Electronic voting no threat yet to the old style ballot box

July 12 2010, by Adrian Addison

An employee (L) of Smartmatic demonstrates the function of election automation machine next to Philippine Commission on Elections officials in Manila last year. It was hoped electoral automation in the Philippines would cut rampant cheating, where ballot boxes went missing or were stuffed with fake votes and local officials sometimes simply fiddled the results themselves.

They held elections within days of each other: The Philippines, a lively democracy where politicians get shot dead in the street and Britain, the rock solid 'mother of all parliaments'.

But the Asian state's quick-fire digital vote made the European nation look more like a grandmother as its citizens stuck to the old style of dropping bits of paper in battered old boxes.

It was hoped electoral automation in the Philippines would cut rampant cheating, where ballot boxes went missing or were stuffed with fake votes and local officials sometimes simply fiddled the results themselves.

There was also the logistical nightmare of collecting votes from a country made up of over 7,000 islands, some of them tiny.

The May 10 poll, which was overseen by the government authority Comelec, had some minor glitches but Comelec commissioner Gregorio Larrazabal said: "Definitely it was a success.

"Everybody knows that it worked. There were some kinks that need to be ironed out but it was generally successful," he told AFP.

"Ask the people on the streets, ask the citizens' organisations who monitored the elections, the teachers who conducted the elections, they say the same thing."

In Britain, there were angry scenes outside a handful of polling stations which had closed before thousands of people had voted on May 6, leading some commentators to describe it as a "third world" ballot.

"It’s largely a legacy of the Victorian era," said Jenny Watson, the chairman of the Electoral Commission which sets the standards for running elections for Britain's 45-million voters.

"It’s not sensible to have a system that was designed when five million people were eligible to vote," she told the BBC.

In the Philippines, Venezuelan company Smartmatic won the contract to run the electronic election. Voters still had to go to a booth and mark a piece of paper, but it was fed into a machine for counting, not a ballot box.

The results were then sent electronically to election headquarters in Manila, with 30 copies printed out and sent to stakeholders as a back up.

"Electronic voting can bring credibility to a country with a bad history of fraud, and whose officials are not considered legitimate," Cesar Flores, the company's president for Asia-Pacific, told AFP

"Electronic voting will be the norm in 20 years from now, and only a few countries will remain counting votes manually. It is not a question of 'if', but 'when'.

"As long as the system is auditable, and recounts are available, the benefits significantly outnumber the possible risks."

But it is exactly these risks that make the world's electoral authorities nervous.

Ingo Boltz, an Austrian electronic election expert, urges caution in adopting automated voting. The human element in traditional elections, he says, can often be its greatest asset.

"With a traditional ballot box, every layperson can, without the use of expert knowledge or tools, follow and verify every step of the election process," he told AFP.

"As long as an observer is physically present, the process is completely transparent to the naked eye. The price of automated voting is the delegation of these tasks to a handful of information technology experts.

"And most IT security experts agree it is basically impossible to guarantee that an eVote system does exactly what its programmer says it does. We are obliged to trust that programmers are incorruptible."

As ever more people bank and shop online, will the world soon vote remotely online?

Most election experts think not. The biggest problems of fully remote systems are secrecy and "cyber-terrorism".

Secret ballots could be compromised, for example, if the patriarch of a large family wanted them all to vote in a particular way -- he could be in the room to make sure they did exactly that.

Computers could be infected with a virus that would manipulate the vote without the voter ever knowing, or used to launch a denial-of-service attack in which infected computers bombard the system until it overloads and shuts down.

The Open Voting Consortium (OVC), a US advocacy group dedicated to delivering trustworthy elections, was set up after the debacle of the 2000 US presidential elections because, the founders said, "nobody could figure out how Florida's voters had voted".

The election was left in disarray partly due to errors in the state's punchcard system that brought infamy to "chads" -- fragments left when holes are made in paper.

The election was so tight, and the vote so close in Florida, that these voting machine errors became crucial. An OVC electronic voting machine should be available soon.

But one of OVC's founders, Alan Dechert, says mass uptake of fully electronic elections is not on the horizon.

"We are a very long way from having a system good enough to be widely trusted for this type of purely electronic voting," he told AFP. "I don't

see this type of system taking hold in the US over the next 100 years."

Electronic voting machines are currently used in India and Brazil and have been tested at some level in many other countries, including Britain.

But in India there is growing concern after Dutch and US scientists proved that the Indian system can be manipulated, and results altered. Holland, Germany and Ireland have all abandoned using electronic voting machines.

Silvana Puizana, an electoral expert who has worked on very different election challenges from Afghanistan and Albania to Suriname and Australia, is also cautious.

"Think of the evils bestowed on so many people by bad governments and governments who will stop at nothing to stay in power," Puizana told AFP.

"The most effective fraud is done by changing results after the count is done -- how much easier is that going to be to do undetected when there is no paper trail to trip you up?

"And you, as the corrupt government, control everything anyway. Don't like the result? Just change it, and no one will ever be able to prove you did it!

"I've seen too much fraud and corruption done with impunity to wish to make it even easier for them to do it in the future -- with a virtual promise of being undetectable."