KICTAnet

KENYA ICT ACTION NETWORK

Memorandum on Election law (Amendment) Bill (Detailed Considerations)

Submitted to the Senate

January 3, 2017

Kenya ICT Action Network Comments for Submission to the Senate on use of technology in the 2017 General Election

Step	Event	Description
1	**Voter Registration** *Technology*	Biometric data is collected. These systems are off-grid hence no network connectivity is required.
2	**Register Clean Up and Distribution** *Technology*	After registration, all data should be collated by IEBC to check for redundancies and irregularities. Voters with problematic details should be contacted. Before the election, the complete voter register should be split per-polling station and each chunk copied onto a device. For now, let us call and picture this device as an "external hard disk". The "hard disk" shall contain the biometric data required to identify a voter at only one polling station – where they registered. After copying, the data on the disk should be hashed and compared with the hash on IEBC servers for integrity purposes. This will be useful on election day.
3	**Verify Voters on Election Day** *Technology*	Before election day, these "hard disks" should be securely distributed to their respective locations. Before the start of voting, the data on the disk should again be hashed and compared with the hash on IEBC servers. If the hashes are the same, the register is clean and voter verification can begin. If the hashes differ, they should try a backup disk. If the hashes still differ, that polling station will be on hold as they await a fresh voter register to be transmitted from IEBC HQ.
4	**Cast Vote** *Manual*	Voters pick ballot papers for the different posts and cast their secret ballot for each.
5	**Count Votes** *Manual*	The key here is that the total number of votes cast should not exceed the number of voters that the biometric devices verified.
6	**Transmission of Results** *Technology*	After all parties and agents agree on the results, they should be manually entered onto the "hard disk" for transmission. Again, once entered, this data should be hashed.

		If the polling station has network connectivity, the results should immediately be sent together with the hash. IEBC then verify the hash with the data received and if they match, they approve the results. If the polling station lacks network connectivity, the "hard disk" should be physically and securely transported to the nearest point with network connectivity for transmission from there. After all, the constitution speaks of polling station > constituency > county-level. Agents should be involved until they see "Successfully transmitted" on the screen confirming receipt of results by IEBC.

With proper testing (load testing, penetration testing, etc) staff training and sufficient voter education, the above should work seamlessly to deliver a free, fair and credible election. The most effective way to test is by carrying out at least two mock elections/simulations with dummy data to prepare all parties for any eventuality and equip them with the knowledge of how to react.

Comments from Washington Odhiambo

I have keenly considered this matter that seems to have divided the country down the middle: Manual Backup during the 2017 voting process. From the Jubilee government side this is a do or die and so it must be there. The government side seems hell-bent on confusing the masses, as well as the experts like the ICT Community. From the Opposition side, the agenda seems to be very clear - that of ensuring integrity of the Voters Register and stopping 'ghost voters' from ever casting their votes.

That brings us to the famous acronyms - BVR (Biometric Voter Register) / BVI (Biometric Voter Identification).

Having been to a Voter Registration Centre (later to become a Polling Station) to register as a voter, I did look at the equipment in use for the registration process. I saw the laptop which was fitted with a camera and fingerprints scanner. All these require power to run. I did not dwell on how they were powered, but probably there was a battery backup somewhere (besides the electricity) given that they needed to run for a whole day for several days during the voter registration process. When it comes to the Elections, they only need to run for about 11 hours. My point here is that of Backup Power should it be that there's electricity blackout and the built-in batteries can't last the whole day. That backup is very important.

However, I did not see any piece of equipment which could suggest that the equipment in use required any form of connectivity back to some central server in order to function! This now brings me to the currently national debate - Manual Backup during the Poll Day. What is it? Was the CS honest with his presentation before the Senate/Amos Wako committee yesterday? Does the CS himself really believe in the content of his presentation? I am asking that because I watched him and I don't believe him. I actually think he mislead the committee, and hence the nation at large.

Someone please prove me wrong. I am at that point where I believe that the BVR/BVI does NOT require any form of connectivity and so this Manual Backup being touted by the ruling coalition side, strongly supported by the ICT CS is a big lie. WHY?

My very first answer: Simply put, when there was no requirement for a manual backup during voter registration, it goes without saying that there is NO NEED for on the polling day.

1. For the issue that is in contention - BVR (used for BVI during polling) - this is a database that can be (and should be) statically stored on the equipment for each polling station. We are not supposed to rely on the Mobile Network to access this voters database. And every polling station can have two/three laptops/Biometrics scanner/Backup batteries to ensure that the voter identification doesn't fail.

Some excuse has been fronted about some voters being mechanics, such that their fingerprints wouldn't be recognized by the BVI systems hence need for manual identification. My take on that is that every voter must carry their voter's card on that day. The clerks can check that card number against the electronic system - enter it, and it will bring the person's picture, ID number, etc and let him cast his ballot.

2. For electronics results transmission (ERT), this is not even necessary in the first place. We can have the results collated/announced at the tallying centres after being certified - forms 36A, and such. However, if the ERT must be done, the data footprint is so tiny that a 2G network can be used. Besides, it can be an SMS based system, which doesn't require 3G or VSAT. The results data isn't that large - it can't be in Megabytes to be sincere. Well, VSAT can be used if they MUST, but this is after the voting process itself is complete, has nothing to do with BVI.

The ERT and the BVR/BVI are two distinct systems. That is what I want to believe. The ERT gets feedback from a manual process - of voters casting their vote, clerks/agents counting, verifying, and certifying, filling requisite forms then communicating the same via some customized phones which are programmed to communicate to a backend system. Am I right on that??

Now the big question here is, where do we need this much touted manual backup where network connectivity is being used as the major reason???

(a) Citing terrorism and the possibility of Al Shabaab knocking off base stations seems like well thought out lie meant to cover our eyes! If they attacked an area, I doubt there will be voting in the 1st place. And even so, the network connectivity is not required for BVI so there is no disenfranchising anyone if there is no manual backup (whatever that is).

(b) Citing hacking is neither here nor there for a BVR/BVI system because it's not being accessed live during the voting. It's a static database, unique to the polling station, resident on the laptop used by the clerks. The only hacking that can be done then can only be by an "insider". Quoting Victor Kapiyo from Social Media, "I guess it's a question of trust. Trust in systems and in trustworthy people to do the right thing. For M-Pesa, or KCSE results, we trust both. For IEBC, I guess the jury is still out."

The main issue is not allowing the dead voters to rise again to vote in the presidential vote, then disappear. So the important component here is the BVR/BVI, the credibility of the register and hence the vote.

At what point does the BVI system require this connectivity they are talking about, which then necessitates the so called "manual backup"?

Did the CS ICT lie to the Senate?? Did the CAK lie to the Senate in supporting the lie from the CS??

There is insincerity in this whole debate about 'manual backup' and the ICT community seems to either support it or is simply lost in the pool of confusion being peddled by politicians.

You say "Conversely, if the RTS fails but the BVR and EVID work perfectly, there should be less cause for alarm. Essentially, the three subsystems have a symbiotic relationship that can be used to validate or cross-check each other."

=> I do not clearly get the symbiotic relationship between the three systems as far as the main issues of contention (EVID) are concerned.

If the systems are interconnected, then, looking at it from an SQL perspective, the RTS system borrows only one column from the BVR tables - Total Registered Voters in a particular Constituency, which I believe is just a factor for cross-checking the results (reminds me of Tiaty saga).

However, this isn't necessarily part of the critical system that is supposed to stop dead voters from resurrecting and voting! I therefore think that we can mentally (or even practically de-link the RTS from the EVID to stop this insistence on connectivity, which gives birth to the "manual backup", no?

You say "Sometime the failure is maliciously engineered, while other times it is a reflection of the genuine weakness inherent within man-made systems."

==> With specific reference to EVID, I am of the opinion that it is pretty easy to mitigate failure of the system by having 3 sets of the system, which is affordable. That would address the "technical failure", but not a human/maliciously engineered failure, because the humans can kill the three or even all of the equipment. If they do this (corrupt the static DB - as that is the only show-stopper), then really, there should be no voting. I hope that doesn't happen. We still don't need 3G/4G/VSAT for this.

You say "So Cord, just as prescribed for Jubilee, should be discussing what level of electronic failure is acceptable, beyond which the results can no longer be acceptable given the potential exposure to manipulation that would arise from the manual alternatives."

==> Jubilee are advancing/contemplating the imaginary failure of connectivity occasioned either by absence/failure of fast network (3G/VSAT) or Al Shaabab knocking off what is there. This is more like making a nightmare a reality instead of the dream that it is. CORD is insisting that EVID should be used without the option of the "manual backup" and we all know that EVID doesn't require this connectivity, which supports the CORD argument.

You say "On the other hand, electronic voter identification (EVID) and the results transmission system (RTS) are quite time-sensitive. If they failed, manual intervention may be the only option available"

==> I still insist that EVID has very little to do with RTS. EVID is being used statically. The equipment, at most, has the constituency register, not the whole national register, and at the least, has just the registration/polling centre register. RTS is a system that kicks in later, once EVID has completed its role. RTS waits for data from humans - clerks/agents/presiding/returning officers. They can all congregate at the County HQ and send this data. Most County HQ have 3G. If they don't, VSAT is something that can be set up in less than 1 hour!

Your other view go well with issue about addressing possible failures, but in no way support the "Manual Backup" for EVID. This manual backup thing is a red herring, visible immediately you de-link connectivity from the debate.

Which brings me to your conclusion: "So who is right and who is wrong? Unfortunately, both sides are right and at the same time, very wrong."

Comments from John Walubengo

Point1: Can we delink RTS from EVID?

Yes we can. From the perspective of functionality, EVID does NOT need RTS to work and vice versa.

However, from an audit perspective (e.g after potential rigging), the data in EVID can be compared to the data transmitted by RTS to identify ghost voters. Hence the symbiotic relationship - and the need for ensuring that at least one of these two systems MUST work. In cases where BOTH EVID and RTS fail, then voting exercise must be repeated since the exposure to rigging is far too high to the point where reliability of the results cannot be guaranteed as per the constitution (ref: secure, verifiable, transparent, accurate)

In other words, we must accept that failure may occur, but we must also reject that failure will occur in totality. Where failure occurs in totality, we must be willing to repeat the process in the specific constituency/county/country. That is the cost of democracy.

Point 2: Can EVID fail - Maliciously or otherwise?

True you dont need 3G/Satellite systems for the EVID component since it is simply comparing your fingerprint at the point of voting, to the fingerprint you digitally supplied at the point of biometric voter registration (BVR).

However, failure can occur in what we call false positives or false negatives arising from environmental conditions rather than technical (battery failure etc). Humidity, dust, temperature variations can make the fingerprint reader fail to recognise you (false negative). More advanced EVID can then identify you by your eyes (Iris), voice or other biometrics but I doubt the IEBC system will be this advanced.

Solution: allow for manual identification - ON CONDITION that the RTS will work within reasonable time. We must set time frames within which RTS should work, it cannot be acceptable that it works, 1, 2 or 3days later since this defeats the whole essence of RTS, which is to provide randomness in the elections results; making it difficult for parties to do the mathematics needed to pass the magic 50%+1. This mathematics only happens when their is a pause or stability in the results being released.

Point3: CORD insisting on pure electronic system vs Jubilee insisting on manual system.

Whereas electronic systems reduces chances of manipulation, CORD stubbornly refuses to appreciate Point2 above, which is that e-systems can fail. Jubilee on the other hand stubbornly refuses to accept that manual systems introduced are open to manipulation. There must be a middle ground that allows for failure, without necessarily allowing for rigging. Both sides do not want to spend time on that agenda. How to plan for failure, while reducing chances of rigging.

Point4: VSAT technology?

Ofcourse VSAT can work. Even if Alshabaab blew up the GSM masts, we can still transmit results via VSAT/satellite phones. Last time I checked, terrorists do not yet have technology or grenades that can blow out and bring down satellites from the skies.

==> That's because we are not there to talk to them and enlighten them.

Comments from Grace Mutungu

I remember a quote by the IEBC CEO during the Kenya IGF where he stated that being a Republic based on democracy, we have made elections the only means to access power. https://livestream.com/internetsociety2/kigf

He recalled the use of technology in the 2010 Referendum, 2013 elections and the various by-elections that have taken place. In the Referendum and most by-elections, there was not much contest about use of technology while for 2013 some issues were raised- these included multiple registers, voter impersonation and transparency.

The tech community has an important role to play in demystifying some of these concepts.

a) The wording of the amendment read "complimentary mechanism for identification of voters". It has now been expanded to include transmission of election results "where technology deployed initially fails". What would this mean, in the case of identification of voters and in the case of transmission of results? What complimentary systems were envisaged here? "Manual backup?" The ambiguity in the wording is a challenge as it leaves too room for interpretation in a system of high contests.

b) The mischief that technology was meant to cure in elections management was among others allegations of voter impersonation and transparency in management of elections. Tech is therefore supposed to achieve simplicity, accuracy, verifiability, security, accountability and transparency. Is the conversation about a “complimentary" system a necessary one at this stage?

Outside of the amendment, has anyone come across the data that CA presented on network coverage in the counties? A visualization of that data besides the polling stations would be useful in helping us identify the specific polling stations/tallying centers that are not covered. I am asking this because the presenters spoke of areas not covered by network as opposed to polling stations/tallying centres not covered.

Comments from Collins Areba

Main issues in the debate:

1: Voter registration: collecting details, photos and fingerprints. (Multiple data types)

2: Verification: ascertaining that registered persons are in the system, and dead / expired ones are removed from the system. (Boolean: yes / No)

3: Voting: choosing from one of several options.

4: Tallying : counting the choices at the polling stations and recording the results on paper or device.

5: Transmission: sending this information to regional and national tallying centers.

Comments from Ngigi Waithaka in response to Collins Areba

The only areas that require Information Technology are 1, 2, 4, 5. 1 has already happened.

For 2, 4, 5, why would a backup have to be manual? Manual has to be the last resort. What worries / concerns me is how it seems that there is almost a quick rush to use a manual system!

Case in point, for verification; all the polling data should be local, hence on laptops at the polling station, if one laptop fails, then you can verify with another. Probability of say 5 laptops failing in a single polling station at the same time is close to nil, unless direct sabotage.

On transmission, if Safaricom fails, use Airtel, if Airtel fails use Orange, if Orange fails, use Satlink. All you need is to have 3 Phones with various SIM Cards and you good. If no network coverage, get Thuraya!

On most modern systems that we use and that provide for the fabled five 9s (99.999%) uptime, there is never an option of a manual backup.

Or is there a manual backup for MPESA? Anyone here whose bank has a manual backup? Does KRA have a manual backup for iTax?

We have more than 6 months to the Election date, enough time to query the IEBC's systems.

Comments from Jimmy Gitonga

I have the same concerns myself. I reached the conclusion that it would be nice if "ICT Experts" could lay their hands on a BVI machine and show the rest of us what the problem really is. The ERT issue is a red herring. It has worked flawlessly in the bi-elections that have happened ever since. With PKI and 2 factor authentication, this can be solved for Election Day.

Comments from Eddie Kiama

In the debates I have seen raging online and elsewhere about need for a non-IT based backup system, the ICT Ministry and Communications Authority are quoted talking about the 3G coverage in the country or lack thereof. No one is talking about 2G and Satellite phone coverage. Isn't most of the country covered by 2G? Does it mean we suddenly can't transmit data over 2G which we used to before 3G? Interesting that the same Safaricom whose Mpesa can't be hacked by Al Shabaab can have electoral results transmission hacked (According to CS Joe Mucheru)! Are we suddenly analogue because elections are approaching?

Could experts here appear before the senate committee on Elections Act next week and save this country from an impending calamity driven by ignorance around ICT?

Comments from John Kieti

In my understanding, the use of electronic means to identify voters and to transmit results is more about the integrity of the election than efficiency of the process.

Therefore, when we say we need a fall back system, we should look at a solution that not only safeguards fulfilment of the bill of rights as regards the right to vote. The solution should also have in itself a fallback mechanism that safeguards the integrity of the electoral process as envisaged by the notion of "electronic means".

Simply reverting to "manual" appears a little too simplistic. This is because the spirit behind the law's insistence on "electronic" is that of safeguarding the voter identification process by way of biometric technology for instance. As technologists we will easily have consensus that biometric person identification is much more fool proof as regards positive identification than its manual alternatives (therefore not letting in the so called ghosts.

Likewise, the spirit behind electronic transmission of presidential vote tallies from the polling station is to safeguard the integrity of the tallying and aggregation process. This ostensibly reduces chances of crooks tampering with signed tally forms (form 34s and form 36s) later on, after the tallies have been announced at the polling stations.

Therefore as we consider the matter of "what if the system fails?", it may be that to maintain the spirit and intention of safeguarding the integrity of the vote, a fall back process needs to ensure that the integrity of the vote is not compromised.

For instance, why would we insist on a manual back up when both the primary system and the redundant system could be electronic. As it may have been said, in the case of presidential tally transmission, GSM technology could constitute the primary system. Then in areas where GSM connectivity is absent or doubtful, a small deployment of vsat or satellite phones could provide redundancy. It could even be a temporary Wimax arrangement in specific geographical locations. It could also be that a extra government supported investment in GSM for areas of doubt between now and June 2017 is possible. Of course commercial viability is an issue but the bill of rights argument also appears to invoke the essence of the Universal Access Fund. As one may argue, the general election is one of the crucial activities where every citizen can exercises article 1 and article two of the constitution, and it happens once every five years. Arguably there might be no better use of the Universal Access Fund than for facilitating the exercise of article 1 and article 2 of the constitution.

As regards voter identification (for EVIDs), there is people with very sweaty fingers. Others may have had accidents in the period preceding the election, causing amputation of the fingers linking them to the biometric register. Therefore such identification failure is plausible.

Notwithstanding the possibility of EVID failure, if incidences of such failure exceed 5% or say a certain threshold in a polling station, then something would be amiss and should raise a red flag. It could either be a cultural / environmental challenge in the geography of that polling station, or it could be a case of power issues with the gadgets, or as some would say, it might be "artificial" failure to facilitate "ghost" voters.

Regardless of the cause of EVID failure, and in the spirit of safeguarding the integrity of the election, it will help that every EVID failure instance triggers a sequence of well documented steps that can guarantee verifiability of a positive "manual" identification of the voter.

The easy one of EVID failures to solve is the instance of power (battery) failure. It should not be impossible to eliminate this through better training of IEBC staff and pre-charging devices. More so, increased rural electrification in the last 4 years might contribute more to alleviation of this challenge.

In conclusion, it seems important for those dealing with the Election Law Amendment to separate the two issues (1) The bill of rights and the right of every Kenyan (who has registered as a voter) to vote.

(2) Safeguarding the integrity of the vote through ensuring we have up non corruptible, verifiable and auditable electoral systems. More specifically, voter identification and presidential tally transmission appear to be areas of enhancement.

Comments from Ben Chege

Every 5 years Kenyans queue to vote, this is an exercise that we have engaged in passionately for as long as I can remember and when each round of elections is done and dusted we as a nation learn a couple of lessons which we then reuse in succeeding election cycles in an attempt to make them better.

However, looking at the current debate on the use of technology and witnessing what is happening, I suspect that there might have been an important lesson to be learnt in the 2007-08 when compared to the 2013 election cycle that has been missed and this lesson is that Having consensus among all players beforehand regarding the electoral process generally leads to widespread acceptance of the results of the process.

Electoral process should be seen as contests, where groups of people with various interests engage willingly in order to not only determine political representation but also wield the power of the state, and just like any reputable contest it has its rules. These rules are well known and understood by all players and are accepted from the onset. These rules are deterministic in that they are predictable and must be seen by all parties to be fair. For a country to have a credible election - we need everyone to feel like they have a chance in this contest since from the onset the rules of the game do not favour their opponent(s).

In 2007 ODM did not agree to the way the commissioners were picked after the terms of some expired as they felt it contravened the IPPG agreement and after the contest was done they did not accept the results announced by the commission. When the same commission asked them they refused! We all remember the situation the country found itself after the opposition refused to engage in a process they felt was flawed and disadvantageous to them. The 2017 election process is slowly mirroring the 2007 pre-election period especially when it comes to the role of technology on voting day. We are witnessing an emotive debate regarding the use of technology and the disregard of the voices of political players who hold contrary opinions. If lessons from the past hold true, this threatens the expectation of a peaceful electoral process and at the very least a credible one.

On voting day there are 4 core activities that happen within a polling station, these are:

1) Voter identification/Verification? This answers the question ? ?Are you registered to vote in this polling station??

2) Voting by secret ballot? You are given a ballot paper and then you mark it in secret and the cast the said ballot into a transparent ballot box.

3) Counting of results and declaration? Counting of all votes cast in the polling station for each race and the declaration of the votes cast in favour of each candidate.

4) Results transmission? Forwarding these results to the next level namely the constituency tally center for?tallying? and dispute resolution just in case there were any.

The? Manual? vs ?Electronic? Debate is really touching on activities 1) and 4) and therefore at the core of this debate are 2 questions namely:

1) Can we solely verify/identify voters electronically using biometrics that they submitted?

2) Can we solely transmit results to the next level using electronic means? Fortunately, these two are not really new initiatives as the IEBC has been using technology in these two areas over the last 4 years.

No one doubts the credibility boost that well executed technology has on elections. An example of this is the by-election in Kibwezi West where the winner won the race by the narrowest of margins - a paltry 175 votes and the loser did not file a petition challenging the results. This was unheard of in previous elections. Why then do we have a debate around it? Previously, the use of technology was not explicitly dictated by the Elections Act but rather the stipulation to use one form of it was found in regulations. Until now the official Electoral process has been manual where technology had been added for efficiency and confidence building. The latest Election Amendment Act 2016 has raised the profile of the said technologies from just being tools to be used in boosting confidence to be the exclusive means of conducting voter identification and results transmission.

They say once stung? Twice shy and thus it is s understandable that the IEBC is jittery in embracing technology full throttle without a fallback especially because it had technology failures in the said areas during the 2013 General elections. Technology is playing an increasing role in our lives and for us to move forward on the electoral field - I feel that this discussion needs to be informed by a mindset from big technology companies have when it comes to failure. Companies like Google, Yahoo and Facebook plan for failure more than they plan for success. They have a culture that says ?failure is OK?, a culture where people are encouraged to ask:

1) What do we do if our technology fails?

2) How do we continue fulfilling our core business that is serving our customers and users when the systems around us fail? So as Kenyans we need to ask ourselves the same set of questions and ask how it affects the core business of elections. But for that to happen we need to synthesize what our core business on Election Day is. It?s said that ?Election Day is still the one day when we strive to give equal voice to every eligible voter; the day when the woman working in the market stall has as much of a say as any wealthy banker, and the illiterate menial laborer has a voice that speaks as eloquently as any university professor. It is our shared responsibility to strive for processes and systems that ensure that every voter is given the opportunity to make their will known, and that every vote is counted? If we agree that this is the core business of elections and everything on Election Day must support this, we should ask ourselves a couple of questions, namely:

1) What happens WHEN we place a piece of technology as a prerequisite to the recording of this voice and the said technology fails and thus affects the ?core business?? What are the fallbacks available to us?

2) Since this is a contest, which out of the array of fallbacks available is most acceptable to all players?

The issues around the failure of technology have been well documented. The IEBC conducted an internal audit of the March 2013 election and rather candidly highlighted these failures. I will try and address them and possibly give recommendations in question form that should advise our choice of an acceptable fallback or perhaps a list of fallbacks to be executed in when certain scenarios playout. When it came to the identification of voters electronically, the issues fell broadly into 3 categories namely:

1) Technology problems ? some voters could not be found on some EVIDs but were present on the

manual register. Some devices run out of power, some even exploded during charging

2) Procurement problems ? getting the wrong device because procurement requirements were not met.

3) Rollout problems? Some devices were not charged, insufficient training due to late delivery and lack of manuals e.t.c. With proper planning and time to go through the procurement procedures most of these can be sorted out. The new Elections amendment act stipulates that the IEBC should have procured and set in place technology 8 months to an election and then have it tested 60 days to an election. Even with this in place some of the problems categorized as ?Technology problems? may not disappear or may only manifest themselves on polling day. In order to address them we need to ask ourselves what are the real risk factors related to technology? If the approach to voter verification is similar to what was employed in 2013 ? then the disruption of telecommunication is not a potential failure point ? why? The devices were self-contained? The register was loaded on the device and thus the device really had no need to communicate with external systems after rollout. If this is the model envisaged in the new KIEMs Rollout? We should not concern ourselves with telecommunication availability in the matters of voter verification. What should concern us is the issue of availability of power as the devices will be constantly in use throughout the day. The devices used for verification conduct a one-to-one match of voters against their biometrics? Computationally? It can be a costly affair especially if a potential voter has to submit multiple fingers to get identified if one fails and so we need to have devices that can work for 18 hours or have capability to accept external power in the form of portable power cells. Can the software be written in such a way that it alerts the users well beforehand that it has X number of hours of charge left and that the clerks at the polling station need to make arrangement to keep the electronic means working? Ghana deployed a solution that utilized dry cells and they put in place an operational plan to replace them within 4 hours.

The issue of some voters not being found on the EVIDs yet being found on the manual roll was puzzling, this may be aggravated in 2017 this is because the bulk of the current set of fingerprints were collected in 2013 and it will not be farfetched to expect that the quality of fingerprints submitted for verification in this election cycle by an eligible voter who work with their hands to be lower and thus this may require multiple passes. The current setup is one which a subset of the fingerprints collected is used to verify voters electronically. If we are to go full throttle, we will need to ensure that all fingerprints are available for matching on polling day to increase the chances of matching. An exercise to get fingerprints resubmitted for persons who fall in this category and also for all those that had their biometrics lost during the mass registration drive when BVR machines crashed and did not have backed up properly.

Another reason that could explain why some voters were not found on the EVIDs and were found on the printed register is data corruption during copying polling station data into the SD cards that the devices used. How can we ensure that databases are not corrupted during saving into the machines? I propose that each device should have a way of hashing a file and checking the hash against a verified hash of a working copy and where it differs transferring data to this device should be repeated. Backups of these registers on verified SD cards should also accompany each EVID to the field. We should explore how to keep the logs of the persons who have voted safe when devices get technology issues. There is also an inconvenient reality that in any given population there will always be some persons whose fingerprints are difficult or impossible to capture or verify. This raises a fundamental ideological question of whether a person should be disenfranchised because of limitations of a technology. The issues around the provisional transmission of results were also well documented; these also fell into 3 broad categories namely:

1) Technology problems? the server? well documented issue with system logs and it running out of space due to server misconfiguration; The failover issues that followed this. Network coverage issues; Erroneous display of tallied votes due to late integration and limited retesting.

2) Procurement/Acquisition problems? there was no time to really develop the transmission application.

3) Rollout problems ? Late delivery of phones and specially configured simcards; issues with user credentials; versioning issues between server and phone; Lack of proper training.

As with electronic voter identification, most of these can be sorted out with proper planning and following procedures, why do I say so? The IEBC has transmitted 100% of the results from all the by-elections that it has conducted since 2013. While in terms of scale these by-elections pale when compared to the general election, it?s my considered opinion that there have been numerous lessons learnt ? these can be documented and used to inform the training and rollout process. What should happen in the event that result transmission fails for whatever reason? The IEBC still needs to have a fallback for electronic results transmission. Can some other technology offer a fallback? e.g. If results transmission from a primary device fails, should we have an electronic fallback using a different technology? Can the current election transmission system be used as a backup of whatever fancy results transmission system the IEBC procures? The IEBC has used satellite phones with success to transmit results for the Kalolol and Mosiro by-elections, why can this be used as a fallback on the telecommunication side. I think we can have all these fallbacks in place and these would be totally acceptable to all stakeholders. These questions are by no means comprehensive but should act as a starting point in deciding what the fallback(s) should be and when to fallback. It has always been my opinion that leaving the determination of important electoral matters at the polling station level to the discretion of people there without a trail of documentation that guides their decision making and a trail of accountability to why they took the action they did exposes the election operation to credibility questions. In 2012 Ghana went into their election with the NVNV (No [biometric] Verification, No Voting) mantra and they had to extend the voting period and also had many people disenfranchised because of the inadequacies of the technology they rolled out. In 2015 they rolled back and then introduced a manual verification fallback. The manual verification process required the presiding officer fill a manual verification form for each voter who is manually verified. The only way we can come up with this list of scenarios is if we carried out a proper and candid risk assessment and management process. This process should inform the IEBC on what to do to ensure that the ?core business? on election day remains unaffected. From my perspective, human beings should always play the role of final "exception handlers" to ensure that during electronic voter identification no voter is ever disenfranchised by technology malfunction or its limitation. Indeed, if the electoral process must err, then it must err on the side of inclusion. However, these errors must be accounted for and thus the most appropriate role of technology is to ensure a level of transparency and accountability that allows for review of any of those human decisions on how to handle exceptions. As noted earlier on this paper, the process used for verification involves a one-to-one match of voters against their biometrics. The voter gets his ID No. captured by the verification device in a bid to? Identify? Them and once their records are loaded on the screen of the device an additional fingerprint scan is required to? Verify? This person i.e. answering the question? Are you really the person who you claim to be? So, for example, if the validation device is unable to verify the fingerprint of a voter who the presiding officer knows or strongly believes to be a legitimate voter, and his/her particulars are on the voter register, the presiding officer should have the authority to override the device and allow the person to vote. In order to trigger the manual verification process, the presiding officer should collect as much information about the person being excluded from being electronically verified as possible. This information should include a photo of this person and the Serial Number not ID No. found on their National Identity card. Manual verification should not be misconstrued to mean manual verification using the physically printed out register or green books. This process should be endorsed by all party agents present at the polling station. It is important to have this information both in physical and electronic form. At the end of the day, any final reconciliation should include the number of decisions the presiding officer made contrary to the technology. This allows for review of the decisions of the presiding officer, and provides a deterrent since that officer knows that there will be an accounting of how many decisions he made of this nature. It also allows for reporting on anomalies where a polling station or ward has an inordinately high number of human exceptions. This information can be transmitted periodically so that during the course of the day to all stakeholders and thus all players are able to identify polling stations that have inordinately high numbers of human exceptions and vigilance can be increased to ensure only legitimate cases are excluded from electronic verification. Once this discussion has been held and we have a product that this has the blessing of all players contesting in the election. When accepted by all stakeholders the post-election process of massaging bruised egos and selling peace i.e. the 'accept and move on' message will be much easier.