Image not found or type unknown

www.juventudrebelde.cu

Sufragio en EE.UU. ¿Fraude en las teclas?

La posibilidad de fallos en las máquinas electrónicas de votación, e incluso de un engaño a gran escala en los comicios estadounidenses, es cada vez más alarmante

Publicado: Jueves 30 octubre 2008 | 01:47:08 am.

Publicado por: Amaury E. del Valle

Foto: AP Un simple golpe de tecla, un cortocircuito y hasta un «cambiazo» masivo de votos aprovechándose de las debilidades que aún tiene la aplicación de las nuevas tecnologías en los sistemas de votación, podría determinar quién será el próximo presidente de Estados Unidos.

La afirmación, aunque parezca exagerada, es real y cada vez más alarmante, según han denunciado diversas organizaciones independientes e investigadores, quienes han puesto al descubierto la fragilidad del sistema de votación electrónico estadounidense.

Ya polémico en las elecciones de 2000, cuando hubo máquinas que registraron votos a favor de Bush y en realidad el elector había marcado por Al Gore, el sistema de votación electrónica se ha extendido, al punto de que se estima que unos 50 millones de norteamericanos de 24 estados lo usarán en las venideras elecciones.

A lo anterior hay que sumarle que el sistema de votación en Estados Unidos es indirecto, ya que el presidente es elegido por un Colegio Electoral conformado por delegados que se seleccionan en cada estado y cuyo número está en relación con el número de habitantes.

Así, el candidato que triunfe en cada estado ganará la totalidad de los delegados que corresponden a ese territorio, por lo cual todo voto de más o menos cuenta mucho. Y en ese contexto, cualquier adulteración a las máquinas puede ser mortal.

¿Hackers demócratas o republicanos?
Un artículo publicado en Granma Internacional por el periodista Jean-Guy Allard sobre las venideras votaciones del 4 de noviembre en Estados Unidos, denuncia que órganos de prensa como PrisonPlanet.org han afirmado que existen hackers o piratas informáticos listos para robar la elección presidencial 2008 a favor de John

McCain, al manipular el funcionamiento de las máquinas de votación.

«Stephen Spoonamore, un republicano que trabajó en las campañas electorales de Rudy Giuliani, Michael Bloomberg, y que es especialista de sistemas de comunicaciones, asegura que McCain tendrá una “espeluznante recuperación” que le otorgará 51,2 por ciento de los votos», asegura el periodista.

Y la tesis pudiera hacerse muy real, ya que es conocida la fragilidad del sistema de voto electrónico, e incluso algunas verificaciones realizadas por equipos independientes atestiguan que se puede adulterar el funcionamiento de las máquinas de voto en apenas 30 segundos.

A lo anterior hay que agregarle que el uso de esta tecnología implica a su vez la transmisión de datos a través del teléfono, redes privadas de computadoras o Internet, todas las cuales son vulnerables a cambios espurios a favor de uno u otro contrincante.

Para entender mejor lo expuesto es importante saber que el llamado voto electrónico o «e-voto» comprende varias modalidades que abarcan tanto modos electrónicos de emitir votos como medios para contarlos.

Creados desde la década de 1960, con el uso de tarjetas perforadas que podían leer las máquinas, existen también sistemas de votación mediante escáneres ópticos, que visualizan las marcas hechas por uno u otro candidato en las boletas, e incluso se han extendido con fuerza los quioscos de votación especializados (Sistemas de votación de Registro o Grabación Electrónica Directa, DRE por sus siglas en inglés).

Estos últimos han sido especialmente polémicos, ya que en ellos el elector pulsa una tecla o acciona una pantalla táctil para manifestar su preferencia, lo cual muchas veces no ha funcionado correctamente.

A los sistemas DRE se les ha criticado especialmente porque en la mayoría de los casos el voto es totalmente «electrónico», ya que muchas máquinas no emiten ninguna papeleta de verificación, con lo cual el registro no es transparente, y quien pulsa la tecla nunca sabe si la máquina, efectivamente, registró su verdadero deseo.

Otras polémicas sobre el voto electrónico involucran también a los sistemas de transmisión de boletas por redes informáticas, que son especialmente frágiles a la introducción de datos espurios, ya sea alterando el software que usan o simplemente modificando las bases de datos a donde van a parar las «intenciones» de voto.

El mal de las teclas locas

El primer escándalo a gran escala sobre el fraude masivo con el voto electrónico se dio en las elecciones de 2000 en Estados Unidos, cuando el actual presidente George W. Bush ganó por decisión de la Corte Suprema, a pesar de que su rival Al Gore había acumulado más votos populares.

En ese entonces, si bien todavía estos sistemas no estaban muy extendidos, varias organizaciones alertaron sobre la posibilidad de que hubieran sido manipulados a favor de Bush. Sin embargo, serían las elecciones de 2004, cuando Bush volvió a imponerse sobre el demócrata John Kerry, el volcán en erupción del voto electrónico, cuando se demostró la actuación «fallida» de muchas máquinas.

Así, por ejemplo, las computadoras del estado de Carolina del Norte no registraron alrededor de 4 500 sufragios, y muchos ciudadanos se quejaron de que al intentar manifestarse por el candidato demócrata, John Kerry, lo registraron como un voto para Bush. Similares denuncias hubo en varios estados, donde las teclas parecían haberse vuelto «locas» y marcaban a favor de un Bush «bendecido» por los bytes.

Curiosamente, apenas unos meses antes, cuatro de las empresas que proveyeron de sistemas electrónicos de voto

al sistema electoral de Estados Unidos, se vieron sometidas a una serie de pruebas en las instalaciones de Compuware, y se descubrió que el código fuente de las aplicaciones era vulnerable y que podrían sufrir ataques de intrusión críticos.

Los análisis de los sistemas de Election Sys- tems & Software, Diebold, Hart InterCivic y Sequoia Voting Systems arrojaron un total de 57 agujeros de seguridad identificados como potencialmente peligrosos en una supuesta votación electrónica, algunos tan graves como el de permitir que una persona no autorizada pueda acceder a la base de datos donde se almacenan los resultados y cambiarlos.

Lo más interesante es que las propias empresas sabían ya de sus «debilidades» y las ocultaron deliberadamente, como demostró nada menos que un hacker, quien en marzo de 2003 se introdujo en los servidores de la compañía norteamericana de sistemas de votación electrónica, Diebold Elections Systems, y copió 1,8 gigabytes de datos, la mayoría correos electrónicos desde 1999 y documentos internos.

Diebold, quien suministró máquinas a 37 estados estadounidenses y repartió más de 50 000 terminales por el país para las elecciones generales de 2004, conocía los graves errores de seguridad en sus programas, que podían provocar fraude, como la posibilidad de cambiar votos sin dejar rastro, o la instalación de programas no certificados por las autoridades.

Aunque Diebold trató de evitar que documentos internos donde se evidenciaban estos problemas salieran a la luz pública, un grupo de estudiantes del Swarthmore Collage, de Pennsylvania, conocidos como Why War? iniciaron entonces una campaña de desobediencia civil digital, negándose a retirar el material de Internet.

A pesar de todo el escándalo, y de que Diebold fue sometida a alguna que otra verificación, sus máquinas estuvieron presentes en las elecciones de 2004, y su sistema de votación Premier Election Solutions (antes Diebold Election Systems) TSx descalificó a muchos ciudadanos en los condados de Alameda y San Diego, a causa de tarjetas cuyos códigos no funcionaban.

Desde entonces entidades como la Escuela de Derecho de la Universidad de Nueva York han emitido informes donde atestiguan más de 60 ejemplos de fallas de máquinas electrónicas de votación en 26 estados entre 2004 y 2006, pero la práctica ha seguido ganando posiciones, incluso con empresas muy poderosas a la cabeza, como Diebold, que dicho sea de paso, fue una fuerte contribuyente a la campaña electoral de McCain.

Voto espacial

Un informe reciente elaborado conjuntamente por el Centro Brennan para la Justicia, de la Universidad de Nueva York, la Fundación Voto Verificado y la organización Causa Común otorgó una baja calificación a los sistemas que se emplearán en varios estados clave, entre ellos Colorado y Virginia.

Según declaró a la agencia de noticias IPS Lawrence Norden, director del Proyecto de Tecnología Electoral del Centro Brennan, «si no se hace un control efectivo luego de la votación, es fácil perder 100 o 200 sufragios aquí y allá.

«Estos problemas son mucho más serios cuando la elección es reñida. Si este llega a ser el caso en Colorado y Virginia, los problemas pueden ser potencialmente grandes», advirtió el experto.

A su vez un informe conjunto de estas entidades, titulado ¿Está Estados Unidos listo para votar?, asegura que es muy posible que el próximo 4 de noviembre los sistemas de votación fallen en una o más jurisdicciones del país.

Las mismas entidades estatales han reconocido estos problemas en informes anteriores, como el publicado en

mayo de 2004 por la Oficina de Responsabilidad Gubernamental de los Estados Unidos, titulado El voto electrónico Ofrece Oportunidades y Presenta Desafíos; o el emitido en septiembre de 2005 detallando algunas de las preocupaciones y mejoras alcanzadas, bajo el título de Están en marcha esfuerzos federales para mejorar la seguridad y confiabilidad de los sistemas de voto electrónico, pero se necesita completar actividades claves.

Las preocupaciones se centran, en lo fundamental, en la posibilidad de que fallen los circuitos electrónicos, sean afectados por un virus, se introduzcan informaciones erróneas, se desconozca cómo funciona el software de las máquinas y por ende no sea auditable, no haya modo de verificar en papel el voto electrónico, o simplemente se cometa un fraude a gran escala.

Con esos truenos, y ante la posibilidad de que por primera vez un afroamericano llegue a la Casa Blanca, muchos se preguntan qué pasará con los teclazos de los electores, o cuánto cambiarán los datos al viajar a través de las redes electrónicas.

Quizá lo mismo se estén cuestionando los astronautas Michael Fincke y Greg Chamitoff, quienes por primera vez en la historia emitirán su voto desde la Estación Espacial Internacional, a más de 450 kilómetros de altura, y lo harán por vía electrónica.

Habría que ver si en el largo camino desde el espacio sus boletas no cambian de candidato.

http://www.juventudrebelde.cu/suplementos/informatica/2008-10-30/sufragio-en-ee-uu-fraude-en-las-teclas

Juventud Rebelde | Diario de la juventud cubana
Copyright © 2017 Juventud Rebelde