionaries /party leader, and nobody would suspect, since it is the right of candidates and parties to urge people to vote. In this case the crucial aspect of the first (early) voting can be mystified as being "auspicious", a ritual that evokes fate or heaven in one's favor as additional reason for such urging. Similarly, the first vote cast need not arouse suspicion[13]. [Conceivably, the last one / two votes cast can be used to identify the favored candidate, but it is tricky to ask party workers to ensure that the last one/ two votes are theirs. They would wonder why and the matter is likely to spawn speculation, and unlikely to remain concealed for long].

4. Since most EVMs now in use have a clock[14], the rogue need not limit itself to being effective only in machines where the total votes cast is more than the check number (500 /1000/ 1500). With a clock the pathway of corrupting the report based on when the machine is queried opens up. Thus if queried say "d" (say 3/5) days after voting, it reveals the biased results, but not when queried before "d" days. As such none of the field tests, nor the FLCs after manufacturing could reveal the presence of such a rouge.

5. Thus, the claim of the EC that the alphabetical order of the names of the major candidates is used and nothing else (candidates have a number and identity that is not known to the EVM) is true. **But that does not mean that that the machine with a small rogue cannot identify the favored candidate through information embedded in the voting pattern. This is a classic case of operational information being used to change procedure/ parameters of a system.**[15] And the method for corruption outlined here does exactly that. The ECI and the entire system is quite unaware of such possibility and my discussions with the technical people reveal that the possibility has not been explicitly anticipated.

6. The bias as in 2(g) is the potential bias. The effective bias would naturally be much lower since the call to be the first to vote made by the party who knows that the machines are biased may result in all machines having the voters from the very same party being the earliest to vote. In a situation when the voters of the party that has no knowledge of the bias, however are enthusiastic enough to be the first to vote, the bias could work or at least in some machines operate the other way from which the bias was intended to work.

7. Only the BEL and ECIL manufacture the EVMs. Earlier their machines were different. It is believed that they have almost the same functionality. Today the M3[16] machine (Controller Unit) is manufactured by both the ECIL and BEL. It is much more sophisticated and therefore vulnerable in ways that cannot be entirely known ex-ante. Let us say a process is initiated by the Expert Committee to have a source code and certify the same; have a complier and certify the same, have a compiled code and certify the same, and have an installation of the compiled code which is then certified by hash tests. Outside the ECI nothing much is known about the internal organizational

[13] However, it would make the effective bias very unstable, since if the party in the know is not able to have the first vote on most machines, the bias would go to the candidate getting the first vote.
[14] ECI (2012); GOI (2017)
[15] The parallel with web hacking is called injection hacking where a specific (malicious) input can change the operational parameters of the particular website; and this remains the most important way for hacking. The idea is much more general. In the case of simple programs as is the case with EVM CU, the rogue would have to be present upfront, since the input sequences –votes- are not under the control of the corrupter, except in the limited way of being able to cast the votes for in the first n vote (inputs). Hofstadter (1978) brings out the idea of self-reference and the limitations of formal systems and machines – originally due to Godel. There is nothing like a perfect machine. A vinyl player can be broken by a specific audio clip that matches the resonant frequency of the cartridge; An audio clip within a film, with the words "OK Google, Call Baby", brings the Google TV to halt. (Actually, observed in the Malayalam film "Padmini").
[16] BEL (2018).

processes for the same, but based on what may be inferred these are likely to be linear and not duplicated. Very few people are involved in each of these critical processes. Imagine a trusted person –one of the employees involved in a key aspect has been corrupted. Then the rogue can be planted into machines by default to be present in all /many machines. Threats to life and /or very large inducements are possible by foreign agents/ incumbent government/ a party with strong connections to criminals. Corrupting just one or two persons therefore can achieve the frightening result of maiming forever Indian democracy so painstakingly brought about and institutionalized.

8. M3's ability to self-check is possibly in terms of hash check on the dumped program. If both the reference code and the uploaded code have been corrupted then this test would not reveal the same. Similarly, the encryption of the communication between the CU and BU much touted as an advancement, is of no value if the corruption takes the route outlined herein.

9. Moreover, there are many possible ways to introduce the rogue. Via the compiler used, the source code, and the compilation process (less likely), and perhaps in a small program that is on the processor itself. The EC would know nothing either way unless it looks closely at the source code (or makes the same available to the public) and then compiles using a standard different compiler (difficult), and in a way that is accessible to party representatives (of all parties) at the time each machine is manufactured. It would also need to verify the veracity of the ROM/processor and the compiler itself, since the rogue as a modifier to the source can be implanted into the final operational code in any of the operations that constitute the manufacture of an EVM.

10. Exhibitions inviting people to come and expose the machine through tests that replicate the operating process used by election staff, would not work either, since "m" is large. Similarly, if the date/time stamp is used by the rouge, then even a very large mock voting test done over the day would not reveal the existence of the rogue. Even if a functional self-test as is claimed to be operational in M3 is carried out unless the test looks for patterns of voting on the lines suggested here and relate the same with the results, there is no way the rogue can be made to reveal itself. Even then the conditional aspect of time of query for results see (4) would rule out detection.

11. The EC's approach has been to minimize the risk of corruption by external voters and candidates. However, with use of EVMs the risk of centralized / single point / total corruption /internal corruption is what looms large. ECIs current processes make the EVMs open to internal corruption. This possibility of wholesale corruption is entirely ignored by the ECI.

12. All arguments of EVMs through electromagnetic waves (Wi-Fi, radio or microwaves), their improper storage, selected EVMs being sent to particular booths, etc., have been made many times. These are not to be confused with the method of corrupting EVMs proposed herein. These other methods are unlikely, as they are not centralized, and require many persons to act in cahoots, chances of which are remote. And such corruption would be revealed, since many people would then have to be involved, and some people would talk. Similarly, the guarding of EVMs, use of strong rooms, use of security paper seals randomization of EVM distribution will in no way prevent the use of these centrally corrupted machines. Small deviations from the laid-out process by the ECI in actual operations, have drawn much of the attention of the media. This has taken the attention away from the possibility of wholesale corruption is significant.

13. However, arguments made in the media and in courts to open the process of manufacture and programming of EVMs to the public for all varieties of testing are valid.

14. The Election Commission, in the main, has used a "confirmatory" approach, which is not entirely scientific, since robust machines (or hypotheses) can be "accepted"[17] only if test/ experiments are done with the intention to break/falsify. This requirement of falsifiability is what has demarcated science from all other human endeavors.[18] And such attempts to break / falsify need to be initiated, encouraged and facilitated. The EC has been averse to such tests, and to open invitations to corrupt (i.e. to carry out ethical hacking).[19]

15. Moreover, the approach of the EC has been guided by the assumption that corrupters would be external to the process and never internal. This leaves a door open for large scale or complete corruption. For corruption to take place, only one link in a chain of processes need fail, as the method proposed here would indicate. This is a process issue and security issue, and not merely a technical issue, where the paramount driver of the process of development and manufacture should have been to guard against internal corruption, which is not the case. Significant parallelization of all processes by multiple teams, including the use of multiple microprocessors, ROMs, and electronic components is absent[20].

16. The role of the Technical Expert Committee (TEC) is largely in the nature of consultation, advisory, oversight of technical improvements, response on queries raised by the ECI including on issues raised on tamperability. It has no role in OPERATIONs or in the PRODUCTION OF EVMS. As such the undoubtedly high integrity and capability and knowledge of the members of the TEC is of little consequence. The EVMs' veracity depends critically on the robustness and incorruptibility of processes within BEL and ECIL[21].

17. Also, if the rogue is generated during the design and development phase, or is embedded in the compiler, or the EVM's control unit itself, i.e. before the mass manufacture and upload, the corruption of only one individual has to take place only once. Indeed, then subsequent checks and tests are of no avail. So, the entire process, even in the past is called into question.

18. The Technical Expert Committee's public statements of Indian voting machines being superior to German and American, constructs a straw man to argue against. Similarly, the contention of the technical experts including some members of the Technical Expert Committee that jealousies due to the Indian capability to develop superior machines having driven the opposition to EVMs on the part of many in the public is unfair, since it has no bearing on the issue of corruption of Indian EVMs which undoubtedly are the best, but still not without pathways for corruption.

19. Similarly, the endorsements by the courts of the technical soundness, the veracity of the sampling for statistical tests are of little value since the courts are not fundamentally

[17] More correctly not as yet rejected.
[18] Popper, Karl (1963).
[19] The ECI, as "an extra-ordinary measure, threw an open challenge to all stakeholders between 3rd April and 7th August, 2009 to come forward to prove if the ECI-EVMs could be tampered. However, none could do so". P.9 of Election Commission (2021). To make the challenge meaningful the EVM as such must be made available to all to study, examine and test, including testing that could be destructive. The challenge held on 20th May 2017 attracted very little attention, p.10 ibid. In none of these has the prospect of a simple (few) line of rogue code through internal corruption been raised or discussed.
[20] Extended ledgers using block chains are far more robust than conventional records maintained by one organization.
[21] Page 16, EC (2021) ibid.

equipped to rule on this matter. On matters like security of the strong room its notings are important though[22].

The matter of corruption in the manner proposed above being very simple and requiring a mere 1 or 2 individuals to act in cahoots to result in a corruption that can bypass all the tests of the EC, is a matter of utmost concern.

ECI cannot shy away from this issue. The samples to do statistical tests of match between VVPAT and EVM results are presumed on the understanding that random failures of equipment are all that are possible Hence the very low sampling of 2-5%. Random unintended technical failure is hardly the issue when the manufacturing processes today can be very sound and highly reliable. The tests should have been to detect internal corruption via purposeful means such as those suggested herein. Admittedly these are going to be difficult.[23]

COROLLORIES

1. In case the clock is not used by the rogue, or older machines without a clock are involved, the corruption would be more effective in elections when the voter base per constituency is large i.e. in Lok Sabha elections over Assembly elections; and would be least effective for local body elections.
2. In states with smaller numbers per constituency, the rogue would be less effective, since votes cast per machine is likely to less than 1000.
3. In case the date readout on the clock as in the M3 machine is used by the rogue, the bias could carry through to be effective even in elections with small numbers per voting machine.
4. The likelihood of the corruption having effect so as to change the result in constituencies that are closely contested is higher.
5. Nearly all the processes laid out by the EC (sealing using security press tape, "FLCs", checking for functionality) would not reveal corruption of the EVMs of the type proposed herein.
6. The evidence that the EVMs have been fixed would not be revealed to the EC, the political parties, or in any election. It would only be known to the one person who has ensured the planting of the rogue.
7. If the corruption has taken place, then nearly all machines are likely to have been corrupted (i.e. have the rogue code).
8. The effective bias (2(g) from first list above) is likely to vary from election to election depending upon the calls for early voting being followed by the party voters of the party that knows that the EVMs have been corrupted. Thus, in some states where the cadres of party A are first to vote it could help that party even though the corruption may have been carried out by a person sympathetic to party B!
9. (8) would mean that the defense of the EVM based on the fact that parties in opposition to the centre, have recently won elections at the state, is no "proof" of non-corruption, nor of a bias. In state level elections, EVMs corrupted in line with the method suggested

[22] For a list of court rulings on the matter see p.12 EC (2021) ibid.
[23] It is unfortunate that an earlier version of this paper sent as an open letter to the members of the ECI, did not evoke any response. (August 20, 2023 from morris@iima.ac.in, by email).

in this paper, could also act in favour of "opposition" parties if their cadres are enthusiastic to be the first to vote.

POSSIBLE REMEDIES

1. The first task would be to actually test a large and random sample of EVMs from the field in large scale mock tests where people are invited to participate, the machines kept for many days/ even a couple of weeks after the mock polling closure, before the results are read out. (As is the practice of the EC in actual Lok Sabha elections). And the root cause of every failure has to be examined. The examination would have to be by teams which are different from those who have designed, prototyped, manufactured and tested the machines before. The machines being far simpler than current PCs, should have almost no instance of failure, even in a lot of 10,000 machines. Even one failure in a lakh machines would have to be considered as a serious matter. The test would have to include a delayed test where the mock results are read out after 3, 6, 10, and 15 days. The mock tests would have to allow for specific sequence of inputs including majority of first 5, 10, 15 votes going to a specific candidate.
2. Next would be to put the entire process from source code development, to upload on machine, to critical examination. And to put in place multiply parallel processes around different teams, with due safeguards.
3. **However, such a process would take time, since many elections are already scheduled. The only immediate measure would be to have 100% use of VVPATs and the election results to be confirmed only after the VVPAT slips have been counted, and the results are declared as being tentative on counting day; and finalized only after all the paper slips have been counted. A discrepancy of no more than 2% of the margin of victory as recorded by paper voting VVPAT or 10 whichever is less ought to be allowed for the EVM. Every case of discrepancy between the VVPAT and EVM (even by 1 vote) should invite thorough re-tracking of the process to establish the reasons for the difference between the two should be carried out. The count of the paper votes would have to be the basis for declaration of results. Statistical approaches are nearly out of question since corruption is different from the random errors that machines are likely to have.**
4. **The EC should set up a committee of all parties and a multiskilled team to seriously examine the dangers of low probability of very large (consequential) errors. This group should have access to be able to "ethically hack" and to point out possible loop holes in the process. In other words, it should engender and empower efforts to falsify the process[24], the technology and the manufacture under its own aegis. The hackers would have to worry not only of the technology, but of the processes involved.**
5. **Indeed, the EC has to be in charge of the entire process and also be the entity that contracts with vendors. The EC (with its Advisory Committee) should deal directly with the political parties and make available opportunities for hash tests, and destructive testing, besides testing in any manner that they desire. Furthermore, they must ensure access to the source code, to the compiler and to EVMs on a sample basis for their own testing. All personnel involved in the process of manufacture, system design, source code development, compilation,**

[24] Science is what it is because as a process it subjects itself to falsifiability. Popper, Karl (1963).

procurement of compiler and ROM should be available for questioning by a committee of experts whose job is to break the EVM.

6. **The assumption made by the technically- expert votaries of the EVM, that Public Sector Companies are beyond errors, or that they do not have a motivation to corrupt, is not tenable since we are not talking of a company but only of individuals who can be corrupted. Moreover, PSUs in India lack autonomy and their CEOs are highly amenable to government /dominant party influence. Having little autonomy, and the fact that ex-ante, governments can involve themselves in operational matters of PSUs / SOEs, creates a conflict of interest here. Thus, the government in allowing political appointees to the boards of many PSUs including BEL and ECIL has, on that count alone, created the need for the EC to examine the operational veracity of EVM design, development, procurement, manufacture etc. of these companies, and their supply chains. This is relevant to our discussion since we are laying forth an easy and credible method to (internally) corrupt EVMs.[25]**

7. Allow private citizens /parties NGOs to develop in parallel, vote casting machines (that use the compiled code) that can be used for testing with the intention to break/ falsify the veracity of the EVMs. Some 1% of the EVMs randomly chosen out of every lot, must be made available for hacking, and falsifiability tests both internally and by the special committee. Any critical process is safe only if they are in parallel. [Hence multiple keys to safes in banks].

8. Make available publicly the source code, and the compilation, as well as the processor and ROM design details to all, so that the public as a whole can verify and actively engage in the task of "falsification**". Trust or secrecy as the basis for veracity is entirely mistaken in the context of the conduct of elections[26]**. Robustness would demand parallelization of critical processes.

9. Use of paper and ballot boxes**. This is the only final solution to voting. E-Voting and all e-approaches have the problem of nonzero probability of wholesale corruption**. Condemning those recommending use of paper ballots as "Luddites" is entirely unfair. Every technological solution found would also invite an ability to corrupt. In normal electronic transactions (e.g. financial transactions) parallel records are generated for the debtor/creditor, or payer/payee, government/citizen, so that errors are noticeable by people to lead to a continuous process of self-correction.

   In financial transactions there is a strong motivation for ensuring correctness. And there are multiple records, receipts, and such like materials that are generated. Most importantly repeated transactions would expose bugs. (In voting the system cannot be proven in repeated operations). Moreover, the errors being financial can be corrected retrospectively. With extended ledger approaches financial transactions become more secure. In the voting by EVMs as it stands today there is no parallel independent record since there is no concept that is analogous to the payer and the payee noted in financial transactions. Hence no retrospective correction/ compensation is possible.

   I would reiterate again the problem with electronic voting is that, however carefully the machines are designed and however well managed the processes is there is always the

[25] The process within the PSUs as described by in EC (2021) is sketchy (p.17) and does not give the assurance that the process of "burning" the compiled code or the compilation, or the microprocessor manufacture /design itself cannot be tampered by a sufficiently powerful / resource rich entity.

[26] It is however a valid approach in the case of protecting property by corporates and others. Models from the world of protecting property have been carried over to the EVM manufacture, which are very risky.

small probability of an event of humongous import, which is not easily detected since the design would integrally include concealment, and even if detected later, cannot be corrected, since history cannot be changed. In other words, in terms of system theory, electronic voting is entirely dependent on the system and hence on the key steps in the process and in security of the machines from both internal and external corruption which can be reduced but never eliminated.

While a society can and should take the risks of new technology generally, if the risks are of the kind that voting involves, then they should not be taken. Accuracy and robustness should not be confused to be the same.

a. Paper voting on the other hand has larger (still small) probability of a number of independent random or purposeful errors (which with basic checks and balances their scope can be greatly reduced) and which would also not be correlated. And when detected can be corrected without the outcome being dramatically affected. However electronic voting when corrupted can change outcomes radically i.e. can change history.

b. The main stated problem with paper ballot is large time -about a day –for counting. Ballot papers are claimed to be corruptible to "chain" voting. This is hardly a problem if the staff at the booths are vigilant. Similarly buying votes large resources are required, and presumes that the ECI and the police are ineffective as organizations. Moreover, such corruptions are easily detected so that EC can cancel the elections in the particular constituency. In other words, this is a low probability low impact error that can be detected, even if subsequently. It can always be corrected, with no great effect at the national/ state levels. In the era of mobile phones, with the representatives of the major parties being present in all booths, it would be difficult for the ECI' staff (on deputation from government) to favor any candidate.

c. Paper voting has the advantage that the system cannot be "systematically fixed". Fixing /cheating would involve many people and the evidence would be there. It is not accurate in the extreme. However **extreme accuracy with a vulnerability of "systematic fixing" is entirely undesirable, hence the ballot paper approach remains the best.** It is for this reason, and for the additional reason that paper voting and counting involves little "mystery" that many countries do not use electronic voting.

10. The ballot paper approach can be greatly improved to leave copies for the individual[27]. That the vote of the individual can be revealed in case of doubt, in no way implies that the vote is known to the balloting or counting staff! The two aspects have been mixed up by the votaries of EVMs.

    a. The practice of avoiding booth level counting on the ground that candidates can find which locations voted against or for them is, on closer examination, is a red herring. Only "person anonymity" is required in voting, not sub-constituency level anonymity. Thus, in voting for MLAs, MPs would anyway know at the sub-constituency level the preferences, and in a party centered world that is

[27] The argument that this would allow inducers to effectively buy votes is tenable, and could be avoided till such time as the ECI is able to check on small moneys being used to buy votes. Today the lack of a voting receipt allows voters to vote for the candidates of their choice, even after taking money from another.

India, at the ward and village level given that regular elections at lower levels have to be conducted under the 74th/73rd Amendment.

b. The notion that knowing which locations voted against a candidate can be used as information to bias public policies towards those who voted in favor and against those who voted against, violate the very idea of representation. If such bias can be expressed then the problems are elsewhere in the structure and design of governance, and attempting to "overcome" them through the design of voting or counting, by harming the voting process (since traceability would then be difficult if not impossible) is a case of one perversity being allowed to create another.

11. The arguments of speed of counting, and the" need for anonymity of voters in groups, "apparent" cost and convenience, are specious. Traceability, 100% reliability even at some small cost in terms of the accuracy, the need for de-mystification, and people's acceptance, are additional arguments that have been made time and again by votaries of paper ballots. We concur with these.

12. **However, the main point here is to bring to the notice of the ECI, and the people of India, the possibly of corruption of EVMs, which can be "wholesale" with none of the current checks and tests being able to uncover the corruption.**

References

The Representation of the Peoples' Act 1951. (https://www.parlament.cat/document/intrade/181101)

Gopinathan, Kannan (2021), "Vulnerabilities in the EVM-VVPAT Process", *The Hindu,* April 13, (https://www.theindiaforum.in/article/vulnerabilities-evm-vvpat-process-and-potential-threat-integrity-elections)

FAQs on VVPAT, ECI of several states and union territories.

FAQs on EVM, ECI of several states and union territories.

ECI (2010), "Protocol on First Level Checking (FLC) of EVMs. 4th August K.N. Bhar (Sec.), No. 51/8/16/4/2010-EMS.

ECI (2021) "Status Paper on Electronic Voting Machine (EVM)", Edition 4, Nov. (https://ceo.karnataka.gov.in/uploads/media_to_upload1637061008.pdf)

ECI (?) Presentation on EVM, Sept 2021, (ECI?)

ECI (2008) Manual on EVMs and VVPATS, July. (Download from https://old.eci.gov.in/files/file/15217-manual-on-electronic-voting-machine-and-vvpat-edition-8-august-2023/)

ECI (undated a) "A State of the Art, User Friendly and Tamper Proof EVM". Powe Point Presentation. (https://ceojk.nic.in/evm/EVM.ppt)

ECI (undated) "Status Paper on Electronic Voting Machine (EVM)". (Download from https://old.eci.gov.in/files/file/8756-status-paper-on-evm-edition-4/)

ECI (2012), Note from secretary Mr. K.N. Bhar, "Replacement of original real time clock battery during first level checking of the EVM –regarding", No 51/8/16/4/2011-EMS

GOI (2017), "FAQs on Security Features of the ECI_EVMs", Press Information Bureau, ECI, Govt of India., 9th April. (https://pib.gov.in/newsite/printrelease.aspx?relid=160754)

BEL (2018), "Electronic Voting Machine (EVM) M3 User Manual", Bharat Electronics Ltd, under the authority of the ECI. (Download from https://old.eci.gov.in/files/file/8991-electronic-voting-machine-evm-m3-electronic-voting-machine-evm-m3-user-manual/)

Douglas, Hofstadter, R. (1979) *Godel, Escher Bach – An Eternal Golden Braid (A metaphorical fugue on minds and machines in the spirit of Lewis Carroll,* Basic Books.

Popper, Karl (1963*) Conjectures and Refutations: The Growth of Scientific Knowledge*, Routledge and Kegan Paul, UK.

Popper, Karl (1997), *All Life is Problem Solving*, Routledge, London 1997.

Appendix 1: Text of Letter to the ECI

To

Mr. Rajiv Kumar,

Hon. Chief Election Commissioner

Dear Sir,

I would like to draw your attention to the attached note regarding the EVMs currently in use in India. Despite their many strengths, these machines could potentially be corrupted in a way that would avoid detection, given the current protocols used in their manufacturing, testing and use. I hope that, in the interest of democracy and the highest standards for the exercise of the right to vote freely by the people of India, the Commission will thoroughly examine this note. This will help to ensure the veracity of the voting process. I would be delighted to be proven wrong.

With thanks

Yours sincerely

Sd/-

Dr. Sebastian Morris (a concerned citizen of India)

(Senior Professor and Chair Centre for Public Policy and Governance, Goa Institute of Management; Former Professor, Indian Institute of Management,
Emails: morris@iima.ac.in , morris@gim.ac.in)